**Appendix N**

**Transcript from think aloud study**

**P302**

P302: The e-mail address is HR\_dept33433; it doesn’t sound very official. It’s @yahoo rather than at a company address. The e-mail, CV isn’t capitalised, but that might not be too big a thing. “My shortlist” doesn’t sound very professional. No spelling mistakes that I can see though, but the e-mail address is dodgy. I’m going to put it at a 2 because it’s not definitely phishing, but it looks dodgy.

The e-mail address is not particularly easy to understand. It’s unlikely you’d use the, “I am writing you,” if he was born in London. It’s American. “\_\_\_[0:02:50]” is strange phraseology, bad grammar. It does improve, grammar and spelling etc. Definitely phishing because, well, for one, it’s very strange to not know the full name of the person you think of trustworthy enough to leave your entire fortune to.

[HMPSrecruitment@igrasp.com](mailto:HMPSrecruitment@igrasp.com), I’m not sure who “igrasp” is, but it’s more \_\_\_[0:04:34] than the first one. You can paste it into your browser. The two web links are different, for different things. It could just be if you had an account with something called igrasp, I guess.

Verifiedbyvisa.com sounds very legitimate. It has at least a logo. But banks don’t ask you to just click on links and reactivate your credit card and it’s highly unlikely. So although the e-mail was legitimate, what they’re asking doesn’t sound legitimate, so 2.

So it’s paypal.co.uk, sounds a legitimate e-mail. That is the PayPal logo. They know the card number so if you find that’s correct, we’ll be able to work from somewhere that could mean they’re more legitimate. They’re not asking for a PIN and it’s a likely thing for PayPal to need. The reply stuff sounds genuine. I’d say 5.

\_\_\_[0:08:24] natwest.com sounds fairly legitimate. That’s the Natwest logo. That’s the current account number, which I assume it is and they have that information. It talks about online security, so I’d say a five.

Gucci, Cartier, Rolex, \_\_\_[0:09:33]. Yes, that sounds very dodgy, the name of the people doesn’t link to the actual e-mail address. They’re all desirable luxury brands, put together. It doesn’t look very visual. It’s definitely phishing.

The name is Philippe Jean; the e-mail is \_\_\_[0:10:21], that kind of links. I suppose it depends whether you know a Philippe Jean, if you don’t, definitely phishing. If you do, it could be, but still, never trust an e-mail directly asking for money, so two, three.

eBay administration, admin@ebay, well, I mean eBay but eBayz.com doesn’t sound as legitimate. That’s the eBay logo. I suppose it depends whether the user agreement section online actually does say that. The link does say ebay.com, but obviously that might not be where they’re taking you. That is all the copyright things. Three, four… four.

\_\_\_[0:14:04], [cards@classicFX.com 0:14:05]. Okay, I don’t know about that. It’s not directly asking for information or money. I’d say five, it looks very legitimate, I mean obviously the link could take you anywhere.

DDF.193@ \_\_\_[0:15:01] .com really, really doesn’t sound legitimate; though that is the correct tracking number, that’s impressive they know that, or disturbing. Yes, the FedEx situation is believable, the FedEx logo, but yes, the e-mail just doesn’t look – so two.

\_\_\_[0:15:51] USextra.co.uk, if that’s where the actual e-mail address has come from rather than just the name of it, looks fairly legitimate. That’s a very basic e-mail and the link is incredibly long. That’s the correct IP address. That said, just confirming password things are normally all quite basic. Four.

barclaysonlinesupport@vnet. I wonder what vnet is, it sounds a bit dodgy, but Barclays online sounds right enough. Barclays logo, it doesn’t have a name. No descriptions of your name, but other than that, legitimate situation. I’m using legitimate too much. Three.

The name and e-mail address match. The fact that they have a Doddle account is very dodgy, the fact that it’s from a person at the college, rather than a company or business where you might have an account. I would say definitely phishing, one.

\_\_\_[0:18:28] .co.uk, fairly legitimate, as far as the e-mail address makes sense, but the hyperlink is going to myface.com, which really, really doesn’t sound right. It has no logos or company styling or that you’d associate with an e-mail from a big company, so definitely phishing.

PlusNet Sport, [sport@plus.net](mailto:sport@plus.net), I suppose that sounds right. Yes, I assume that’s your username. No logos and stuff, but fairly basic. It says McAfee \_\_\_[0:19:44] downloads in the link, or the link name, so they at least bothered to get that right, if \_\_\_ wrong. Five. It looks quite legitimate to me.

[Frank@easyroommate.com](mailto:Frank@easyroommate.com), so it’s got the easyroommate.com. The link is titled 2uk08 and true, it does say “\_\_\_[0:21:07] scam,” so this person is \_\_\_ there, if it is one. Four.

[Info@hsbcbusiness.co.uk](mailto:Info@hsbcbusiness.co.uk), that’s a fairly sensible sounding e-mail address. The HSBC logo, does it look like that or is that an old one? It shows no kind of, “This account,” what your account number is and what your name is, so a two, phishing to me.

It’s tiny, so it’s not very considerate if they did decide that. \_\_\_[0:22:26] co.uk is a fairly sensible sounding e-mail address. Invoice number, registered name. It doesn’t have any branding, but it looks fine to me. Five.

Again, tiny, not very considerate. \_\_\_[0:23:37] fairly sensible, \_\_\_, case number, service tag, so that helps and sounds better. Dell logo. Five. That looks pretty good to me.

I haven’t heard of \_\_\_[0:24:43], but I have mail.com, matches, sounds sensible. The e-mail address is okay. The attachments are strange, show attachments, that’s a bit dodgy, but it sounds a realistic situation, normal e-mail, Google branding. Four.

The \_\_\_[0:26:53] doesn’t match Natwest, so that’s dodgy. It does have Natwest branding though. I didn’t really know online accounts did expire, I’m not sure if they do. \_\_\_ I’d say definitely phishing.

\_\_\_[0:27:33] not Amazon, so that’s strange. It does have Amazon branding, it’s in Amazon font, layout etc., so the e-mail looks really right. So yes, this e-mail looks fine, just the e-mail address isn’t correct, so two.

Dropbox, dropbox.com makes sense, so that’s right. It says your name and has Dropbox branding and the e-mail address sounds fine. I’d say it’s probably legitimate, fine.

[service@paypal.com](mailto:service@paypal.com), well, the name of the account sounds right, [approximatingdz100@makingmusic.com](mailto:approximatingdz100@makingmusic.com), really doesn’t match the e-mail address. That’s the seller, so I don’t know about that. There’s a lot of information, kind of like mail. I’ve never bought anything off eBay so I don’t really know what it would look like, or paid via PayPal like that. Four, considering I thought that was weird. Maybe it’s the seller, that makes sense.

[paypal@e.paypal.co.uk](mailto:paypal@e.payment.co.uk), fairly sensible, e.paypal is a bit weird, but yes, branding looks nice. There’s the name, there’s details like, “Trouble reading this,” “Copyright,” I don’t think it’s a spoof e-mail. It sounds slightly too eager to owe you \_\_\_[0:30:57] number, really suspicious. Four.

Customer care e-mail, mail@wsystems sounds sensible, branding is correct. It sounds a realistic situation. But if they’re saying an attacker hacked into their network, you’re going to be slightly suspicious of anything going on right now, so four.

\_\_\_[0:32:14] makes sense as an e-mail address. That the images don’t process is a bit weird. It doesn’t really have that many links so unless you are going to [save all 0:32:42]. Cancel the transaction is not working, that’s something you’re going to definitely click on the link for, but the fact the images don’t come through is a bit weird, but you know, computers are computers I guess. Four.

Facebookmail.com doesn’t sound \_\_\_[0:33:24], not sure about that one. It does say Facebook mail, but then doesn’t everyone have Facebook mail? It does have a name. Four.

Virgin Mobile sounds sensible, yes. That there isn’t a name for the attachment is weird and that there is an attachment and they don’t say what it is is also strange. There’s no particular rush for you clicking on the links though. There’s no branding, which is weird, so I think four.

\_\_\_[0:34:44] name and e-mail don’t match. I don’t actually know what they’re talking about, but yes. If it’s an American company it makes sense that they spelt \_\_\_ that way, but if it’s not, it doesn’t. “If you already authenticated your account,” looks bad; a two, it sounds very fishy. No branding.

\_\_\_[0:36:14], two Es in finance is a bit weird, but @direct.gov.uk is sensible sounding I guess, not personal though. It does have correct branding though, well, not up to date branding, but if it was in 2012 it might have been, I guess. Three, pretty sure it’s phishing.

\_\_\_[0:37:17] .co.uk, maybe \_\_\_ survey I guess. No branding. I don’t recognise it as a survey thing, like SurveyMonkey or something, but that doesn’t mean it can’t be one I suppose. The fact there isn’t branding is weird. Three. They would be shouting about the winning thing more.

The e-mail didn’t load. Oh no, it has now. DFT, the name and e-mail address don’t match, the e-mail address doesn’t sound right. It has a logo. It’s not personalised. .gov.uk, yes, the situation in which you don’t upload your details within two weeks of receiving this and having to take a fresh driving test is completely ridiculous, so definitely phishing.

@Lancaster.ac.uk, it’s a Lancaster address, it makes sense. “Dear student…” yes, no particular reason why that would be personalised in this situation, SurveyMonkey, I recognise that as a survey company. FCUG survey 13 makes sense. I’d say five.

**P303**

P303: Blah, blah, blah… \_\_\_[00:00:11]…

[Silence 00:00:11 - 00:00:37].

“Lung cancer”… I would \_\_\_, especially for…

“Confidence… [To hand 00:01:01]”.

[Silence 00:01:01 - 00:01:40].

Okay so… Phishing, because [everybody can go].

“Important customer information”.

[Silence 00:02:01 - 00:02:41].

I think it’s legitimate because there’s the logo of the company. Yes, I think it’s legitimate.

[Silence 00:03:08 - 00:03:24].

I’m not sure about this one, but it seems like… “We will expire in three days.” Why can your password be expired? I’ve never heard this before. “Upgrade your webmail”. The email address seems not very common; I would \_\_\_[00:03:57] to them.

Paypal.uk…

[Silence 00:04:08 - 00:04:50].

Yes, I think it’s definitely legitimate.

[Silence 00:04:54 - 00:05:07].

“Write the first and last name if you are concerned about a security attack”. Yes I think it’s definitely legitimate because there is the logo of the company.

[Silence 00:05:39 - 00:07:00].

I’m not sure about this one, because the \_\_\_ everyone can \_\_\_, so it would be two or three.

[Silence 00:07:17 - 00:07:35].

I think it would be two.

I think it is definitely legitimate because… “Verify your address”. “Now we require your postal code”.

Well, the address is abnormal because it’s support@vns.com.

[Silence 00:08:15 - 00:08:38].

\_\_\_ the [contact number] \_\_\_.

[Silence 00:08:43 - 00:09:16].

“Student Finance England”.

[Silence 00:09:18 - 00:09:37].

“SL student key”. I think it’s definitely phishing. Yes because the address is abnormal, [my face 00:10:05].

[Silence 00:10:05 - 00:10:32].

I think it’s definitely phishing because the logo is not correct and… “[chefsbusybusiness.co.uk]”. Yes and customer business \_\_\_.

The email address if wrong because e, b, y is set after EBay, and the email of EBay members would be someone’s first name.

[Silence 00:11:33 - 00:12:35].

“\_\_\_”. Yes I don’t know if they would suspend my account because… \_\_\_[00:12:46 - 00:12:56].

[Silence 00:12:56 – 00:13:10].

Yes I think there is no connection between legal liability and financial loss and the update of personal records and online experience.

I think this one is legitimate because the address is directgov.uk.

[Silence 00:13:59 - 00:14:21].

Yes, I think it is legitimate.

\_\_\_.com.

[Silence 00:14:29 - 00:15:05].

Five, if I have just signed up to the website. Or four. “Please do not reply to this email”. Yes, four.

[Silence 00:15:33 - 00:15:52].

Why is it an attachment? \_\_\_. “Because we are the same [lettings firm]”.

[Silence 00:16:12 - 00:16:29].

I think it is two. It could be. Or with that \_\_\_ one.

Why is it after 20th October but it’s not? But you already have [mobile bill].

I won’t definitely finish it.

[Silence 00:17:17 - 00:18:29].

I think it is definitely legitimate because it doesn’t ask me to click on any address and just the information of the payment that I have made, so yes, definitely legitimate.

[Silence 00:18:58 - 00:19:30].

Yes, I think this one is legitimate because they say, “Your latest statement for account” ending 801, so they know your account number. Definitely legitimate.

I think this one is legitimate. “[Phone caller green 00:20:15]”. Yes, there was \_\_\_ should be \_\_\_ not phone caller green. Definitely phishing.

[Silence 00:20:36 - 00:20:53].

Definitely phishing because “\_\_\_ award. Get ready for…” Yes, definitely phishing.

[Silence 00:21:06 - 00:21:59].

I would say five. Or four. Five, because the emails seem alright. The address is a little bit weird.

[Silence 00:22:17 – 00:22:46].

I’m not sure. I think it could be more detailed. \_\_\_ big companies I would say.

“Create a new password”. \_\_\_[00:23:12], I’m not sure.

[Silence 00:23:14 - 00:23:36].

I would say five. \_\_\_. I would say six. Five. Six. Because the address seems weird, but it’s facebookmail.com. Facebookmail.com, facebookmail.com. Two. Four.

[Silence 00:24:26 - 00:24:57].

[Set meals], put into. I would say definitely phishing because the \_\_\_ may not, my name is \_\_\_, and here you’re saying, “Hello”. This email could be sent to anyone.

I would say definitely phishing, because this is \_\_\_[00:25:40].com.

[Silence 00:25:42 - 00:26:15].

I would say six. Yes, because it’s only an \_\_\_, it doesn’t ask you for money or…

[Silence 00:26:26 - 00:27:22].

I would do two, because the address and the [person] who sent it does not match, which I \_\_\_. Yes.

Yes I would say six, because it doesn’t do anything, just... Let’s you just purchase some items.

[Silence 00:28:17 - 00:28:51].

“\_\_\_”. I would say two. Three. Yes, because if there is some reason that they have to suspend my credit card they will ask me to come to the bank instead. Update my information on there.

[Silence 00:29:34 - 00:30:02].

Be a guess was \_\_\_. I think they would have my last name. Two.

[Silence 00:30:15 - 00:31:11].

Two. Four.

[Silence 00:31:27 - 00:31:45].

\_\_\_ because the address \_\_\_. \_\_\_.com.uk.

[Silence 00:31:53 - 00:32:43].

Yes I would say four. “Update card”. Or five. “Make sure you’ve \_\_\_”. Yes I would say it’s legitimate.

\_\_\_[00:33:25]. Well I think it’s definitely legitimate because, “You’re card is about to expire”. They will have your expiry date and security code already.

[Silence 00:33:44 - 00:34:49].

Yes I think it’s… Five. “Tracking number”. “Tracking number…”

Yes I think it’s definitely legitimate because they have your tracking number as well as the order number, yes.

[Silence 00:35:37 - 00:36:05].

Two. “\_\_\_ or attachment”.

[Silence 00:36:07 - 00:36:32].

Five, or four, because there is no attachment. I would say four.

[Silence 00:36:46 - 00:37:08].

I think it would be six because how would someone know that you have the \_\_\_ which \_\_\_.

[Silence 00:37:25 - 00:37:49].

I would say… \_\_\_ the address. Carphone.com.uk.

[Silence 00:38:00 - 00:38:24].

I think it would be legitimate because \_\_\_[00:38:27 - 00:38:31].

**P304**

P304: I think this is a phishing e-mail.

This is a legit e-mail.

[Background noise, 0:00:19-0:01:02]

Hmm, not sure if legitimate one. It’s just asking for feedback, so I think it’s legitimate.

[Background noise, 0:01:22-0:02:29]

This is a phishing e-mail. The e-mail extension doesn’t have ‘.ac.uk’ for a student account. It’s also asking to fill out your information.

[Background noise, 0:02:46-0:03:09]

This is an Amazon order. I think it’s genuine.

[Background noise, 0:03:19-0:03:45]

This is an e-mail from eBay, invoice notification. It’s not asking you to do anything in particular, just to view your invoice. I think this should be legit.

[Background noise, 0:03:59-0:04:10]

This is a job application form. First, the extension is wrong, no ‘.co.uk’. It also asks you to download a file and double-click on the application form. So this should be phishing.

[Background noise, 0:04:30-0:04:42]

This is a Facebook contact e-mail address notification. Looks legit. It doesn’t ask you to do anything in particular.

[Background noise, 0:04:54-0:05:30]

This is a PayPal receipt for PayPal payments. It doesn’t look…

It looks legit.

This is eBay suspension. Doesn’t look like it’s…

[Background noise, 0:06:00-0:06:54]

This one is legit. It doesn’t ask you to do anything. Just a tracking number.

[Background noise, 0:07:04-0:07:15]

This is an e-mail from I-Offer, for the [history line 0:07:21]. Just sending you your invoice.

[Background noise, 0:07:28-0:08:22]

Hmm, this is an e-mail from PlusNet support. I don’t think this is phishing.

[Background noise, 0:08:28-0:10:34]

This is a transaction from PayPal, [Erin Jones 0:10:39]. Looks legit. Just to view recent transactions. This can’t be fishing, so it’s legit.

[Background noise, 0:10:53-0:11:10]

Usually with phishing, the account’s e-mail extension is wrong.

[Background noise, 0:11:15-0:11:45]

This can’t be phishing. Sending you a new [Uber bill 0:11:49].

[Background noise, 0:11:50-0:15:13]

**P305**

P305: So it looks like a normal NatWest email. It’s to a legitimate email they’ve got. The email address that they’ve sent it from is [somebody@natwest.com](mailto:somebody@natwest.com). That looks quite legitimate. I’ll give that a five. This one looks a bit less legitimate because there’s no, like, proper logo on it, but, again, the email address it’s sent from looks quite plausible. I’m going to rate that one highly as well. I think this one’s less plausible as a legitimate email. The link that they’ve given isn’t really a proper link because it doesn’t end in .com or .co.uk or anything like that.

Also the email address it’s sent from is not really related to the link that’s put in the email itself, so I’m going to rate that one quite low. This one again looks like a proper PayPal email. The only thing that makes me doubt it is the email it’s sent from is e.paypal.co.uk, otherwise that looks good. This one obviously hasn’t got any pictures loaded, which makes you a bit suspicious when that happens sometimes. So I’m going to rate that one somewhere in the middle just to be careful. I think this one’s less likely to be a real email because of the email address it’s sent from, ebayz with a Z and a Y.

So I’m going to rate that one as a phishing email. This one’s quite legit. It’s formatted how you’d expect it to be and the email it’s sent from looks legitimate, direct.gov.uk, so I’m going to say that one’s legit. This one might not be legitimate because it says it’s from TNS and Bath and Dell and the end of the email address it’s sent from looks a bit strange as well. So I’m going to rate that one quite low. This one looks fine apart from the fact it’s from [Koala Craig 0:03:15] not Amazon itself, but otherwise it’s formatted how you’d expect it to be.

At the bottom it says, “Returns are easy, visit our online returns centre,” but ‘online’ is spelt a bit strangely so I’m going to put that somewhere in the middle. I think this one looks legit, the email it’s sent from looks normal. This one, the email it’s sent from matches the company name at the top. I’m going to say that one’s legitimate as well. This one, the email it’s sent from is [battle 0:04:17].com, so I don't really see where that links in to the company it’s meant to be sent from, because that’s [blizzard 0:04:25] not battle.

So I’m going to put that somewhere in the middle. The address it’s sent from looks alright, so I’ll rate that one quite high. I’ll put this one as phishing because the email it’s sent from doesn't really look like it’s got anything to do with the email itself. A similar thing with this one. This one does link quite well, so I’m going to put that one as legitimate. And the opposite again with this, and then the same again here. The content of this email is a bit strange. It’s not something you’d really ask someone. This one’s a bit odd.

This one seems legitimate because the email it’s sent from is the kind of email you get from Google. This along with this. Then again the opposite with this one, regarding the email it’s sent from. This one seems good because of the content and where it’s sent from but it’s not formatted like the other emails so I’m going to put that a bit lower down. It’s definitely phishing because the content... You wouldn’t really email people to ask that. It’s sent from the kind of email you’d expect it to be sent from, but the picture hasn’t loaded makes you doubt it a bit more, but then again that happens.

The link looks like it could be something you’d expect but it’s quite long, so that makes you doubt it a bit more, so I’m going to put that somewhere in the middle. I’m going to put this one quite high because the email it’s sent from, and that matches up with the link they’ve sent in the email. Again, that could be quite legitimate. The link they’ve given is easyroommate.com and that matches up with the email it’s sent from. The fact that CV is lower case, I don't know, it should be uppercase really. The rest of it seems it could be okay.

There isn’t a space between 40 and hours, you think they would have noticed those things if it was from a proper company. It’s from a Yahoo email, which, again, you wouldn't really expect them to use, so that one quite low. The links in the email look like they could be from Facebook. Again, there aren’t any images or formatting to it, which you’d expect from Facebook, so I’m going to put that somewhere in the middle. This one does have the formatting. The email it’s sent from matches up with the footer at the bottom of the page.

That one’s quite high. Again, the link, ioffer.com and the ending of the email, ioffer, matches up with the email that it’s sent from. So I’m going to put that one quite high. It’s got a dodgy attachment which you wouldn't expect from a mobile bill. So that looks a bit dodgy. Then the email it’s sent from is virginmobile.com. That could be what you’d expect. I’m going to put that one quite low just because of the attachment. PayPal matches up, it looks like it should. It’s sent from PayPal email. I’m going to put that one legitimate.

The link in the email does match up to the email that it’s sent from. So I’m going to put that one relatively high. Again, the link doesn’t match up with the email it’s sent from, because that’s a gov.uk and the email it’s sent from is .co.uk. So that makes it a bit suspicious. So I’m going to rate that one quite low because you’ve got to fill out the form to put information in. That’s where they can scam you.

It’s sent from Lancaster.ac.uk. All the links in it look like they could be real links. It’s the kind of email you get, so that one’s legitimate.

**P306**

P306: Okay, the first email seems okay on first sight. It's from Adobe; it's got the Adobe signature. Well, you know, logo.

Okay, it's not asking for them to give a password; it says it's reset. It's an external link; the external link has Adobe in it.

It's to a specific user, rather than to several. It also gives a specific date, so you could presumably Google that to make sure that there was any evidence online. I'm going to say that's very probably legitimate.

Okay, again, this one at first glance doesn't look awful. From Priority Mail posting service. That's not the same as FedEx. DTF at Fort Wayne; that starts to look a bit more dodgy, because you would expect FedEx to have specific FedEx email accounts. It just gives a tracking number, rather than just saying "your order." "Your parcel has arrived at the post office at December 7." That seems a bit iffy; bad grammar with the full stops. "Our postmaster was unable to deliver the parcel…"

\_\_\_[0:02:08] they're not actually asking for any emails or anything here, or passwords. I assume you could print this off and just go to it, so I think that's rubbish. Probably legitimate, but I'm not at all sure. Waste of time if it's not legitimate anyway.

Okay, again, so far the "from" looks okay. Subject looks okay. Sending the same email twice \_\_\_[0:02:53]; that's a little strange. Image doesn't show up. "Even if someone else sent you this email, change the password." Okay, that looks very strange; it's a bit long weird link. It gives superfluous IP address information. Nobody identifies anyone from their IP address, so I think that is probably phishing.

[Carl O'Craig 0:03:29]. Again, we have official Amazon-looking information, but from [Carl O'Craig] seems a bit odd again. I might expect generic Amazon account. Otherwise it looks legitimate, so I think overall that's probably fine.

Okay, well this looks like a load of definitely phishing. From Gucci, \_\_\_[0:04:19] and Rolex. Get your luxury... The "from" looks dodgy, the subject looks dodgy, so it's obviously unsolicited, and a couple of links which I'm certain will give me all kinds of viruses, so it's definitely phishing.

"HR Recruitment department, new applicant." I suppose it's not unheard of for HR departments to have Yahoo accounts, but "HR department 33,433" seems a bit iffy. It gives out strange details as well. If you'd applied for a job, I'd beware of them, but... "Click here to download the application form" is very dodgy. They would either send it as an attachment – you know, as a PDF or something less suspicious than a link maybe – so I think that's probably, but not definitely, phishing.

Yes, this one from \_\_\_[0:05:58] seems fine. It's got an official-looking email, it's not asking for any addresses. It would probably be easy enough to check up. If that's a phishing scam it deserves to con me.

"Easy Roommates"; a little bit strange. If I assume that somebody had signed up to it, it does have a website and the email address to a specific person. "Easy Roommate" is in the URL. I think it's a poor-quality email, but probably a legitimate poor-quality email.

Okay, HSBC. Okay, so this one looks more dodgy. Yes, info and subject looks okay, but "the business account has been blocked for receiving payments." They wouldn't disable an account just for a security issue; they would send a much more personal account, so that is definitely phishing. Good phishing, but phishing.

"Password will expire in three days; click here to validate your email." That's not how companies work, so that one's definitely phishing.

Okay, so this one is very poor. Initially subject: "Sad news" from this particular man. If you knew him, you wouldn't say "Sad news." "Me!" That's weird. He's obviously just soliciting from anywhere. No normal person goes, "I've had a hard time with the police, so I'm going to send emails to strangers", so that is the most obvious piece of phishing you'll ever see.

eBay one doesn't look too bad. I'm not sure "Ebayz.com" would be correct for the address, but it seems to have logos and so attached. I don't know what the text is yet though.

Okay, so it's just saying it's suspending their account; it hasn't given any reason why. It just wants to update their personal records, so this is definitely going to be phishing.

Plusnet; well, it'll be phishing if it's any good, probably. "Dear Mr Jones"; it gives an account name. Yes, this one's harder to tell. "Plusnet Protect, with McAfee." Without the use of any official logos and so on… I think this is relatively poor; this is either quite good phishing, or really poor customer service. Again, it's Plusnet; it could be either, but I think it's just about phishing.

Okay, Student finance. Again, nothing obviously wrong in the "from" dates. It seems to have an official-looking logo. Okay, so poor grammar, "We require all students…"; commas instead of full stops. Okay, so no, that's definitely phishing again.

"Dear candidate"; always the first sign that something's wrong. Okay, so some barely comprehensible URLs, organisations listed as "Send"; "seek a logical assistant." A lot of this is very sparse information; there's not a lot to go on, so I think that is very probably, if not definitely, phishing.

NatWest, but from a very weird email address. "Your online account will expire today." Bank accounts don't tend to expire. And they certainly don't tell you, "you've only got 24 hours or we'll disable it", so that is phishing all day long.

"\_\_\_[0:12:28] received payment." "Googlebox UK has received your payment." This one doesn't look too bad. It's got proper URLs, it probably is a genuine statement, and presumably you would know whether or not you'd just ordered that specific thing, so very probably, but not definitely, legitimate.

Dropbox: again, decent-looking email address, proper logo. "Verify your email address before you share photos" makes sense. Has a little copyright and watermark in the bottom. I think that's very probably legitimate.

PayPal; again, formal-looking thing. Decent email address from the "from". Just gives a login, so it's not asking for email addresses or anything at this point, so it looks okay.

Student Loans Company from Direct Gov. "Be websafe \_\_\_[0:13:51]." This sounds like a wonderful piece of phishing. "The following activity is going on in your student loan account. \_\_\_ update your information securely", but that URL is nothing to do with student…

**P307**

P307: Dear candidate, job alerts. A job which matches your alert criteria has been published on our website, please click the following link. Paste it into your browser and search for the vacancy references list below. It has the official title and you can cancel your subscription. I would say it's probably legitimate.

Usually they will just send you a list of jobs instead of asking you to click on the link so yes, I will chose five. Your password will expire in three days, please click here to validate your email, thanks, system, administrator. The tone is a little bit too casual but it didn't ask for your password, it just asked you to validate your email so maybe I'll choose three.

NatWest with its official title. Your latest statement is available online. Okay, yes, I think it's legitimate because I usually receive emails from my bank like this, Barclays. We have detected unusual activity in your account, this may be \_\_\_[0:02:44] we have decide to limit your account until you complete the steps to have full access.

I would say I think it is legitimate but I don't know, the email address looks reasonable. I don't know. I think it's just conceivable that the bank will send an email like this. Well true, it doesn't show your name. It looks like an email that's supposed to protect you, I don't know. I'll choose four.

eBay suspension. Our email address is from eBay. Deadline is the 10th September and the email address they have sent is probably an eBay - the website they've sent is from eBay so I would say it is five. They are likely to be legitimate.

\_\_\_[0:05:32] user name - thanks for choosing Plusnet. It looks like a legitimate - yes, the email address is from Plusnet. It has different addresses for you to get help. Yes, I would say it's definitely a legitimate - but it asks you to download something. User name, password, follow the on screen download the instructions. I'll choose five then.

Please do not reply, follow the link below into your account to reply. Yes, it does look like a legitimate email. It doesn't ask for any of your personal information. I think I have probably seen emails like this, definitely legitimate.

Dear guest user, Cocoa Box UK has received your payment regarding the item. View the status of your purchase. I think it is legitimate. Yes, I don't know what [I offer 0:08:02] is but I can imagine a confirmation or payment received email looking like this so I'd say definitely legitimate.

From Amazon, thank you for shopping with us. It gives you the delivery detail. It doesn't ask you to do anything. It just confirms that it's shipped so I would say it's legitimate. It's a reply to your email I guess so I would say it's legitimate.

Directgov public service, all in one place. More students to update their account information to ensure you receive a scheduled payment and avoid a missed payment. It does relate to money. I've never seen - well if it asks you to validate your information instead of giving them your information, maybe it is legitimate but I've never seen directgov - I've never seen this website, I don't know what they do. I'll choose four.

Hi Helen, someone recently tried to use an application to sign into your Google account. I think it does look legitimate because it is a Google email address and it gives you the IP address and other things. It looks like they're doing a pretty responsible job instead of just trying to get your money or information so I would say it's definitely legitimate.

Visa. Just the format of the email looks professional. Credit card has been suspended, we need you to update your information to lift the suspension. I don't know what they want you to do but I think - forced to suspend your credit card permanently. I'd say it's legitimate, it just looks, the tone and the format of the email just looks like something Visa can do.

This message for all students receiving grants and loans for students, known company, we have detected fraudulent email, fill out your information securely. I'm not even sure if you are secure. Also, the website you've sent has nothing to do with an official organisation so I would say it's probably phishing. Yes, I would say it's definitely phishing unless someone tells me otherwise.

Dear applicant, thank you for your interest. We have carefully reviewed your CV and you have made the shortlist. It's from the HR recruitment department but the email address is from Yahoo and I don't know. If you've made the shortlist why would you still need to fill in an application form? I don't know, I would say it's probably phishing. I don't even know what company you're recruiting for. Okay, so I don't even know why do you need me to click here. It's definitely phishing, yes.

\_\_\_[0:14:16]. To read your updated terms, it looks like legitimate because it doesn't ask anything from you and yes, the email address looks reliable. Yes, I would say it's definitely legitimate and it even has the real address of the company so I would say it's definitely legitimate. I can't see it, it's too small. Okay, yes, it has the case number so it looks like it's replying to you. Yes, so it asks you for a survey, for some feedback I guess so I would say it's definitely legitimate, yes.

Dropbox. Okay, it asks you to verify your email address. Yes, I think it's legitimate. I've seen emails like this before. Your card is about to expire, from PayPal. It asks you to update your card. Is it truly from PayPal, yes it is. The address is from PayPal. Yes, I think it's legitimate, yes.

A new contact email address to confirm your contact email address, follow the link below, from Facebook. What is a contact email address? Oh, you're own email address that other people can contact you? If you're from Facebook, why don't you have - you should have a title as Facebook. Please disregard this email. Take a look at Facebook Help if you have any questions. It doesn't ask you for anything so I would say it's four.

FedEx. It has your track number but the email address doesn't make any sense. It's not from FedEx or anything so I would say it's three, probably phishing. The bill for your Virgin Media Mobile, the balance is this. Picking up emails from this address so if you'd like to email us back head over to our website to send as an email, Virgin Media Team. Again, it doesn't have a title but the email address is thanks@virginmobile.com.

It doesn't look like an email address that would send out mobile bills so I would say it's probably phishing. \_\_\_[0:19:00], it doesn't ask you for anything. To prevent unauthorised access to your account we have reset your password. Would they actually reset your password?

Any website where you use the same user ID or password in addition, please be on the lookout for suspicious emails. I would say it's legitimate even though I don't know what this email is actually doing, especially if they can actually reset your password without letting you know. So I'd choose four.

NatWest. One thing is the email address doesn't look like having any relationship with NatWest so I would say it's two. eBay. It's from eBay sending you your invoice. It's not that much money. You can only view your invoice, it doesn't ask you to send them money so I would say it's definitely legitimate.

Mr. Gary Cooper, why would you choose - you don't even know my name, why would you choose me as your executor? This is definitely phishing. It asks you to give him the money so I would say it's definitely phishing. Congratulations, you just purchased an item from Cocoa Box. I think it's legitimate even though the pictures are all blocked.

PayPal invoice receipt. It doesn't ask you to do anything so yes, I would say it is legitimate. Your personal Diablo III. I don't know what this asks you to do. What's Diablo III? This tone saying, "You must work with us otherwise we will freeze your account," I don't know, it looks like a game. I would choose four.

Yes, the email address is from NUS Extra and yes, it does look like an email that you would get when you want to reset a password so I would say it's definitely legitimate. HSBC. Yes, the email address is from HSBC as well. I would say it's probably legitimate. It just asks you to verify your account so I think it's legitimate. PayPal. Log in to view your recent transaction.

The email address is PayPal and the format looks like what PayPal would send. Yes. I was just looking at the bottom where it says, "How do I know this is not a spoof email? Spoof emails tend to have generic greetings," which is true, yes. I would say definitely legitimate.

Dear Pleasure Beach visitor. It asks you for a survey. I'm not going to read it through. Yes, I think it is legitimate. The email address is for surveys, yes, five. DVLA. The email address does look like it's from DVLA. It asks you to verify your licence. I don't think they would have you lose your driver licence just because you didn't verify your email, I don't know. It doesn't even have a title. It doesn't even address you or give you their names. I would say it's probably phishing.

I think the DVLA's logo is green speaking of this but it does sound like a serious matter. Anyway, I choose two. It asks you for feedback on the university and its admission process so I think it is legitimate. It doesn't ask you for other things and the email address is from Lancaster. Yes, okay. It is even from this person so I would say it's definitely legitimate.

**P308**

P308: So, I think this email is definitely phishing, because if this man wants to give his fortune to charity then why would he write an email to you to just tell, “I’m giving everything to you,” to a complete stranger? Also, “I chose you as a trustworthy person,” but you are a stranger to him, so it doesn’t make sense. So, definitely phishing.

So, I think this email is not trustworthy, because the dates are incongruent. So it was sent on the 8th October, and it says the online account expires on the 3rd June, so it should be already expired. So, phishing.

So, I’m not entirely sure about this email. It looks strange because usually emails from banks, they don’t have this very long copied and pasted link. I don’t know. I would have a look at my account directly without going through this link, so I would say two.

So, I don’t know much about eBay because I’ve never used it, but what makes me think about this email is the email address of the sender, which is eBayz with a ‘Z’, so it’s quite suspicious, so I would say phishing, again.

I would say that this email is legitimate. Actually, maybe I’m wrong, but they don’t ask you to do anything, so it just… Okay, I would say legitimate.

Well, I think this email is legitimate because they are just informing about the new conditions. So, hmm… I can’t see anything suspicious.

I’m again, not very familiar with Amazon, but I think it’s quite normal for them to send an email about the shipment of the purchase, so if the person who would receive this email actually bought the [tepee 0:12:05] then no problem, I think it’s legitimate.

I don’t know. I have no idea of how this student finance works, but it seems okay to validate the information, so I would say maybe four.

I don’t know exactly what it is, but this makes me think definitely phishing. Well… I don’t know what Diablo [30 0:16:08] is, but it looks [like] spam, or something that might catch you a virus. I wouldn’t open that link.

That’s definitely phishing. I would never give money to a stranger who is asking for money through the internet. Also, it doesn’t make much sense for him to be able to write an email if everything was stolen, mobile phones etc. So definitely phishing.

So, I think this is quite trustworthy, because it’s this service, Verified by Visa, and… Yes. I don’t know. It’s maybe… But it’s also quite strange for them to ask for this information update. I don’t know, but this is becoming confusing, so I would say legitimate.

If the person has subscribed to have these email job alerts, then I think it’s fine to click on the link and have a look. So I’d say yes, legitimate.

No, this is definitely phishing, \_\_\_[0:21:12]. So this… Nobody is ever giving anything to anyone, especially through the internet. You are not the lucky one, so phishing, definitely.

I think this is quite legitimate. I don’t know, the layout looks good and the email of the sending person looks okay. Everything looks… I don’t know, trustworthy. It’s like, from the bank. I would say legitimate.

So, I’ve received a sort of email like that before when I was logging in from other computers, so I think it’s quite normal, and I would say okay, it’s legitimate.

I think it’s okay, it’s just Dropbox… It’s normal for them to ask you to verify your email address, so if you’ve just registered on Dropbox then you know it’s kind of normal. Yes. Legitimate. Doesn’t make much sense.

So again, I’m not very… It’s hard to say. I don’t use eBay at all, so I don’t know how it works, if it’s fine for them to ask for money for the seller account, I guess so. But anyway, I think if you go on the site then you… I mean, the real eBay site, then you can have a look whether it’s true or not that you have to pay for your account. But it looks legitimate from the… Yes, if you have the invoice number and… I don’t know, I can’t even read it very well because it’s so small. Yes, I would say legitimate.

That’s hard. I have no idea about this iOffer, I would say okay, if the person bought that, that \_\_\_[0:29:47] then it’s fine to see the status of the purchase. So, legitimate.

So what makes me think is this sentence that, “The security software will be uninstalled automatically for you,” I wouldn’t trust something that uninstalled my security software, so I would say no. I wouldn’t download this.

I think this is legitimate. It’s just a PayPal service, it’s informing you of your transaction, so it looks fine.

Hmm. I would say this is legitimate. It looks written by a real person. The only thing is that maybe the email address of the sending person doesn’t look very real, but I would say legitimate.

So this email looks legitimate to me. The dates are quite coherent. I don’t know, maybe- The only thing is this \_\_\_[0:36:45], I don’t know, it sounds a bit strange, but I would say legitimate.

So this email… No, maybe… So it sounds a bit strange that they have this parcel arrive on the 7th December and they sent the email on the 18th December, like more than 10 days later, it looks very suspicious so I would say- And, yes. I would say two.

I would say five.

So again, I have no idea of what this iOffer is, and Google Box UK, but it looks okay. I mean… Yes, if she just bought this then it’s fine to receive the invoice. I’m taking so long.

I think this looks quite okay. They even tell you, “Beware of scams,” so, “Do not send money via Western Union,” so it’s fine.

I have no idea. I would say three. I have no idea of this student finance should look, so I can’t say anything about this.

I would say this is legitimate, it looks fine and okay.

I would say this is phishing, because… I don’t know. It doesn’t look very trustworthy from the email address.

This is just paper and the email looks fine, I think. The graphics and the layout look okay.

This is \_\_\_[0:45:17] but here the graphics don’t look very nice. And also, “We notice that your Visa Delta Electron ending in 1234 is about to expire,” 1234, I don’t know, phishing.

This looks [like] phishing.

So from Facebook. The email address doesn’t look trustworthy, so I would say three.

Blackpool Pleasure Beach. I think this is legitimate; it’s just a survey. Yes.

Wow, this is absolutely crazy, how can they take your driving licence? So no, I would say phishing.

Okay, these look legitimate. It’s just a survey from the university. Okay. That’s fine. The dates are coherent, so they give you some time to complete the survey, and it’s fine.

**P309**

P309 It looks pretty real, doesn’t it, the [dialect 0:00:03].

[Break in Audio 00:00:03 - 0:00:17]

The fact it’s from v.net.com, definitely phishing. That’s what I looked at, v.net. What they hell?

Paypal. Okay, it looks as if it’s from Paypal. That looks pretty good. It says, “[Helen Jones].” It’s got a date, time and date, and then it wants you to log in. It’s not saying, “What is your password?” I’ll say five, I’m scared to put six.

That’s the HR department 3343 for Yahoo. You made the shortlist. Why would you be emailing from Yahoo? Please click here, no, it looks unprofessional. Who would put all those weird kinds of things in? Definitely phishing.

\_\_\_[0:01:23] looks weird. I don’t know. I just thought there would be more to it although it is from HSBC Business. Though wouldn’t it be from HSBC.co.uk not HSBC-Business? I’ll put a two. I don’t think.

What the hell? \_\_\_[0:01:49] email address \_\_\_ Kent. Please proceed to this link. Okay, well both versions are the same. It’s a bit weird. I’ve never noticed that before. I’ll put a three. I think it’s a bit weird. It looks weird.

Sanex.

[Break in Audio 0:02:21 - 0:02:52]

How weird. Suggesting that Helen doesn’t know [Phillipe]. What a weird email. You wouldn’t send an email. You’d be ringing people, wouldn’t you? Ring him up for God’s sake. Phishing. I would be like, “What?”

[Break in Audio 0:03:11 - 0:03:25]

I mean, who sends these real kinds of emails? No one. Phishing. I’m not, phishing, like, what the hell?

Click here. No, I’m not clicking there.

Bloody hell. What the hell? £359 on a bloody TV. Bloody PhD student. I love that it is always linked to a Helen Jones 1989. If that’s your name, hilarious.

That’s legitimate. You wouldn’t know if it was or not because you will have ordered it. Dear Miss Jones, it could be Dr Jones.

I’m pretty sure I’ve seen one of those emails before, that looks like that. I guess you would know if you downloaded McFly, McAfee because you would have paid for it. I’ll give a five. If you received that email randomly then probably not but if you would have ordered it then yes.

HSB looks right. The email address looks alright. Yes. I think that’s fine. Give it a five though. Never can be sure of them, yes?

Dear Valued Customer, brilliant. They send to everyone. It would have come from like a \_\_\_[0:05:29], no. Phishing. Awful.

Facebookmail.com. What the hell? No, I don’t think that’s right. That’s weird. No, it’s weird.

Just looks weird. Trying to sell your, what the hell’s that, in the, look at that, in the bloody internet link as well in the title. No, I’m not having that. Awful.

Your account would expire for [Dan Keyore 0:06:09].com. No. Shut up.

What a date. Finance with two e’s. It looks pretty good though but two e’s. Obviously no way. Definitely phishing. Looks pretty good though.

Really no idea. I think it’s okay. It’s not saying, “Give us your details,” but I guess it could be asking.

We’re notified by visa.com, I guess that could be true. It’s weird with all the hyphens. I’ll give it a three.

Passport reset. Yes, I guess that could be true. Okay.

From thanks at Virgin Mobile. Yes, that’s fine. It’s saying, “Email on my website.” You should know if it’s true or not.

Easyroom. Yes, that looks. It’s saying, “Look at website.” Yes, it looks fine.

Yes. Weird email, via iPhone. It’s a weird email. I’ll give it four.

It’s got your name and obviously you know the card number so yes, I think that’s fine. You know [particularly well 0:08:16] your own stuff.

I hate those emails. No. Definitely phishing. From randomemailnet.com. No way.

I’ve seen them before. I know it’s a weird email address. No. Why would someone have sent that? It’s the email address, it just doesn’t look right.

Yes, that looks fine. That’s fine.

It’s that weird email. Why would you have it via, like? Four, I’d say.

Fedex. Again, weird email. [Ford Wayne 0:09:09]. No. Phishing. No, I’m not having that.

EBay member. Ebays, no, awful. Poor Helen, getting all these emails. It’s all those mucky sites she likes to sign up to.

Could be. I guess you would know if you signed up for that website.

No. From the mindface.com.

Yes, that looks okay. That looks okay.

Dropbox. I know Dropbox. Yes. I’ve received emails before because, again, you requested it.

Dear Pleasure Beach. Awful. Survey, I’d guess you would know if you had been Pleasure Beach, wouldn’t you? If you’d been there recently you would be like, ‘Okay.” Whereas if I received that, I’ve never been there so I’d be like, “What the..?”

From info@dft. But you’ll have DVLA. Definitely phishing.

That looks cool. That’s fine. I’d say, “Yes.” I don’t know who Malcolm is now. Interesting surname, isn’t it?

**P310**

P310: Okay, first email.

[Background noise 00:00:10 – 00:00:30]

Right, for starters, the email’s addressed to “Dear Valued Customer.” You’d have thought they’d had it actually addressed to the person by their surname.

[Background noise 00:00:52 – 00:01:35]

The spelling seems to be quite good, which is not indicative of a phishing scam. It’s also got quite a decent Visa header. Obviously, that can be faked. Right, I think due to the fact they’ve got “Dear Valued Customer” in there, I think it’s definitely phishing.

Okay, the second one.

[Background noise 00:02:19 – 00:03:19]

It looks pretty good, this one. I’m not sure though if ‘interruptions’ isn’t spelt incorrectly. That’s the only thing I’m thinking of at the moment. It’s addressed to “Helen”.

[Background noise 00:03:50 – 00:04:12]

I want to say that that could be legitimate.

Right, the third one.

[Background noise 00:04:26 – 00:05:03]

There’s no personal information at the start, there’s no “Dear” anyone, or anything. The link looks a bit strange. But I’m not sure, again, so I’m going to go with ‘four’ because it looks okay.

[Background noise 00:05:28 – 00:06:15]

Shipping address is unconfirmed on this one.

[Background noise 00:06:18 – 00:06:37]

Again, the spelling’s pretty good.

[Background noise 00:06:42 – 00:07:09]

I think that looks pretty legitimate.

[Background noise 00:07:13 – 00:08:22]

It’s a difficult one.

[Background noise 00:08:24 – 00:08:51]

But again, it’s saying that something needs to be done urgently, which is suspicious, because it’s trying to get you to act urgently, which is a general trait of phishing scam, but I’m going to say this is probably a phishing scam. ‘Two’.

[Background noise 00:09:23 – 00:09:50]

There’s a spelling mistake. “If you need to return an good from this shipment,” \_\_\_. Should be, “a good.”

[Background noise 00:10:02 – 00:10:14]

That makes me think it’s a phishing scam.

[Background noise 00:10:21 – 00:11:04]

Again, “An attempted error logins was detected.” The grammar isn’t great. It’s also, again, asking you to do something really urgently. Generally, banks wouldn’t send you something like that with a link. But I think, again, that’s a phishing scam.

NatWest… I think this is probably a phishing scam, again. It starts with “Hi…” I think if it was really from NatWest it would be a lot more formal than that.

[Background noise 00:12:28 – 00:12:53]

There are a lot of links in it, though, which makes it look a bit more credible.

[Background noise 00:12:59 – 00:13:35]

I’m not sure, because it looks like quite a legitimate email. But again, I think it’s just a bit too informal, so I’m putting a ‘two’.

[Background noise00:13:54 – 00:15:22]

I’m not too sure about the next one, but I think it’s probably a scam. I’m going to go for a ‘three’.

[Background noise 00:15:34 – 00:16:12]

I’m not sure about this FedEx one. The header looks good on it, makes it look quite legitimate. “Dear Customer” is kind of informal, but could be used, I guess. A bit strange to have to download a postal receipt. You don’t normally have to do that kind of thing, so I think it’s, again, probably a phishing scam.

[Background noise 00:16:51 – 00:17:32]

This is one from \_\_\_. Again, it greets the person with their name, which seems pretty legitimate. The header’s pretty legitimate. I can’t see any spelling mistakes. The address looks legitimate. It’s not really asking for money or anything, so I think that one’s a legitimate one.

[Background noise 00:18:17 – 00:18:40]

The link on this one just looks absolutely ridiculous. It just seems far too long, so I’d say that’s definitely a phishing scam.

This next one, Gucci, Cartier, Rolex. I think the address is just a normal email address: “someone@[ycos l00:19:23] .com]”, and the way it’s worded and put together, I think it’s definitely a phishing scam.

I don’t like the look of the address at the top, the web address. The header looks very good. There’s a sense of urgency to it, the email.

[Background noise 00:20:03 – 00:20:16]

I think that’s definitely phishing, although the header looks good.

[Background noise 00:20:23 – 00:20:37]

The web address is a little suspicious. The header looks good, the Barclays header, but it could be a bit faded. “Dear Barclays account holder” is a bit too… It’s not personal enough to the person that holds the account.

[Background noise 00:21:07 – 00:21:22]

I doubt a bank like Barclays would send you an email like this to verify your account. So, again, I think it’s a phishing scam.

Web address here looks okay. It’s addressed quite personally. You’d expect there to maybe be a header from eBay or something.

[Background noise 0:22:15 – 00:22:35]

There’s a lot of stuff like “Learn more to protect yourself from spoof emails”. A lot of links there which you would think are legitimate. I’ll give that one a ‘four’. It looks quite good, but I’m not sure.

The web address looks pretty good on this one. “Valued customer” is the greeting. Spelling looks all right.

[Background noise 00:23:47 – 00:24:12]

It’s only asking you to do a survey. That one’s, again, probably good, so I’ll give it a ‘five’.

[Background noise 00:24:27 – 00:24:39]

Header on this one looks good. The email address looks good.

[Background noise 00:24:45 – 00:25:33]

The link looks okay. I don’t know, it’s probably legitimate, so I’ll give it a ‘five’.

[Background noise 00:25:47 – 00:26:01]

This one looks very suspicious. I think this is definitely a phishing scam. I think I’d be ringing the family first of all, but I definitely think it’s a phishing scam. It’s the most obvious one so far.

[Background noise 00:26:28 – 00:26:48]

First off, the grammar on this one is not very good. It seems to be from a complete stranger as well. It seems very far-fetched. I think it’s definitely a phishing scam.

[Background noise 00:27:22 – 00:27:36]

Spelling looks fine on this one.

[Background noise 00:27:42 – 00:28:00]

I think this one could be okay. I’ll give it a ‘five’.

[Background noise 00:28:08 – 00:28:38]

Yes, I’m not sure about the email address, it looks a bit dodgy on this one.

[Background noise 00:28:45 – 00:29:04]

“\_\_\_, the job we offer is a fulltime and part-time positions with a flexible schedule.” On the basis of that I’d be suspicious. I’ll put a ‘two’. I don’t like the address at the top, either. I’m going to change that to a ‘one’, I think it’s definitely a phishing scam.

[Background noise 00:29:34 – 00:30:20]

I think this one looks pretty legitimate. So, I’ll go for a ‘five’. It’s got a good header, spelling’s right.

[Background noise 00:30:53 – 00:31:22]

Hmm. I’m not sure about the attachment, it doesn’t look right on this one. Apart from that, it looks pretty good, pretty good email. I’d say that’s, because of the attachment, I’ll go for a ‘three’.

This looks like a very legitimate one, the headers and everything, even down to the advert on it. If it is a scam, it’s a very, very elaborate one, and the spelling’s good, it’s presented really well. So…

[Background noise 00:32:22 – 00:32:55]

I’m not sure the description of… How I know this is not a phishing email’s that good, that it gives… I don’t think I’ve ever seen a phishing email that’s this sophisticated, so I’m going to maybe fall for it and go for a ‘six’.

[Background noise 00:33:17 – 00:33:33]

The links, link in this looks okay, but I’m not sure about the address. Spelling’s all right. I think if it was something from Facebook it would have more of a professional look, have more logos and things. So, I’m going to say it’s probably phishing, ‘two’.

[Background noise 00:34:00 – 00:34:18]

The link doesn’t really seem to have anything to do with what the email’s about with this one, so I think it’s definitely a phishing scam.

Ms. Jones is… Yes, that’s probably legitimate. The address looks okay. There are no spelling mistakes. I think that’s a legitimate one.

Jesus…

[Background noise 00:35:18 – 00:36:25]

There’s a message at the bottom of this one saying “Beware of scams. Don’t send money via Western Union.” To make it try to look more legitimate. The link’s quite long. It’s not really asking for any money or anything. I think it’s possibly a phishing scam; I’ll go for a ‘three’.

It’s got a decent address, it’s got a decent header. I think that one seems okay. We’ll give it a ‘five’.

[Background noise 00:37:32 – 00:38:50]

This one’s got a good, it’s got quite a good logo on it. I don’t really like the email address, though: “ebays.com”. So, I’m going to say that one’s a phishing scam.

This one’s got a very fancy header. The address looks okay.

[Background noise 00:38:44 – 00:38:53]

There are some spelling mistakes, though. Some grammar errors. Starting with the “We”, which is capitalised for some reason, and “We require all student…” instead of “students”, “… to update their account information.” For that reason I’m going to say it’s a phishing scam, ‘one’.

[Background noise 00:39:30 – 00:39:47]

I’ll give this next one a ‘three’. “Dear Guest User” is a bit strange.

There’s no subject on this next one, which is a little strange. The address, \_\_\_[00:40:24], doesn’t really have anything to do with Blackpool, but it could just be a survey provider, I guess.

[Background noise 00:40:37 – 00:40:59]

I think that one could be legitimate, I’ll go for a ‘five’.

[Background noise 00:41:05 – 00:41:20]

There’s a nice header. Not sure about the address.

[Background noise 00:41:33 – 00:41:46]

And there are some spelling errors: “Drivers that refuses to upgrade”. Yes, it doesn’t really foil well together at all, the text. So, I’m going to say that’s definitely phishing.

[Background noise 00:41:59 – 00:42:13]

The email address looks okay. You could well be referred to as “Dear Student”.

[Background noise 00:42:24 – 00:42:43]

It looks pretty legitimate, this one. I think that one’s definitely legitimate.

**P311**

P311: Okay, the first e-mail is from I-Offer.

[Break in conversation, 0:00:16-0:00:40]

Well, I think the first e-mail is a phishing one, because I received a similar one before. It said I purchased something on a website, and it asked me. But I didn’t order anything from that website. And then the e-mail said you can click a link to cancel the transaction, and I clicked it.

Then it proved that it was, like, the wrong website and it downloaded something bad to my laptop, so I think this one, the first one, is the phishing e-mail.

Yes, okay, the next one, from Visa. ‘Has been suspended, and…’

I think this one is the same as the previous one. It asks you to click a link, and I don’t think this page looks very formal. It says, ‘Verified by Visa.com.’

I think this one is also a phishing one.

Okay. ‘Important: password reset.’

[Break in conversation, 0:02:08-0:02:46]

Well, this Adobe one looks quite alright. But it also asks me to click a link.

But it didn’t say anything about money or my bank account, so this one maybe I’ll give it a ‘Four’. I’m not sure about this one.

\_\_\_[0:03:27-0:03:40].

Well, first of all, the connecting website, the link it gives looks not like a legal link. It has so many symbols, numbers, letters. And also it said that please, the internet…

I don’t think it’s a legal e-mail. I’ll give a ‘Two’. I think it’s a phishing one.

Okay, the Barclays. Well, this one, I think, is a phishing one, because I’ve also got a bank account at Barclays, and every time I received their e-mails, my name is always shown on the e-mail. But this one is just, ‘Dear Barclays Account Holder.’ So I think it’s a phishing e-mail to everyone. So it’s a phishing one, I think.

Oh. The link looks so weird. It’s so long and, like, I think it’s a phishing one. ‘Your password changed.’ ‘Check your password.’ ‘e-mails…”

Yes, every time I receive an e-mail and it says, ‘Click here and you can get a prize,’ ‘You can get something good,’ I just refuse to do that. Because I think it’s a phishing e-mail, and if I clicked it, they would download something bad to my laptop.

I don’t think I can just simply click a link and then I get a luxury watch. So it’s a phishing one.

‘Dear Candidate…’

First of all, the link showing the website is not so formal, like so legal. And then secondly, I think because every time you register to, like, a recruitment website, it asks for your name. But this one, it just says, ‘Dear Candidate.’ So I think it’s also a phishing e-mail to everyone those people want to target at.

[Break in conversation, 0:07:10-0:07:30]

HSBC. \_\_\_[0:07:33].

[Break in conversation, 0:07:35-0:08:07]

I’m not sure about this one, but I think because the e-mail is from a bank, so when I open a bank account, the bank has my detailed personal information.

I think when they e-mail me, they will declare the personal information they have, but this e-mail, it said nothing about me. It didn’t say, ‘Dear my name’ and my personal information, like my card number, on the e-mail.

It didn’t show anything very detailed, so I think it’s a phishing e-mail.

[Break in conversation, 0:09:04-0:09:41]

Well, this one, it looks weird, because I don’t think anyone is lucky enough to get money from a person with hand cancer. It’s just like, they want to get money from you but not give you money, so it’s a phishing e-mail.

I received this kind of e-mail before.

[Break in conversation, 0:10:18-0:10:29]

Well, this one from eBay, I think this is a legal e-mail, because it showed my name on it, Helen’s name on it. And gave very detailed information. And also, the e-mail address is, ‘Barry@ebay.co.uk’. I think it’s a legal one. Finally I got legal information.

‘Log in now.’ Yes, this one also, this is from PayPal, because it has my name, my e-mail address and also this page, it looks like a legal and correct website, so I think it’s a legal one.

[Break in conversation, 0:11:39-0:12:06]

Well, this one because the e-mail was sent to Helen’s Lancaster University e-mail address, so I think as long as it has Helen’s uni e-mail, it should have Helen’s name on the e-mail, but it didn’t. So I think this one is not a legal one. But I’m not sure. I’ll give a ‘Three’ for it.

Well, this one, this one is not correct, because, I’m not sure.

[Break in conversation, 0:13:03-0:13:19]

Not sure.

[Break in conversation, 0:13:21-0:13:48]

Well, this one, it asks me to copy and paste a link, but I didn’t see anything related to the student loan on that link. It’s ‘Mine Fees’. It doesn’t look like a formal website. So I think it’s a phishing one.

[Break in conversation, 0:14:15-0:14:51]

Hmm. This e-mail is from NatWest, the bank, and it also asks me to click a link, but the link is very formal, for me, I think. It’s ‘Natwest.com/yourstatement.’ I think this one is definitely a legal one.

[Break in conversation, 0:15:17-0:15:48]

This e-mail is from Plusnet Support, and I think this one is a legal one, because the link it gives, it gives you the link of the website, the telephone numbers, and I think all the information from this e-mail, they match with each other. So I think this one is not a phishing one.

[Break in conversation, 0:16:21-0:16:51]

Well, the subject of the e-mail is, ‘You have mail.’ It doesn’t look very formal to me. And also, it highlights ‘Please do not reply to this e-mail, follow the link below.’ And the link is something wrong, to me, with so many numbers, so many symbols. I think this one is maybe a phishing one. Maybe.

Dropbox. \_\_\_[0:17:32] Issue \_\_\_. I think this one is a legal one, because it’s from ‘Noreply.dropbox.com’. It’s a legal e-mail address. It’s a formal, official e-mail address. And look at this one, I can choose this. Six…

[Break in conversation, 0:18:04-0:18:30]

Oh, this one, it says that the FedEx delivers some parcel to Helen, but the e-mail is from ‘DTF.193.something’. So I don’t think the e-mail…

The information on the e-mail didn’t match the e-mail address, where it is from. So I think this one is a phishing one.

[Break in conversation, 0:19:04-0:19:35]

Well, since the man has Helen’s e-mail address, but in the e-mail he didn’t mention Helen’s name, so I think it’s weird. He said something bad happened to him, and then he picked Helen to help him. This is unusual, right?

So I think, it’s an extreme situation, so maybe it’s a phishing one. I’m going to give a ‘Two’ for this.

[Break in conversation, 0:20:12-0:20:29]

I think this one is a legal one, because it has an official e-mail address, and also the e-mail, the content of the e-mail, looks rather good. And it has the signature, the address of the company. So I think this one is a legal one.

Yahoo. Hmm, it says it’s from the HR Recruitment Department from Yahoo. But the e-mail address is ’HR33433’. I don’t think the e-mail address is an official one.

[Break in conversation, 0:21:25-0:21:36]

It’s a phishing one.

[Break in conversation, 0:21:39-0:22:07]

This one, also. It said Helen purchased something, and asked to click a link. But the link doesn’t look very trustworthy to me. Maybe it’s a phishing mail.

Facebook. ‘Interview…’

[Break in conversation, 0:22:42-0:23:00]

This one is from Facebook. I think I received a similar e-mail from Facebook, and it was a legal one. I just clicked the link and I confirmed my new e-mail address, so this one I think is a legal e-mail.

[Break in conversation, 0:23:23-0:23:41]

There is an attachment to the e-mail. Usually, it shouldn’t have an attachment, it’s just weird. I give a ‘Two’.

I’m also…

[Break in conversation, 0:24:03-0:24:16]

I think this one is a legal one. It has very detailed information. The order reference, Helen’s e-mail address, Helen’s delivery address. I think it has all the information, so I think it’s a legal e-mail from Amazon.

It’s from Google. ‘Your Google e-mail…’

I think the Google one is also a legal one.

[Break in conversation, 0:25:00-0:25:10]

Yes, because the e-mail address looks very official. It’s ‘.accounts.google.com’. But there are two attachments. I think it’s a legal one, maybe. It’s a ‘Five’.

‘Surveys’. This one, this one I think it’s a legal one. It’s from ‘Surveys@paypal.co.uk’ and it shows Helen’s name on it. This looks quite formal.

This one, it says it’s from NatWest, but the e-mail address is, ‘UUP@Donkeytune.com’. I don’t think it’s an official e-mail address, so I think this one is a phishing one.

‘My address…’

[Break in conversation, 0:26:29-0:26:48]

This ad is a government website. But I don’t think the content of the e-mail is convincing. I’m not sure, I’ll give a ‘Four’ or ‘Three’. I’ll give a ‘Four’.

I think this one is a phishing one because the e-mail address is, ‘Admin@ebayz.com’. Why is it ‘Ebayz’? It should be ‘Ebay.com’. So I think something’s wrong with the e-mail address, so I think this one is a phishing one. I should go through the content of the e-mail.

Yes, it’s also asking me to click on the following link, and the link is weird. It’s a phishing one.

[Break in conversation, 0:28:04-0:28:21]

This e-mail didn’t have a subject. Usually this kind of, like, service e-mail, there is always a subject. So this one is weird. And the content of the e-mail is not convincing. It’s a phishing one. Definitely phishing.

[Break in conversation, 0:28:47-0:29:05]

I’m not sure about this. I’m not sure whether Helen has a driver’s licence or not.

[Break in conversation, 0:29:19-0:29:29]

I think this one is a legal one. It’s from a Lancaster e-mail address and the subject is formal, like \_\_\_[0:29:38] Technology. And also, the content of the e-mail is very convincing. I think so, it’s a legal one.

**P312**

P312: Okay, so the email address, the fact that it has numbers in, and normally… Are the email addresses normally a bit simpler than that? The fact it doesn’t use your name, I guess. But then, if there are specific case numbers, that seems more genuine.

[Background noise 00:01:07 – 00:01:25]

The web address doesn’t look like it’s the Dell website.

[Background noise 00:01:35 – 00:01:55]

Tricky. I think it’s a ‘three’.

[Background noise 00:02:12 – 00:02:35]

This seems like… Okay, so this seems more legitimate, because the link is like an actual email address, not loads of letters. The email address on the “from” thing looks like it’s proper. It’s less cluttered, and it seems like urgent-y, I guess. But then if it was fraudulent activity, there’d probably be a letter rather than an email, so yes, I think ‘three’ again, because it still seems dodgy.

[Background noise 00:03:45 – 00:04:23]

Okay. Okay, so in the email address it says “via” some other email address, which seems a bit suspicious, but then as you read the email, it reads like it’s legitimate, like the fact that there’s a number and an email address for help, and because it’s only reading the updated terms and conditions, that seems… Yes, it seems more legitimate than the last two.

[Background noise 00:05:07 – 00:05:33]

Okay, so the fact that it gives the actual name of the person, that seems, that makes me think it’s more legitimate. But then the fact, if it’s like a job application thing, and then the application form link has got arrows pointing to it, and also if it was a company, again, the email address doesn’t seem that official.

[Background noise 00:06:28 – 00:06:45]

I think ‘four’.

[Background noise 00:06:51 – 00:07:11]

Okay, so the fact that it’s got the webpage, it’s got that look like an invoice-like structure.

[Background noise 00:07:31 – 00:08:01]

Okay, so it says that for assistance you should log onto your PayPal account, which you’d do. Yes, so it’s inviting you to do that kind of separately rather than on it. Also the link is “paypal.com/help”, so that’s like a clear link, so I’d say that’s definitely legitimate.

[Background noise 00:08:38 – 00:08:55]

Okay, so… The link looks really complicated, but then assuming you’ve received that on the back of wanting to reset your password, I think that would legitimate. So, I’m going to say ‘four’.

[Background noise 00:09:42 – 00:10:06]

I’d say not legitimate, only because I think banks would phone you up directly or speak to you directly. I don’t think they’d email asking you to verify your account, because banks tend to do that, tend to be over-the-top with that. I would guess it’s not Barclays. Also the email address, again. I’m going to say that’s ‘two’.

[Background noise 00:10:42 – 00:11:10]

Okay, to be honest, this looks… Yes, this looks legitimate. I guess the fact that there’s no Facebook logo and stuff suggests otherwise, but as I read it, the way it read seemed legitimate. I’d go ‘four’.

Okay, the “Do Not Reply” thing is a common thing, but because it’s vague, like “Guest User” and “Seller received payment” it doesn’t seem as legitimate. I’d say maybe ‘three’,

Okay, so on the one hand, the actual wording of the email seems legitimate. I’m not sure why it wouldn’t be an official email address, though. So, I’m going to say ‘three’.

[Background noise 00:12:35 – 00:13:15]

Okay, this seems not legitimate, but I think I’m basing that on the assumption that big companies wouldn’t ask you to do that; I think they’d wait until you log on and buy something and it doesn’t work. Or maybe I’ve just ignored emails that have said to do this, but, hmm. I think that’s phishing. I don’t think big companies would…

[Background noise 00:14:00 – 00:14:30]

Okay, so it looks right, the way it’s set out; when you get emails from big companies they do look like that. But, the fact that it says “You know it’s not an official email if we use your first and last name.” Well, that could be a double-bluff, I guess. But, if you didn’t read that, I mean… Yes. I’d say it’s still, even despite that, it’s still quite legitimate, I’d say. ‘Five’. I’d say ‘five’. I don’t know if that… It’s not really based on the fact that the phishing thing, it’s based on the look of the rest. I think the bit underneath the login thing makes me dubious, but yes, ‘five’.

[Background noise 00:15:33 – 00:15:50]

Okay, because the English is really bad, I think, right, it’s definitely phishing.

[Background noise 00:16:02 – 00:16:20]

Yes, this looks legitimate. Yes, so the email is fine. Nothing makes me particularly sceptical. I don’t know if the fact that it says the account username makes me more trustworthy of it, I don’t know. Possibly. But I’m going to say ‘five’, I trust it.

Okay, NatWest.

[Background noise 00:17:10 – 00:17:23]

Yes, this looks legitimate. The look of it, for one. Yes, it just seems professional and good. I’m going to go with ‘five’.

[Background noise 00:17:48 – 00:18:50]

Okay, so if it’s a friend, then it wouldn’t just say “Hello” at the end, I think. It would say your name or how you address them. The extreme situation makes me sceptical. The specific amount of money. The fact that they’re thinking about bills. I think they’d just think about that when they get home, wouldn’t they? But then, if their credit cards were stolen, I guess, yes, I’m really dubious. This is definitely phishing.

Okay, yes, so Dropbox, yes. It looks really simple, like there’s nothing… Yes. This seems legitimate because it’s so straightforward, logo as well. The email address seems about right.

[Background noise 00:20:14 – 00:20:40]

No, I don’t think this… No, this isn’t legitimate, because… Or maybe it is. Maybe it is. I just think that if this had happened, it wouldn’t be like a blasé email saying “Just reset your password.” Then again, would they give advice? My initial impression was “No, it’s bogus.” But now I’ve thought about it, I’m wondering if, what would they do, really? My instinct is that it’s phishing. I’m going for ‘three’

[Background noise 00:21:45 – 00:22:10]

Okay, because of the situation I’m dubious. But then again… Yes, no, this is dodgy. Why would they leave that to a stranger if he’s choosing a trustworthy person? And if he knows that you’re trustworthy, then why would he have put all that detail at the beginning? Dodgy. I’d say ‘two’.

[Background noise 00:23:03 – 00:23:25]

Okay, firstly, the fact that there are attachments, but then maybe they’re like the attachments of the border and stuff, and the picture. Yes, it looks like they are. But it says “We’ve prevented the sign-in attempt in case this was a hijacker.” I don’t think… The term ‘hijacker’ seems a bit unofficial. If it is legitimate, it shouldn’t have a link to… Hmm. It kind of seems a bit… I’m not really not sure at all. I think I’m suspicious, so I’m going to say ‘three’.

[Background noise 00:24:49 – 00:25:10]

Weirdly, this seems legitimate, but at the same time, the lack of extra detail makes me a bit suspicious. Also the fact it says “Be wary of scams. Do not send money via Western Union.” Seems a bit strange to be at the bottom of the email, so it might be like a double-bluff. I would say it’s a ‘three’.

[Background noise 00:25:50 – 00:26:35]

Okay, the logo maybe makes me think it’s more legitimate, and the way it’s written, I’m not sure what exactly it is, but there’s something about the way it’s written. Having said that, they’ve made the stakes really high for not doing it by saying that your payment will be suspended, and that might be because they are suspended, but then that seems like to create an urgency to make people want to do it, like want to press it. That could be phishing. I think ‘three’.

[Background noise 00:27:29 – 00:27:50]

Okay, so the email address suggests it’s not NatWest, the way it’s simply done, there’s not much detail. That makes me suggest as well that it’s fishy, I think, definitely fishy.

Yes, that’s definitely fishy, so it’s just blatantly no attempt to be anything like Yahoo or Google. No, I’m going to say that’s ‘one’ – definitely phishing.

To say “We have concerns about the safety and integrity of the eBay community.” Seems a bit of a funny way of saying it.

[Background noise 00:29:17 – 00:29:28]

I don’t think an eBay email would be… Oh, but it’s suspended. “Due to concerns we have over the safety and integrity of… Take these actions if we are unable to verify or authenticate any information you have provided due to the suspension.” Hmm. In some ways… This is a difficult one. In some ways it seems suspicious, certain turns of phrases and stuff I don’t think a customer-based company would write like that, even for someone who’s been suspended. The fact that it’s not just admin@ebay.com as well. Also, ‘safe harbour department’ doesn’t sound like… I don’t know. I’m going to say ‘two’.

[Background noise 00:31:08 – 00:32:00]

This is really hard, I’ve no idea about this one. I don’t know if this kind of company would do that. Based on the email itself, I think…Hmm. There’s nothing exactly that’s saying “Don’t trust it.” But there’s nothing saying “Do trust it.” So I’m going to go with ‘three’.

[Background noise 00:32:40 – 00:33:10]

I don’t know, I think if you were getting an email that your credit card was suspended, I don’t think it would be by email, and again, I don’t think a bank would ask you to do that, so I think ‘two’.

[Background noise 00:33:35 – 00:34:05]

The way it’s casually written; on one hand, all the way through it I believed that it was legitimate, and then the way it said “Head over to our website”. Maybe it is, maybe that’s their tone, and if they’ve given you specific details like how much the things is, costs. The fact that there’s no big logo or anything is a bit concerning, but there’s an attachment, so that’s probably what that is, and then the email address seems fine. I think this is more legitimate, I’d say ‘four’.

[Background noise 00:34:58 – 00:35:20]

This looks legitimate. Yes, it just looks like a normal alert, so it seems legitimate, yes.

[Background noise 00:35:34 – 00:35:50]

The logo doesn’t look quite right. Why would it be… I don’t know why it’d be blocked for receiving payments. Yes, I think it’s phishing, because why would it be for receiving payments and not just everything? And the logo.

Yes, I think the fact that the links are missing, but there is like a template there of where it would be makes me think it’s legitimate. I’d probably say it’s legitimate.

The fact there’s no eBay logo makes me a bit suspicious. Why would it say “spoof” and then in brackets “fake” emails? No, it doesn’t seem right.

Yes, the fact there’s an order number, you can see the details of the thing, like the details of the… The thing, that was fine, but the fact that it’s not from Amazon makes me suspicious. I would say ‘three’. If it wasn’t for the email address, I’d have probably said it was legitimate.

[Background noise 00:38:39 – 00:39:06]

I kind of believe this. I kind of believe this is real, weirdly. It looks like I’d thing it was too vague or something, but I kind of believe it. I’m going to say ‘four’. Can’t put my finger on why, though.

[Background noise 00:39:26 – 00:39:50]

I don’t believe this, because why would.. ? I don’t think it’s the customer’s job to help, what’s it called? Update the system. I don’t think that would necessarily involve the customer. So, I’d say it’s phishing.

[Background noise 00:40:22 – 00:40:33]

Okay, because the email… Yes, this looks fine, because it’s just from a straight email, and because the link seems fine as well. I’d say that’s probably legitimate.

**P313**

P313: So, the Virgin Media one. This one does look pretty legitimate, but it has no name on the attachment. You would hope that it had your details on, like your customer number or your surname or something, or your phone number, but the fact that it says to go over to the website to send an email is reassuring, but you know, links and stuff in emails aren’t always legit, so I’m going to say that one is a ‘five’.

Okay, so now looking at the email about watches, and it’s very impersonal, it just says “Yahoo and Gmail user click here. Good day, give your loved one a luxury watch today. Good luck. Click here.” So, encouraging somebody to click on something, I’d say that’s pretty suspicious. Also the fact that the email has come from an account that’s not from a particular company, and it’s advertising multiple different brands of watch, it just looks really dodgy. So, I’d say that’s probably definitely dodgy, so I’m putting that as a ‘one’.

Okay. Dell one. I’d say this looks pretty legitimate. A lot of the time I get customer experience surveys, and then usually they’re using a third party, so assuming that the recipient has just had contact with Dell support, I’d say this is probably legit. Yes, the bit underneath the separator line seems to be fairly reassuring, and also the fact that it has the option to be removed from the list. So, I’m going to say, the fact that it also references your case number as well, so if it’s not legit you would immediately know, so I’m going to say that’s definitely legit. Oh, nothing’s happening. There we go.

Okay, PayPal. This looks fairly legitimate. It’s from “service@paypal.co.uk” and if your card were about to expire, then it’s legitimate. Well, it at least appears legitimate. All I would say is probably, maybe, if you’re clicking a link, sometimes it can take you somewhere that looks legit, where it isn’t necessarily, so maybe I would just go to PayPal to do it, go straight to the website myself. But yes, it looks pretty legit. I’m going to give that one a ‘five’, because I’m really weary of clicking anything to then put in card details when it’s requested by email. So, like I say, I’d rather just go straight to PayPal to do it.

Okay, NatWest one, telling you that you’ve got another statement available. Yes, I’m going to say that’s legitimate; it’s not asking you for any information, it’s not telling you to click on anything other than something to give you a bit of help, or to contact them. But basically, it’s telling you to kind of, this is a regular thing. The email account that it’s come from looks legit, and assuming that you would get these fairly regularly, you’d know if they were legit or not. So, I’m going to say definitely legit.

PayPal, this is a payment thing. Immediately, the first thing that comes to my head is the fact that the email address is showing a service from PayPal, but it’s not, it’s some personal or made-up thing, which is the person getting paid, it’s their address anyway. So, that’s a bit sketchy, and you apparently ordered a man’s watch, which seems not very legitimate. So, I don’t know. Hmm. That’s a bit of a worry. Because it’s got the address right. Oh, I don’t know now. Okay, that’s a difficult one, but I always air on the side of caution, so… Hmm. It’s just the email address thing seems weird to me. So, I’m going to say it’s likely to be phishing.

I don’t know how they’ve got the address right, though, unless they’ve already got that from your eBay account. I’m just going to put a ‘two’ for that one, because I’m not sure. It could be legit, but I would be really cautious, unless obviously you knew that you’d bought it.

“Please do not reply to this email. Follow the link below into your account to reply.” Okay, so this is quite similar to how a \_\_\_[00:07:06], email looks, so it’s just an automated thing which is why it’s telling you not to reply to it; it’s probably unmonitored. Then it gives you an email to tell you where to get into your inbox. I’d say it’s probably legit. Links and emails, if they’re unsolicited emails are always a bit of a worry, but you said to just assume that they’ve already got accounts with this stuff, so I’m going to say that’s a ‘five’.

So, Caxton FX Cards, but it says “via sut3.co.uk”. I don’t know what the hell that means. But it’s telling you to, that if you do need help, then go straight to caxtonfxcard.com. I don’t know if that’s the correct email, or whatever, for them, but it’s reassuring when they give you a way to get in touch with them, rather than just clicking on whatever. “Card is issued by Newcastle Building Society…” Blah, blah. It gives you its registration number at the bottom, and I guess if you had any worries you could always just call them, or Google a different phone number, check it out, and then… Hmm.

The email address is coming from “cards@caxtonfx.com” and the “info@caxtonfxcard”. They’ve got different bodies of the email address, so one’s “caxtonfx” and one’s “caxtonfxcard”. I don’t know if that’s anything. I’d say probably a ‘four’ for that one, because I get emails like this a lot from my bank people. Like I said, it’s kind of easy to check with the registration number and things.

An Adobe one. This sounds familiar. Okay, so this looks pretty legitimate to me. The email address that it’s been sent from looks legit. The reason that they would be doing this would be, it sounds plausible, and the fact that they’ve reset it. If they’ve reset it, then it probably is Adobe, and you could just try and log on with your old stuff, and if it has been reset then you know it’s legit. Also the fact that it’s got all the stuff afterwards about registered trademarks and stuff. That always seem reassuring to me, because they’re more worried about you robbing them. So, I’m going to say that’s a ‘five’.

Okay, so this Amazon email from somebody called “Carla Craig”, but then the email looks like it’s coming from Amazon. It’s weird. So, it’s a big expensive item, and the fact that it’s coming from a name rather than “amazon.com”, that worries me. I’m going to say a ‘two’ for that one.

This one is the Diablo III account one. This looks pretty plausible if you do have a Diablo III account. Yes, you can’t sell it, you can’t make a profit off of personal gaming accounts. Yes, I’d say it looks pretty legitimate. It is telling you to click on a link, but it’s a secure link, and it’s using the same kind of the base of the URL as the email that it’s come from, and assuming that Diablo III is part of the Battle thing, even though later on in the email it says Battle.net and not Battle.com. I’m going to say that’s like a… I’ll call it a ‘five’. Assuming that you are trying to sell your Diablo account. Actually, later on in that link it does say “Battle.net”… Anyway, that’s fine.

“Your password will expire in three days.” Hmm. It’s from washcol.edu, which I’m going to assume is like Washington College or something, given that it’s been sent to a Lancaster University address, that seems suspicious. The fact that it tells you to just go to an email address that has no security…Well, not an email address, a URL that has no security and nothing to do with either institution. I’m going to say that’s definitely phishing.

HMPS Recruitment and [igrasp.com 00:14:15]. I don’t know what “igrasp” is. It says “Dear Candidate” instead of “Dear [Name]” That’s a difficult one because the job seems appropriate, but that could be based on your search history. I’m going to say like a ‘three’ – slightly towards the suspicious end, but only just.

“Verified by Visa… Your credit card has been suspended, please update.” Hmm. Okay, well it’s “noreply@verifiedbyvisa.com” and the “verified by Visa” thing seems legit. It is asking you to click there to put in banking details, which I’ve said I’m a bit sketchy about, and the fact it says you have to do it within 72 hours or you’re suspended permanently. The things that worry me here is that they’ve not given you another option to contact them, so if for whatever reason you weren’t on your emails for a short amount of time, or you just would rather do it by phone or in person at the bank, they’ve given you no way of contacting them to check that it’s okay.

So, for example, if it said “If you wanted to call your credit card provider or pop into your bank.” Or whatever, then that would reassure me greatly, because then it’s like “You can go to them.” And they’d be legit, and you can do it properly. Also they’re copyright has ran out, I don’t know if that matters. I think also I’m personally biased from this because I used to work in credit card fraud; we always used to phone people to actually speak to them and get their security information, because just clicking through with this just seems dodgy. It seems like anyone with access to your email could do it. I’m going to say… God, that’s difficult. ‘Three’, because the email address is more reassuring, but the rest of it just sounds properly dodgy.

Actually, “noreply@verifiedbyvisa”. Actually, no, it just seems really impersonal. I’m going to go with a ‘two’.

PayPal one. Oh my god, how long is this going to take? PayPal one. Yes, so here they’ve said “We’ll always use your first and last name so you know it’s not phishing.” We know it’s not exactly a guarantee, but somewhat reassuring. The fact that it explains at the bottom as well, which is obviously on the end of every email. It tells you to go and login rather than, like… I mean, I know that there’s a link there, but you could probably just do it yourself. It also says if you’re concerned about security you can just go straight to the PayPal site, so that is greatly reassuring to me. The fact it’s from “epaypal.co.uk” and not “paypal.co.uk” is not something that I’ve come across before, but it seems, still… Okay, so I’m going to say that’s definitely legit.

Suspicious sign-in prevented. “Someone has recently used an application to sign in to your Google account…” This, to me, sounds pretty legitimate. I’ve had similar emails, not from Google, but every time I try and add a new device or something, it comes up with something like this. So, I’m going to say that’s a ‘five’. It does tell you to reset your password which could be a bit dodgy, but… Hmm. It’s got your profile photo and stuff on it as well, which… But that is really available, I guess. I don’t know, ‘five’.

Facebook. Immediately, the address that it’s come from seems really dodgy. It does tell you to disregard it if it’s incorrect. Oh, that’s difficult. So, if you just added this as a contact email address and then you were getting this email, then yes, I guess it would appear plausible, even though the email address it’s coming from just seems really dodgy. But, it’s sending you to bits of the Facebook website, which seems more legit. I’m going to put that as a ‘four’, because I’m not sure, but the body of the email seems really plausible, it’s just the address that worries me.

Okay, somebody from [Philippe 00:20:59]. Yes, it immediately looks very dodgy. I’m going to assume that you don’t know this Philippe person. It started with a rather dramatic story to try and get some empathy and sympathy from you, and then blaming the authorities. Yes, the way that they play it down, but it’s actually a really big bill. “If you can help us with a quick loan to sort out our bills and get back home, all we need is £1,850.” Why is that in brackets? It’s like it’s been entered in afterwards, like this is a template or something. I’d say that’s definitely phishing, assuming that you don’t know this person, personally. In which case I’d be really, really rethinking that friendship.

“Noreply@nusextra…” Okay, this seems legit. There’s a security check on your email address. The site that they’re sending you to is secure, and it’s \_\_\_[00:22:37], nusextra.co.uk, it’s using the same \_\_\_. Showing you the IP address that it was requested from so that you can check if it is fraud. So, I’m going to say it’s definitely legitimate.

FedEx. That seems dodgy, because you wouldn’t have to click a link to get a postal receipt; they’d just put it in the body of an email. Also, the email address that it’s come from is really, just dodgy. I don’t even know where Fort Wayne is, but I think that’s a place. Okay. I’d say that’s… That doesn’t even look like the FedEx logo. I’m going to say definitely phishing.

Barclays. support@vnet.com. I don’t know what “vnet” is. No, because it’s asking here for your account details and stuff, that’s what will be at the end of that link, and the fact that it’s giving you no other option, I would be straight on the phone to my bank, using a number that I had found myself, not from an email or anything. ”vnet”, I have no idea what that is, so I’m just going to say it’s definitely phishing.

Direct.gov. Why is it “studentfinancee@direct.gov.co.uk”? That’s Student Finance England, okay, I get it. Right, that’s immediately suspicious to me, because I’ve never known Student Finance to offer to check that you’ve got your payment and to give you a payment, or to avoid a mis-payment. Okay, if you fill in the requested information directly, like exactly as you filled it in when you were signing up for it, then somebody could just clone it. “Or your payment will be suspended because of failed account verification.” That sounds too threatening to have been coming from a legitimate source.

Also just some of the writing of it, like there’s a comma and then a capital, and a full-stop and then a non-capital. It seems poorly done. Also, all my student finance stuff came from a different company to direct.gov. Okay, so definitely phishing.

This could be legitimate… Oh, no. No it’s not. I’ve just seen the address that it’s come from. So, this is the NatWest one. It’s come from a really dodgy address. It’s telling you to come in to your thing, to click to log onto your online banking, check your profile’s up to date. Again, it’s got a threat in it, saying “If you don’t do it within 24 hours, your account will be disabled.” And I’d say that’s definitely phishing, because otherwise… I don’t know.

Yes, Student Loans Company is who originally I got my money from; not from that one. Okay. “We’ve detected fraudulent activities going on with your student loan account… Please fill out your information securely. You can do this by clicking on this link.” Hmm. So, slc.co.uk, I think is the thing for it, but it still seems a bit dodgy, “directgov@slc”. If anything, it would be the other way around, because SLC are kind of ‘freelanced’ by the government, I don’t know. The fact that it’s sending you to a link that has nothing to do with student loans, and it has “mineface” in it. Anything to do with mining just worries me. So, I’m going to say it’s definitely phishing.

Oh my god, I’m just going to shut that window, because you won’t be able to hear me. Oh, no, apparently I can’t. Can’t close it. Okay.

Okay, this is another one with an immediately dramatic… This is like a Gary Cooper one, by the way, with a fairly dramatic kind of sob-story at the beginning saying that he’s terminally ill. So, he’s chosen you as a trustworthy person, but doesn’t even know your full name and phone number, so that’s very not-legit. It does give you a Skype one, though, so I guess you could actually see him. No, I’d say the email address it’s coming from doesn’t look legitimate, especially seeing as the email that he then gives you is a different one at the bottom. I don’t know what the “.ci” is, but it says he’s in Italy at the moment. The one at the bottom is “.it”, that’s Italy, +39, I think, is Italy. I don’t know. Yes, I’m just going to say definitely phishing, because nobody would leave their fortune to a stranger.

”ioffer”. “Congratulations, you’ve just purchased an item from Gogglebox UK.” This seems pretty… This could be legitimate, I don’t know. “ioffer.com”, assuming that that is a decent website; it says that “You’ll get an invoice with payment and shipping instructions shortly from the seller.” But it also says “Click below to pay.” I don’t know, I’m going to give that one like a… I don’t know, because in this situation I don’t know if I’ve ordered this or not, so… Just going to say a ‘three’.

“Dear Applicant, thank you for your interest in the new role.” Okay, the email address that that’s come from looks really dodgy, because it’s just a yahoo.co.uk one, which is free, anyone can get it. “HR Dep” and then a bunch of numbers, so they’ve probably done this a bunch of times with different email addresses, which means that they’re trying to avoid people that have blocked them. The fact that it doesn’t tell you what the job is. It just seems very, just way too positive. “You can have a fulltime or part-time, it’s flexible. You can get 40 hours a week during the week. You’ll come to this little interview and meet a new team in your dynamic working environment.”

It doesn’t tell you anything about the job or where to turn up to your interview, it just says “Please click here to download application form.” So, they’re an inviting you for an interview before you’ve applied for a job, which does not seem plausible. I’m going to say that’s definitely phishing.

Okay. PlusNet. The PlusNet one seems pretty legitimate. It’s telling you your own account username, so you can easily check if that’s correct; saying that you can get your protection software by clicking this link, and that’s a secure thing, and it has the right kind of stuff in it. It’s got the “PlusNet” bit in it, it’s a portal, it says, to download your McAfee thing, which is exactly what it says in the email. So, it looks pretty legitimate. I’m going to say that’s definitely legitimate. Also it gives you the option of calling them, going to their website at the bottom, the email reference, how to get a help assistant, seeing their help pages. It just all looks really legitimate.

Okay, HSBC, the world’s local bank. This looks really quite dodgy actually, because the HSBC logo’s wrong. It says that there’s “incoming funding blocked” which is always, it’s like the lure of saying, they’re blocking incoming money, “We want to give you money.” Like that guy with wanting to give you his fortune. “This is to inform you the business account with us has been blocked for receiving payments. It will be disabled if you ignore this message.” Any email with a threat in always seems really dodgy to me. The fact that it’s not signed off with a name for something like that. If you’re a business customer, chances are you’d have a named person that deals with you. I’m going to say that’s definite phishing.

Okay. “Gogglebox has received your…” Blah, blah, “Click below to view the status of your purchase.” Okay, this is like the follow-up to the other one, assuming that you have bought it, then I’m going to say that’s definitely legitimate.

eBay suspension. The email address it’s come from is dodgy. The user agreement would be freely available, so it doesn’t matter that they’re quoting that. “If you could please take 5 or 10 minutes and update your personal records, you’ll not run into any future problems.” That sounds really suspicious, because they’re like “Yes, in the future you can just do whatever.” No, so “We just want some data from you, and then we’ll let you do whatever you want.” That’s really suspicious. But it does tell you to go to ebay.com, so… Hmm.

Again, the copyright’s out of date as well. I’m just going to say that that’s definitely phishing. Oh yes, it says you can’t update your actual account, but it wants you to update your personal records, and you’re not allowed to use your eBay account at all, so that would be putting you off trying to check it with eBay. Yes, it’s definitely phishing.

Billing, eBay… That seems pretty legitimate. It’s “billing@ebay.” It’s telling you the account, that you’ve set up PayPal, that it’ll immediately come out. “Remember eBay will not ask you for sensitive information…” That looks really legitimate, so I’m going to say definitely legitimate.

“DropBox needs to verify your email address so you can share folders.” It’s coming from a legitimate email address. It sounds plausible. So, I’m going to say definitely legitimate. I’m pretty sure I’ve had something like that.

“Dear Pleasure Beach Visitor” That’s immediately impersonal. “In response to a survey…” What? Oh, relating to… God, sorry. This could be legitimate. Assuming that you’ve recently been to the Pleasure Beach and given somebody your email, I’d say this is probably legit. I’m going to say a ‘five’.

DVLA. Hmm. DFT. I don’t know what ”DFT” would stand for, because for driving it tends to be DVLA or the DSA, and the fact that it’s saying it’s coming from the DVLA, but it’s actually from DFT, that’s a worry; but then the email address that they’re sending you to is “dft.gov.uk”, but I suppose you could just write that into the URL when you’re creating your website or something, I don’t know. It’s also bad grammar involved in here. “Drivers that refuses to upgrade… They’ll lose their driver’s license and have to take a fresh driving test.” It just all seems really dodgy. So, I’m going to say that’s definitely phishing, because they’ve used threats and vagueness.

“rmalcolm@lancaster.ac.uk”. “Dear Student, welcome to Lancaster. I hope you’ve enjoyed your first few weeks. We want you to do a survey.” Yes, that all seems really legitimate. It’s using SurveyMonkey, which I know about, it’s a secure URL that they’re sending you to, it’s from “rmalcolm”, which is an internal email, and it’s attached to the institution because it’s @lancaster.ac.uk. It tells you to go and speak to \_\_\_[00:38:57], Malcolm if you need to, which is the same thing. Yes, that’s fine.

**P315**

P315: PayPal. [Helen Jones 0:00:03]. 'Re your recent transactions on…' Okay, it looks legitimate with the logo of PayPal. Yes, I think that's definitely legitimate. 'How do I know this is not a spoof or phishing email? \_\_\_[0:00:28] PayPal [only]…' Yes, it's got the reason why it's not a spoof email, and it says who it is. 'Dear Helen Jones…' Okay, I'll go for six; definitely legitimate.  
  
'Dear Candidate, a job matches your \_\_\_[0:00:50] criteria \_\_\_.' Mmm. This is less so legitimate, because it just says, 'Candidate.' But then 'a job which matches your… has been published on our website.' Yes, I think that's quite legitimate. It doesn't have any logos in it, or anything like that, but it looks quite normal. It doesn't say anything about putting bank details in.   
  
Student Finance. I think this is less so. I think that's less legitimate, because of the font. I think that's Times New Roman. No, because it's money as well, and all the stars at the bottom make it look less legitimate, I would say. No, definitely phishing.   
  
Next. 'Hi Helen. You recently entered a new contact email address.' No, this doesn't look very legitimate, because there's no logo or anything like that. It just says, 'Thanks. The Facebook Team.' Their email address, facebookmail.com, and the weird email address just doesn't look right. So I'm going to go for not definitely phishing, but probably phishing.   
  
'Your mobile bill dated…' No name for attachment. No, that's definitely phishing. [Virgin Me- 0:02:59]. From just the email, it could be legit, but then I don't like- The subject is bolded, and it's about money. I think it's because of the attachment.  
  
Plusnet support. 'Thanks for using…'

[Break in conversation 0:03:23 - 0:03:37]

I don't know. They've got the user name, so if the user name was right, then maybe it is just a… I'm not sure about that; somewhere in the middle.   
  
'Greetings. Trying to…' Blizzard Entertainment. noreply@battle, so the email is different to the name of email address and the subject. It sounds like a different account as well. 'Greetings. You are trying to sell your personal… As you may not be aware… \_\_\_[0:04:17].' Mmm. 'Open this connection,' doesn't sound very real. 'If you had already authenticated your account, please disregard.' No. I think that doesn't sound very professional.   
  
'Please open this connection,' that just doesn't sound right. Then even just the fact that the comma isn't straight after the Diablo III sign, I just don't trust that. So I'm going to go for not definitely phishing, but more than likely.   
  
eBay suspension. eBay is .com. I'm not trusting… 'Dear Valued eBay Member,' mmm. I think they're trying to use the user agreement, section nine, as making it legitimate, but it doesn't make it sound as legitimate. Safeharbor Department, eBay.   
  
Then, I don't know whether it's just this computer, but the actual quality of the eBay logo and the eBay suspension is a bit grainy. It doesn't look very good. I just don't like eBay's… It usually has some sort of logo at the bottom or at the top if it's going to be an actual logo'd email, I think. So I'm going to go for two.  
  
Service PayPal, okay. 'Your card is about to expire.' No, I don't think that it would send you an email to do this kind of thing. service@paypal.co.uk seems legit, but then, usually, it has a title, and then the email. 'Update your card details.' No, it's not too bad, but I wouldn't trust that. I would have to get a better email than that to actually change banking details, because that's obviously quite dangerous.  
  
Ooh, I can't really read this. TNS, on behalf of Dell. dellsurveyhelp@email[2.rap 0:07:13].tnsonline. Mmm. Well, because it's got a specific case number and a service type, that sounds quite legit. Yes, and it's just a survey. I don't know. 'To be removed from the list, remove, click here.' That looks quite legitimate. Okay, I'm going to go for a five, even though it's quite small writing. There's the Dell at the top, but… I don't know. Yes, I'll go for five. Okay.  
  
PayPal. This looks more legitimate. I don't know. There are the different colours, the 'Unconfirmed' in green, the questions with the little question sign. This all looks quite good. It all looks quite well laid out. The colours aren't too extreme. 'You sent a payment of… to [Kenneth]…' [They're actually using PayPal 0:08:16]- Yes, I definitely believe that.  
  
FedEx. 'Dear Customer, your parcel has arrived. Our post rider wasn't able to…' The 'Get postal receipt' isn't central in the button. It looks like you could've made that on Paint. I don't know what the actual FedEx logo is. I think it might actually be like that. Hmm, I don't know. It's a cross between it not being legitimate, and then FedEx just not being a very good company.   
  
Tracking number. I suppose it has the tracking number in the subject. That could be quite good. I'll go for a middle one, but more so phishing.  
  
Visa. 'Dear Valued Customer, your credit card has been suspended as an error was detected in your credit card \_\_\_[0:09:19]. You need to update… To lift-' No, the 'Click Here' and those little arrows don't look legitimate at all. 'To lift your suspension' just doesn't give you enough information to have to do something so extreme with your credit card. It says, 'If it not resolved in 72 hours… as it may be used fraudulently.' No, I think I'm more likely to say that it's phishing if it's something to do with bank accounts.   
  
HSBC. 'The world's local bank. This is to inform you that \_\_\_[0:10:03].' 'Click here to begin to resolve the issues' seems less extreme. 'If you're not authorised to [continue], please forward to the [authorised]…' 'Customer Business Unit' is a bit vague. I would probably ignore this email if it came to me, even if I had an account. Yes, I'm going to go, 'No.'  
  
iOffer. No, there's not enough information. There's no logo. It's all in the same font. It looks like I could've written that.   
  
[Frank]@easyroommate. 'Please do not reply.'

[Break in conversation 0:11:01 - 0:11:17]

I don't know. 'Just received a message from [Graham], an Easyroommate member.' It's a very long link, if it doesn't work. Then I don't like the red, in capitals, 'Please do not reply.' I'm going to go for more phishing than not.   
  
eBay [sent this message 0:11:46]. 'eBay notification for Monday.' \_\_\_ makes it look more legit, and then, 'Amount due. You've set up PayPal as your \_\_\_.' Yes, I think this looks quite… 'eBay invoice notification \_\_\_.' Well, because it's eBay, and that's such a well-known company, you'd expect the logos to be on there. I wouldn't say it was definitely legitimate, but everything else looks okay.   
  
'Important \_\_\_[0:12:26].' When it's like this, like more of a PDF style, rather than actually written, it makes me question it a little bit. 'An attacker illegally entered our network and may have obtained…'

[Break in conversation 0:12:44 - 0:12:59]

Yes, when it says things like, 'Too many newsletters, you can unsubscribe or schedule automatically…' that makes me trust it a bit more.  
  
NatWest. 'Your latest statement is avail-' I'm used to that font; that is the NatWest font. 'Online banking... ending 801 is ready for you online now. Just log on to NatWest. If you need more help…'

[Break in conversation 0:13:30 - 0:13:42]

Yes, I think that's quite legitimate. I'll give it a five.   
  
Barclays. See, now, barclaysonlinesupport@vnet, that doesn't really seem to be anything to do with Barclays. 'An important account notification. Dear Barclays Account Holder… Unusual activity.' No, I don't think I would trust it. It's only got the Barclays logo that anyone could have copied and pasted. No. I'm going to go for a two.   
  
Oh, Gucci, Cartier or Rolex. No, straight away, I don't even trust that a tiny bit. No, definitely phishing. There's nothing on there that looks remotely legitimate. It's just one link, and then, 'Good day. Give your loved one good luck.' No, that doesn't look anything like Gucci.  
  
Now, these have obviously got these little pages that are things that haven't managed to load up, which makes it look a bit dodgy. Then the, "This is an automated email. Please do not reply,' that doesn't look right. The fact that you can't- I don't know. Unless you've got a slow computer that's not picking that up, but usually, it would do that, wouldn't it? Less legitimate than legitimate. I'll give it a three.  
  
Caxton FX cards. \_\_\_[0:15:19]. Yes, that looks okay. It's just terms and conditions to have a look at. It gives an address, and then a phone number. I don't know about this cards@caxtonfx.com via \_\_\_[0:15:50]3.co.uk. That makes me trust it less, but I probably wouldn't think about that too much. If I just received this, I'd probably just look at it and think, "No." I'll go for three.  
  
Job application \_\_\_[0:16:06]. 'Thank you for your interest in our new role.' So it doesn't say a specific role. It goes from, 'We have reviewed your CV,' to '\_\_\_ and my shortlist.' No, and then he only just introduces himself later on. No, and then the way that the arrows are pointing to the 'Download application form,' it just looks dodgy. And it's a Yahoo account. Surely, if it was a real company, they'd have their own company account. I'm going go for two.   
  
SLC UK. 'This is a message for all receiving grants and loans. \_\_\_[0:16:58].' No, 'This is a message for all students receiving grants and loans.' No, there's nothing on there that makes me trust it.   
  
[Sad news 0:17:19], and then loads of… Oh, absolutely not. No, anything that emails me, if I don't know them and it's about illness, then it's just obviously a scam. 'I'm counting on your good faith to carry out this work, and better.' No. How would he have got the email address then? No, that's just silly. And the way that he's saying specifically where he was born, and what date and everything, just makes it look silly. No.   
  
NatWest. I think the email address of this- It could be okay, but then, when you look at the email address, it's nothing to do with NatWest at all. No, that's just a way to easily get onto your internet banking. I'm going to say, 'No.'   
  
'Your password will expire in three days. Click here to validate your email. [Shaun Tegran 0:18:57] \_\_\_ system administrator.' That's an education account. 'Upgrade \_\_\_.' No, I feel like, when you have to update your passwords for emails, it'll do it while you're actually logging on to the emails. Definitely phishing.   
  
Google download. I think when things come with an attachment, I tend to not trust them. noreply@googleaccounts.

[Break in conversation 0:19:33 - 0:19:46]

I don't know, because they've got the Helen Jones, and they've got your little profile picture. That's what's been attached. It's got the IP address. I don't know. I'd go either way for this, but I'm less likely to believe it, because of the attachments.   
  
No, this looks awful. That's such a long web address, and the black line across, with something that hasn't quite loaded just makes me think that it's definitely phishing.   
  
Amazon. '\_\_\_[0:20:30].' I feel like ellipses make things look less professional.

[Break in conversation 0:20:40 - 0:20:53]

I suppose if it doesn't say, 'Click on this,' to get where I- Oh, I suppose, 'Please visit your orders.' Mmm. I suppose you'd know, wouldn't you, if you'd actually ordered that? That probably is legitimate. But then from [Carla Craig], I don't know. No, maybe not. I don't know, but probably phishing.  
  
Dropbox. That looks legitimate. noreply@dropbox.com, and then they've got the logo. Yes, I believe that.  
  
[team 0:21:35]@blackpoolpleasurebeach. I don't know.

[Break in conversation 0:21:40 - 0:21:51]

'Gain unlimited entry to Pleasure Beach for the whole year.' I don't know. No, I'm not really trusting this that much, because there are no images or logos or different kinds of fonts. It's all the same, and then some things are in capitals. It just doesn't look very professional. I'll go for a two.  
  
DVLA. Yes, the link is a little bit of a different colour to match the DVLA. We've got the copyright at the bottom, with where it is. I'm not sure about the email address though. I don't know if DF Department of \_\_\_[0:22:37]. No, I don't know what that could be. But then dft.gov/dvla, that would be good. Yes, that's okay.   
  
'Welcome to Lancaster.' Yes, [r.markham 0:23:02]@lancasterac.uk is somebody's email address. That's how everyone's works. Faculty of science. Yes, and it's specific. Yes, and then you can email him with any questions. Oh no, email her, sorry, with any questions. Yes, that looks okay.  
  
Okay.

**P316**

P316: ‘Hi, Helen, you’ve just received a message from Graham, an Easy Roommate member. Click here to see the message and the profile.’

Hmm. And the link about, ‘Click here to see the message and the profile. If the link above does not work, just copy and paste this URL into your browser.’

\_\_\_[0:00:35] message box. Source equal send, easy mail, mail at ETM. Medium equals mail, internal. Content application. Campaign application.’

‘Regards, Frank. We’re committed to helping you find the right flatmate. Beware of scams. Do not send money by Western Union.’

What?

Okay. I don’t understand why there are two links, because surely one link would work, and the fact that there are two makes me doubt it. And also, the thing at the bottom saying, ‘Beware of scams, do not send money via Western Union’, I don’t understand why that’s even relevant to this E-mail.

Why would I be sending money?

The link that I would be copying and pasting looks fine. I mean, like, it’s really long, with all the numbers and everything, but in terms of the words that are there, there’s nothing kind of like, ‘Info, blah, blah, blah, blah, blah.’

And the fact that it says, ‘UKeasyroommate.com’ as the website makes me think it’s okay, but the ‘Click here to see the message’ makes me wonder whether or not the ‘Here’ is going to open up something.

But the scams thing makes me, like, the ‘Here’ thing could download a virus or whatever. But the ‘Beware of scams’, I don’t understand why that’s even in there.

And the fact that they’re saying, ‘Oh, beware of scams,’ as if they’re your friend, warning you about stuff. I would go with a ‘Three’. No, I’m going to go with a ‘Four’, because it seems more legitimate because of the ‘Easyroommate’ and stuff, the link website for the browser.

But it’s just a bit dodgy, so that’s why it’s not definite. ‘Four’.

‘HSBC, The World’s Local Bank’. The logo’s wrong. The logo’s completely wrong. That’s not what HSBC looks like.

‘This is to inform you that the business account with us has been blocked from receiving payments. An attempted error log-ins was detected by our security system and this account will be disabled if you ignore this message. Please…’

Definitely a scam. Hundred percent scam. Because the wording is all dodgy. It doesn’t, like, make sense, and the, ‘Please click here to begin to resolve’, that line. No.

‘If you are not an authorised signatory, please forward to the authorised signatory. Best regards, Customer Business Unit.’ No.

But also, for HSBC. HSBC, it would be saying, ‘Don’t reply.’ It would have, like, a sign-off thing underneath the person that’s sending it. It wouldn’t be some random thing like, ‘Customer Business Unit.’

And also, I know from banks you don’t get an E-mail, you get a phone call. So this is, yes, definitely phishing.

‘Barclays’, okay. This looks a bit more legit.

‘Dear Barclays Account Holder.’ Hmm, it think it would say my name. Yes, it would say my name.

‘Support, Barclays Online’, and then the E-mail address is ‘Support@B.net’. Okay, no. It’s just a good scam.

‘We have detected unusual activity in your account,’ yeah, whatever. ‘This may be the cause of logging into your online banking from several IP addresses. To reduce the risk of unauthorised access, we have decided to limit your account until you complete the steps…’

Damn.

No, it’s phishing. It’s just a good phishing thing because it’s asking me to give it all my information. Again, they call to tell you that something’s going on, and they would know my name. So, definitely phishing.

Oh, and the E-mail address.

Okay, so ‘HR Recruitment Department, HR-Dept.’ Hmm, Yahoo? Really?

‘Dear Applicant, thank you for your interest in our new role we have opened. I would like to…’ That should have been new \_\_\_[0:06:03]. ‘I would like to let you know we have carefully reviewed your cv.’ That should have been in capitals. ‘And I am glad to inform you that you have made my short-‘

‘My shortlist’ or ‘Our shortlist’?

‘We will be interviewing candidates in the next few weeks.’ ‘Interview’, again, should have had a space. ‘It will last no more than 20 minutes. It’s a great…’

Okay, so the spelling and grammar is all off.

‘It’s great to ask for you to sit…’

[Whispered reading, 0:06:33-0:06:47].

Hmm, if it’s part time, it’s not going to be 40 hours, then, is it?

I think it’s a bit scammy, because he said that he’s attached it, but then it says, ‘Download it.’ And it would be an attachment, not that.

Mmm. No. I think it’s a scam. I don’t know, I just think even if I was applying for a job somewhere, if I was sending out loads of things, he hasn’t said what company he’s from. Nowhere does it say what company he’s from. And all the spelling and grammar is completely off.

I wouldn’t have to download it. And then it just seems really immature coming from a business, unless it’s a really crappy business, so I’ll go with a ‘Two’.

PayPal. Hmm, looks pretty legit. ‘@e-paypal.co.uk’. It looks pretty legit.

‘Helen Jones, we have found that…’

[Background noise, 0:08:23-0:08:38]

Yeah, I don’t know. I think it looks okay, but then it’s just a screenshot. Hmm. The thing is, I wouldn’t never do it, though, because I would be concerned that it was. I’m going to go with a ‘Three.’

I [would say with 0:09:14] caution.

‘Gucci, Cartier, Rolex.’ Woah. This is completely, no. Its phishing.

‘Yahoo and Gmail user, click here.’ Why? What, so you’re spamming everyone.

‘Good day. Give your loved one…’

No, it’s completely phishing. It’s completely…

‘Lacos.com’, who is that? Who? It’s nothing. You’re just going to go download a virus and they’re going to get your stuff.

‘NatWest’. Looks okay. It looks alright. E-mail. Website. No go.

Mmm, surely account numbers always end in four numbers. But then the fact that it’s specific, and you know, if that is me, they can’t have sent that to a load of people.

But why would they say, ‘Hi’? Surely it should be, ‘Hello.’

I think this is…

[Background noise, 0:10:37-0:10:47]

I think this is fine. It’s not asking me for anything and all it’s directing me to is Natwest.com/online. Provided that the hyperlink that I then click on doesn’t take me to another website, then I think it’s fine.

Yes, I would go with a ‘Five’.

‘Caxton FX.’ ‘Fias@3.co.uk,’ hmm, what’s that?

‘Changes to the terms and conditions of your Caxton FX pre-paid Mastercard. Hmm, this sounds already dodgy.

‘Dear Helen Jones, please take the time to read your updated terms and conditions, which are available here. We recommend that you retain a copy of the updated terms and conditions for your records.’

‘Here to help. If you have any questions about…’

I just don’t believe that it’s real.

Mmm. Meh, I don’t know. If I have a Caxton FX pre-paid Mastercard, I think that’s fine. And then obviously, they’re 0845, that’s their phone number. Yes, I don’t know, I think it’s fine. Given an address, proper sign-off thing. Yes. I’ll go with a ‘Five’.

Hmm, maybe ‘Six’. Yes, I’ll go with a ‘Six’.

‘Your card is about to expire’, ‘@PayPal’, okay, yes. Ooh, which makes me think, this is a different address. It’s not ‘E.PayPal’. It’s ‘PayPal’.

‘Your card is about to expire.’

‘Dear Helen Jones, we noticed that your Visa Delta Electron ending 1234,’ really, 1234? No-one’s card ends 1234. ‘Is about to expire. Please update your card, expiry date and card security code as soon as possible to avoid any interruptions using PayPal.’

‘Be sure to activate your new card with the bank first.’

I don’t understand why it’s in this little window box thing. It looks like it’s copied and pasted into there. It just looks like everything’s been copied and pasted, one thing from, like, an E-mail that someone’s been sent from PayPal below, like, the sign-up thing at the bottom.

And then the PayPal logo at the top, and then this bit in the middle just looks like a text box inserted in.

And why is, ‘Update card’ highlighted in yellow? It wouldn’t be. No, I think it’s weird. And it’s asking me to provide information. No.

I would say, ‘Two.’ Phishing.

‘Gary Cooper, mail to GMB@aviso.ci.’ Confidence.

‘Hello, I’m Mr. Gary Cooper. I was born,’ hmm? What?

‘I was born January 13th, 1933 in London, England. I’m in a medical institution in Italy where I’m writing to you…’

‘How is your life?’

He’s pretty old.

‘The doctors have asserted that my days are numbered, therefore I would kindly leave you my fortune to good use. Especially for a charity primarily provide support to orphans.’ Is he foreign? No, he’s not, he’s English. Then his English is bad.

‘Therefore I would kindly leave you my fortune to good use. Especially for a charity primarily provide support to orphans, destitute and homeless. I have no heir apparent, and my situation does not allow me to assume management to these funds.’

‘I chose you as a trustworthy person, at least, I hope, to follow my last will. I count on your good faith to carry out this work and better. Could you contact me, your full name and your phone number via E-mail to complete the procedure? Waiting to hear from you, sincerely, Gary Cooper. Blah, blah, blah.’

Why has he said all that information at the top, as if I don’t know him, and then E-mailed me to leave me his fortune, apparent fortune? How about there?

The information that he’s asking for me is for my full name, my phone number and my E-mail address. Even though he’s already got my E-mail address. I guess it’s to check it’s right.

It seems okay, but I don’t know whether I would do it. I probably wouldn’t. I just wouldn’t believe that some randomer would leave me his fortune. I’m going to give it a ‘Three.’

Already looks legit, the logo, the E-mail address. ‘This is a formal notification of an important account update. Due to a recent update in our database.’ Hmm, grammar and spelling are all wrong. ‘We require all students to update their account information to ensure you receive…’

Scam. ‘Click here to validate your information. Please fill the client requested.’ [Your spelling app 0:16:40].

‘Student Finance England.’ No. It wouldn’t just be ‘Student Finance,’ or it would be Direct.gov.

And ‘Student Finance’ is spelt wrong in the E-mail address. Definitely phishing.

Dell logo looks a bit odd. Looks like a copy and paste jobbie.

‘Dear valued customer, thank you for your recent contact with Dell Support regarding case number blah, blah, blah, blah, blah. At Dell, we are committed to delivering the best customer experience to our customers.’

‘Valuable feedback regarding your expectations…’

The E-mail address looks a bit dodge.

[Background noise, 0:17:25-0:18:27]

Okay, so it’s talked about privacy and protection policy, which is good. It explains the E-mail address because it says that TNS is conducting their market research. I don’t know. It seems okay. I’m going to go with a ‘Two,’ because why wouldn’t Dell send it to me, rather than TNS, and what does TNS stand for? It doesn’t say anything about this TNS company.

I would probably want to Google TNS, and to be honest, I probably wouldn’t do it anyway. I’ll go with a ‘Two’.

‘Helen Jones, I’m sorry for reaching you rather too late due to the situation of things right now. My family,’ spelling and grammar, ‘and I…’

Aw.

[Background noise, 0:19:37-0:20:05]

No. Okay, if I know this Philippe person, and that’s his E-mail address, then I don’t really know. I don’t know, I think it’s legit.

If I know Philippe and that is his E-mail address, yes, I think it’s legit. ‘Five’.

‘Igrasp.’ Okay, it’s got the sign-off thing. Looks okay. \_\_\_[0:21:06].

‘Published on our website. Please click.’

Yes, I think it’s real. It just seems like all the other E-mails that you get from these places. Yes, legit. The website looks right, the E-mail address looks right.

No. The E-mail address is completely wrong. I don’t even need to look at anything else.

You set up payment to that person. ‘Thanks for using PayPal’. Okay.

Well, it’s not asking me for anything, so I don’t understand, why would that be a scam, or phishing, even?

No, I think that’s fine, if that’s what I bought and I sent that person money, he’s just sending me a receipt, basically. Yes, legit. Didn’t ask me for anything.

eBay.

[Background noise, 0:22:28-0:22:48]

Yes, that’s all fine. Sign off, E-mail address. No.

Website’s all good. Definitely visit.

No, it’s just asking me for my information, and that would never happen. Also, the E-mail address is completely wrong, and no.

It’s like a threat. No, definitely phishing.

‘Dropbox’, I have a Dropbox. ‘Please verify your E-mail address before you can check orders.’

Yes, I think that’s fine, because that’s what you normally have when you start a thing, ‘Noreply’, yes. Definitely legit. And it has the little ‘Copyright 2012 Dropbox’ thing at the bottom.

‘You or someone else entered this E-mail address to the password of your NUS access.’ Okay. Yes, I think this is valid. I’ve had E-mails just like this. And if I did that, then I did that. Yes. Legit. I don’t know why their NUS thing isn’t coming up ,though. That’s weird.

Now I’m going over to Adobe systems.

[Background noise, 0:24:35-0:25:04]

No, don’t believe it. Oh, I don’t know.

It just doesn’t look right.

[Background noise, 0:25:20-0:25:32]

Okay. If this happened in October, and then it says, ‘Please beware, on the lookout for suspicious E-mails or phone scams seeking your personal information.’ Yet this is one just like that. I think it’s just tricking me and taking the piss

No, I’m going to go with ‘Phishing.’ I would never do that.

‘Greetings. It has come to our attention that you are trying to sell your personal Diablo III account.’ What even is that? ‘As you may be aware, this conflicts with the terms of agreement…’

[Background noise, 0:26:10-0:26:48]

Well, this sounds very weird. I don’t know. I’ll give it a ‘Three.’ I’ve got no idea what this is about. But it’s \_\_\_[0:26:57]. Actually, I’m going to go for ‘Two’ because it’s threatening me.

FedEx logo’s wrong. E-mail’s completely not FedEx. ‘DTF’, what are you..?

‘Post…’

No, I just think it’s going to download a thing. I’ve not used ‘Four’, [Wave 0:27:29].

No, I’m going to go with ‘Three’, because it’s got the order date, and if that’s right and the order number is right, I don’t know what it’s asking me to get.

I’ll go with, ‘Three’. Don’t trust it.

Why doesn’t just tell me he website rather than..?

No, definitely phishing. I don’t understand. Why is it going to take 16 quid out? Then you have to go on your bill. I don’t want to click on the bill because it says, ‘No \_\_\_[0:28:33] for attachment.’ A zip file, 50kb? No.

Don’t give them your address.

Looks right. ‘eBayz’? No.

It should just be ‘eBay.’

[Background noise, 0:29:00-0:29:36]

It looks pretty legit. Oh, attachments. Does that mean that it’s not actually automatic, and it’s just saved that information and then had to attach it because it’s not real?

Nope. Go with, ‘Two’.

‘Dear Miss Jones…’

Mmm. It seems fine. Why is it no from McAfee? No, I’m going with a ‘Three.’

Fine. I think it’s a ‘Five’. And all it’s told me, about all the information about it.

Pretty fast delivery, next day. [Insist 0:31:27] a receipt. I understand. Yes, fine.

Spam. Nope.

Well, the picture’s loading.

No, I’m not doing it. Being like, “Oh, I made a mistake”? No. Not me, because it’s not me, I’m not clicking here to cancel a transaction. And also, it’s asking for payment and shipping information. I haven’t even paid, so it’s not going to be cancelled. Just ignore it.

[Background noise, 0:32:20-0:32:44]

No, you’re not confirming anything. I can just disregard it.

[Background noise, 0:32:52-0:33:09]

‘Mineface’? No. Definitely phishing.

No, it’s fine. Legit. E-mail address good, link good.

[Background noise, 0:33:36-0:33:54]

No, I just think no one would \_\_\_[0:33:56]. I don’t understand. I think this is a scam. Download something?

[Background noise, 0:34:01-0:34:30]

I think it’s fine. DFT.

[Background noise, 0:34:38-0:34:48]

Copyright’s nice.

But I don’t like this threat. And also, \_\_\_[0:35:06].

I’ll go with no. It would be Direct.gov.co.uk. Which does DVLA. DFT.

[Background noise, 0:35:22-0:35:37]

Definitely legit. [Classic. Classic 0:35:42].

**P317**

P317: [Philip@btinternet.com](mailto:Philip@btinternet.com). “Sad news. All the money and credit cards was taken.” Peter Busheron@btinternet. “Sad news.” I think it’s definitely legitimate. “Gary Cooper. Hello, I’m Gary Cooper from Tottenham England.”

It’s definitely phishing because the email address on that Gary Cooper header from... It’s different from the email in Gary Cooper’s email signature, so that’s definitely phishing. [Noreply@ioffer.com](mailto:Noreply@ioffer.com) via ioffermail.com. “Received payment. Google Books.” This is legitimate because it’s from [noreply@ioffer.com](mailto:noreply@ioffer.com) and it’s via ioffer and noreply, usually it says, “Do not reply,” so it’s definitely legitimate.

[Adobecustomercare@adobesystems.com](mailto:Adobecustomercare@adobesystems.com). “Important password.” Yes. Adobe password, yes. “Please receive this.” Okay. Yes, I think this is legitimate because from the email and the line adobecustomercare is [email@mail.adobesystems.com](mailto:email@mail.adobesystems.com). It says here, “[Www.adobesystems.com.](http://Www.adobesystems.com.)” Adobe Systems Incorporated. I’m just looking for any other place where there is mail.adobe-systems.com, or there’s an Adobe... There’s a mail.adobe-systems domain, but I can’t find. It looks legitimate to me, so yes. I would respond to this. It’s definitely legitimate.

Plusnet Support. [support@plus.net](mailto:support@plus.net). “Your Plusnet...” Okay. “Go to Plusnet.” Yes. So there is a consistency in the domain provided email address. So from, the sender is the plus.net domain, the address is plus.net/mcafee, which references a McAfee product. “For more help, go to plus.net accounts.” So the domain is consistent, so I think this is definitely legitimate. [Frank@easyroommates.com](mailto:Frank@easyroommates.com). “You have mail. Please do not reply to this email. You have received a message from Grant, an easyroommate member.”

I’m not quite sure about this. The domain says easyroommates.com. UK.easyroommates.com. Frank. It looks legitimate. [Noreply@accounts.google.com](mailto:Noreply@accounts.google.com). Yes. Legitimate because the domain is consistent. \_\_\_[0:09:58].edu. “Click here. Your password will expire in three days. Click here to validate your email.” Why is... I’m not quite sure because the domains are not consistent, although the names are consistent, \_\_\_ It doesn’t say if this is the \_\_\_ email address.

I’d be very careful with this one. So I’m just going to say it looks legitimate but I’m just going to stay here. “Security verified by Visa.” Hmm. I’m just looking at the domain really. Visa. “No reply. Verified by Visa.com.” Legitimate. “Virgin Mobile. [Thanks@virginmobile.com](mailto:Thanks@virginmobile.com).” Yes. Definitely legitimate. Surely because it doesn’t say “Click here.” It says, “Go to our website.” So I think that’s okay. HSBC. Hmm. It looks legitimate to me. I’m going to stick with that.

[PayPal@e.paypal.com](mailto:PayPal@e.paypal.com). Email address. [1989@gmail.com](mailto:1989@gmail.com). This looks legitimate to me. It’s definitely legitimate. Blizzard Entertainment. [Noreply@blizzard.com](mailto:Noreply@blizzard.com). “Three accounts. For the investigation... If you wish to... Please open this connection.” Okay. Dynamic pathway.net. “In the form of an email...” I’m not quite sure about this, to be honest. It looks legitimate because there’s consistency between... But this .com and .net. Battle.com. Okay. Looks legitimate to me, to be honest, but, you know...

Domains are consistent. Noreply@dropbox. Legitimate. This is phishing because eBayz.com, that’s not eBay, and that’s not consistent with what’s in eBay.com. So I’m going to be very careful with this one. It’s definitely phishing. This is a very suspicious email address. The domain is not even trustworthy. This looks legitimate. It’s not asking you for anything. I-offer. It’s consistent so it’s legitimate, yes. This is definitely phishing. I’m not quite sure about this, to be honest. Okay.

“Sent to.” It’s phishing. It looks good but I think it’s phishing because... It’s legitimate because the domain is consistent. “FX Card.” It’s definitely phishing. Legitimate, because of the domain. That’s alright. “Koala Creek.” Seems legitimate. It’s not asking for any moneys. It’s definitely a phishing because the email address I’m not even sure. This is phishing. Direct GOV. Legitimate. EBay. Legitimate. Consistent domain. It’s legitimate.

This is phishing. FedEx. This is phishing. This isn’t FedEx email address. Blackpool Pleasure Beach. This is phishing, because of the wrong domain. DVLA. This is phishing, because the email address says so. This is okay, legitimate. Straight from the email address, same email address as referenced.

**P318**

P318: This is email number one. I'm pretty positive it’s phishing, because it’s incredibly vague, and it’s just providing a simple link, and it’s offering a free gift. I'm pretty sure that’s fake.

‘This is a message for all students receiving grants and loans from student loans [companies 0:00:20]. \_\_\_ fraud activities [on what is going on in student’s] accounts to allow us \_\_\_.’

Okay, second email. This also looks fake, because there’s no greeting, and the link is obviously not to Student Finance. It’s also very vague, and usually they're a bit longer than this, and have return details as well. I'm pretty confident, less confident, that this is fake.

Email number three. Again, this looks a little dodgy, simply because it doesn’t give a reason why your online account will expire. Also, they will ring you and they only give you 24 hours. Again, not as confident as the first, but pretty confident this is fake.

[Break in conversation 0:01:22 - 0:01:39].

‘Create a new password.’ That is a very long URL, and it doesn’t appear to be relevant. Yes, I don’t know why it would give you an IP address either, so I think that’s also a phishing attack.

Are these all dodgy?

Ah, this one looks more real. I will have to zoom in a bit. How do I do that on this computer?

‘Dear valued customer, you have recently contacted us \_\_\_[0:02:10].’

[Break in conversation 0:02:12 - 0:02:22].

Http… That does not look like a legitimate link. Do these people not know you can fake a link? This looks pretty legitimate, apart from the fact that the URL is dodgy. I will put that as a three, ‘slightly concerned’.

Direct.gov. ‘This is a formal notification of an important account update. Due to recently updating our database \_\_\_[0:02:55].’ Ah, this one does know you can hide a link. ‘Please fill in the requested information exactly as you have it [on your sign-in for Student Finance] \_\_\_ [payment suspended].’

This looks legitimate, except for the fact that they don’t explain why all your accounts will be wrong, and these sort of things never actually ask for your details again. It looks the most legitimate, but I still suspect it’s wrong, so I will put it as a three.

[Break in conversation 0:03:39 - 0:04:01].

[Captain FX]. Okay. This actually looks legitimate. Again, hyperlinking is always a bit suspicious, and I'm expecting that it will ask you to download something when they talk about terms and conditions, but otherwise I suppose that looks fairly legitimate, so I will put it on that scale.

At this point I'm suspecting they're all fake. Then again, on the previous one they didn’t… Can I go back? No. They didn’t mention a user name. That’s bad.

Well, there’s a typo there from Amazon. That doesn’t look legitimate. ‘If you need to return ‘an’ good from this shipment…’ ‘This shipment ‘have’ no…’ Hmm. Yes, spelling mistakes from a company like Amazon is not likely, especially two in one email. Phishing.

[Break in conversation 0:05:22 - 0:05:41].

Okay, people don’t actually get this sort of email. You don’t send an email to someone if you got attacked randomly. (Laughter) ‘£1,800.’ That’s fake.

‘Hi. Your bill to Virgin Media is [overdue 0:05:58].’ (Laughter) Ah, you don’t send a bill through a .zip, and you don’t send links. That’s also definitely fake.

Barclay’s. ‘Dear account holder.’ See, that’s not right. They would have your name. ‘We’ve detected unusual activity in your account. [Please login to online banking 0:06:23]’ \_\_\_ [IP addresses]. Again, banks will ring you before they email you. They don’t use a name, and it just sends a dodgy link, so [a two 0:06:44].

Again, the email from eBay doesn’t use the name, but I do not know if you require entering your name for eBay. There are no login details either. \_\_\_[0:07:09].

[Break in conversation 0:07:12 – 0:07:24].

The link is to something.eBay, which means it’s not actually sending it to eBay, so that’s also a phishing attack. Although, it does look pretty legitimate besides that.

Blizzard Entertainment. Diablo [3 account 0:07:38] \_\_\_. ‘Please open this connection.” That is definitely not Blizzard. They're trying to rush you by only giving you three days. That’s also fake.

I'm pretty sure these are all fake.

Random person getting donations from a terminally ill person? No. Also, how did they get your email address, if they're not just emailing it to everybody?

PayPal. ‘Your card is about to expire. Hmm. ‘Please provide \_\_\_[0:08:57].’ This one actually looks legitimate. [They add a link somehow]. It’s still not 100%, because usually they would just ask you to log in to your account rather than providing links. Other than that, it’s the first one that actually looks legitimate.

Dropbox. This is the sort of email you often get when you log in, but they would never send you a link to verify your email address like that, and they will provide your own account details when you do it, so I will put that as a three.

[Break in conversation 0:09:44 - 0:10:00].

Again, vague, but usually they wouldn’t do it like that.

[Break in conversation 0:10:05 - 0:10:18].

Once again, though, there is a spelling mistake. That otherwise looks pretty good. ‘To receive a parcel please go to the nearest [our 0:10:27] office.’ Plus, you don’t get postal receipts, I'm pretty sure.

HSBC. Again, it doesn’t provide customer information, and there’s just a random URL link. It doesn’t provide any RSVP details either, so that’s pretty dodgy.

Visa. ‘Dear valued customer.’ Again, no name. Dodgy link. Trying to rush you. Yes, that’s phishing.

Google. Two attachments. Someone recently [tried to sign into 0:11:35] your Google account. \_\_\_ account \_\_\_.’ Well, the URL actually looks legitimate, but why would they send you a [PNG and a 0:11:54] JPEG? Hmm.

[Break in conversation 0:11:58 - 0:12:21].

Why would you put, ‘To view this message in another language please click here’, in English, for Adobe? If someone had hacked into Adobe I would have probably heard about it at some point. Everyone has Adobe. The URL looks legitimate. Adobe.com. Mentioning phone scams feels ironic.

[Break in conversation 0:13:02 - 0:13:17].

It looks fairly legitimate. I don’t think it happened, but I will give it a four.

‘Hello.’ Email from a bank that doesn’t mention your name. Vague. The URL is legitimate, NatWest.com. It’s actually spelt correctly. It’s a common thing to just slightly misspell the URL. Also, I think it is possible to have a URL but have it actually link somewhere else. Other than the lack of name in the email receipt, this actually looks legitimate. I will give it a five. Ah, I will give it a four.

\_\_\_[0:14:25] opened. From HR Recruitment Department, and the email is [hrdep33433@yahoo]. Yes. (Laughter) ‘Dear Applicant.’ No name. \_\_\_[0:14:43] [inform you, you made my] shortlist. ‘We’ and ‘my’. That’s a bit of a… \_\_\_. No space. \_\_\_. Yes, dodgy URL. Asks you to email back, but doesn’t provide an email address, other than this weird Yahoo one. Yes, that’s phishing.

(Laughter) A link to Facebook. No. ‘Confirm contact information.’ That’s basically a Facebook scam. At least it uses your name though.

[Break in conversation 0:15:48 - 0:16:07].

[Hang on a minute]. Yes, that’s not right. Invoice number, eBay. [Automatically generated 0:16:25] \_\_\_ [reply] \_\_\_ [Helen Jones], eBay invoice for your period \_\_\_ PayPal.’ It has a name. That’s a good start. \_\_\_. The URL looks legitimate. \_\_\_. It is asking you to sign in though.

Ah, well, this actually looks legitimate. I don’t have an eBay account, so I don’t know what they look like. (Laughter) \_\_\_[0:17:02]. It does look legitimate. I will put five. It looks legitimate, but I'm paranoid.

‘Please do not reply to this email. Follow the link below to…’ Yes, no. From frank@easyroomate.com. No.

\_\_\_[0:17:35] download. Yes, you get McAfee with other bits of software. They don’t need to email you. ‘[Login] to your account, username, [portal plus].’ No.

‘Your password will expire in three days \_\_\_[0:17:58] now. (Laughter) [O2]. Thanks, system administrator.’ Dodgy email. No.

Who falls for these, really?

‘Dear Guest User’. Dodgy URL. ‘Thank you, [ioffer].’ No.

PayPal. ‘If using PayPal to see all the transaction details login to your PayPal account. It may take a few moments for this transaction to appear in your account.’ \_\_\_[0:18:40] PayPal. Yes, this looks legitimate. The description [looks about] right. It’s not sending you to an URL \_\_\_[0:19:04] transaction. That looks legitimate.

PayPal again. Yes, PayPal wouldn’t send a login button on email. Big companies don’t do that. There are usual adverts. Let’s give it a three.

‘Dear Candidate, \_\_\_[0:19:43] website. Please \_\_\_.’ Dodgy URL. Dodgy email address. No name. Second dodgy URL. Also very vaguely worded and short. Phishing.

iOffer. ‘Congratulations from Google Book.’ No name. [Invoice 0:20:08]. ‘Click here to cancel the transaction.’ Yes, deliberately vague. Something that people wouldn’t buy.

‘Dear Pleasure Beach Visitor.’ Why would you go to Blackpool? \_\_\_[0:20:30] [development]. Why would you get an email for visiting Blackpool Pleasure Beach? ‘To enter the survey…’ Why would someone actually click on that link if they didn’t go to Blackpool? Then again, if people are stupid enough to fall for the other ones… I'm pretty sure it’s phishing though, especially because the URL is dodgy.

DVLA. \_\_\_[0:21:08] dft.gov.uk/dvla. I'm pretty sure that DVLA is the first part of that URL. \_\_\_. Again, it’s one of those ones where they will already know your details. You don’t have to re-enter them. And they don’t have your details. Phishing.

‘Dear Student, welcome to Lancaster.’ Oh, it’s from a .Lancaster@ac.uk address. That’s a good start. \_\_\_[0:21:46] university. It doesn’t have your name in it, though, but if they're sending it to many people [like that].

‘[We’re interested in how you chose] \_\_\_. Please complete this short survey.’ It wouldn’t be at SurveyMonkey.com, would it? ‘Please note \_\_\_[0:22:03]. Any queries…’ Well, apart from the URL being off, that looks alright, so I will give it a three.

**P319**

P319: Okay, so, I have been given a [false 0:00:03] e-mail, and it says, ‘Pension.’ Okay.

We have a full safety target with every community. Hmm. To me, it looks like more of a legitimate e-mail, because generally these websites and the community related to Amazon and eBay, they keep sending you such kinds of e-mails to make sure that the user has got their authenticated rules and everything.

Okay, so NatWest. It says that your last statement for the account ending, access their sale, just log on too.

Hmm, okay, generally the e-mails from NatWest are something. It’s a kind of updated e-mail, but trust me, out of my experience, I don’t trust such kind of e-mails generally, because most of them are phishing e-mails. If somebody knows the [end digits of your 0:01:17] ATM, they can easily generate such kind of e-mails. So I will mark it as a definite phishing e-mail.

Okay, it again goes to Barclays, and, ‘We have flagged a logged on your account.’ Ah, that’s fine. Whenever you try to log in from a different device or a different account, the mobile banks, they keep warning you about this change. So that, to me, sounds like a definite legitimate e-mail.

Hmm. Uh-oh, Google mouse, malware 101. I just hate such kind of e-mails. I remember, I have been told that I got £10,000 draw money, God knows from what, and I never liked such e-mails. Because they generally are from awkward e-mail addresses, like I-offer blah, blah.

So for me, yes. If I won something and I’m not sure about it, definitely it’s going to be a phishing e-mail, so I’ll mark it too.

“Dear Miss Jones, thank you for choosing…” Oh, blah. Hmm, that’s fine. So the same thing where they generally send it to you. If you have made a new account and they just want to make sure that you activate the settings. So for me, that’s a legitimate e-mail.

Hmm. I like Facebook notifications, because they keep updating you about what’s happening around you. So that’s a definite legitimate e-mail.

Mmm-hmm. Okay. That’s a little bit risky, because it says it’s a bit about a Virgin Media mobile, and sometimes yes, you can get such kind of e-mails if you are using any of such things. But to me, I will put it in phishing e-mails, because half of the time they just want to make sure that they get your identities and all the ID values, which can affect you.

Mmm-hmm. This sad news of Philip Bertrand. It reminds me of an incident when I have been told that someone with a similar surname has sent me a good amount of money, for which I didn’t even know. So yes, it’s a definite phishing e-mail. Just to make a fool of people around them.

Hmm. Virgin send you such e-mails to make sure that the user has got updated accounts. Hmm. That’s a definite legitimate e-mail, Dropbox. There are Mega and Skydrive. They keep sending you e-mails to make sure that you have your proper e-mail addresses.

Mmm-hmm. Okay. It is a little tricky again, because generally when you’re making a transaction and your Visa card is not responding the same way, one of the reasons can be that probably, it is actually from a bank telling you that something has happened with your e-mail account.

But most of the times, it’s the bad people who make a user feel innocent, so I will mark it as a ‘Three’ and I’m just giving them the benefit of the doubt. It’s a kind of warning e-mail.

I just hate these administration team e-mails. “A terror treatment development.” Okay. Hmm. These are like typical job application e-mails, which should be taken as a legitimate e-mail. Most of the companies really apply something for them. And they keep asking you a lot of questions. And yes.

Hmm. I don’t know. I never update anything when it asks me that, you know? It’s a kind of security staff and something. So I will like it.

Hmm, yes, I like such e-mails. This is a legitimate member e-mail. When I was looking for a new house in town, it kept sending me early.

Okay. That can be tricky, again, because sometimes if you have irregular transactions, HSBC, they do suspend, block your account, so a good couple of minutes. So, it depends.

Hmm, that’s okay, because once you use the account, they want to know all the information you have been using for a number of years, and that just gives you a total of what you have been doing and how it’s going to help you.

This Amazon stuff, it’s a good e-mail because it’s telling you you have ordered something, which costs a specific amount of money, and this e-mail is just a notification to update you for something which is coming along.

Okay. If you are doing, I’ll again give them the benefit of the doubt. If I am someone who actually wants to change the password of this, and this extra card, it can be responsible. But mostly, you never know when it’s someone else who’s just trying to change the password and trying to use the same card. So, yes.

I don’t like phishing mails. That’s always…

That’s FedEx. Hmm. Okay. That’s one of the loveliest e-mails you’ll receive, especially on your birthdays and the special occasions you actually want to get something. And you’re just sitting and waiting for the e-mail to come.

Mmm-hmm. That is rubbish, because in my knowledge, if your password is expiring, they can’t ask you for e-mail, because sometimes the people, they still know your e-mail, and they can actually change your password, you know? Yes. So…

Okay, keep going. Mmm-hmm. It’s on behalf of Dell. Mmm, hmm, hmm. So that says that I have changed the legitimate certificate and I cannot give this to anyone else, which is fine. I can receive such kind of e-mails.

That’s fine as well. Okay, you get, like, sometimes they do send you e-mails but with such a proper layout that you don’t even feel a difference between why you’re deleting or putting in, ‘Legitimate,’ or the phishing side. Even in the worst notifications that I have to download, this is money from my bank, this is a legitimate e-mail.

Which actually warns you that something has been taken out of your account. That’s fine. I would count it as a close legitimate, because sometimes if your password is expiring they keep sending you reminder e-mails, just to notify that, you know, something’s going to happen in a day or two.

So again, the payment e-mails for me are all legitimate e-mails. Because they give you an exact figure of what is going to happen.

I don’t like that e-mails, in which there is improper information about what you’re going to buy. Okay. Hmm, hmm.

I’m giving the benefit of the doubt to this by giving it a, ‘Four,’ because they do ask you to change the password. I’m not sure that they do this in an e-mail or not. I don’t remember. Except this [chemical brain 0:11:15] was deserved to establish spam. Half of the e-mails I just see and delete them for nothing.

Hmm, hmm. I have a plan to go with their survey. Mmm, hmm. It’s a legitimate e-mail, because when you plan a journey for something, they expect you to give them a feedback so that they can improve it for further use.

You’re not supposed to fill in all the details if you receive an e-mail saying it’s from the Government and blah, blah, blah.

Okay, this [a fester 0:12:04] e-mail, I would like to give it a, ‘Four,’ because I have been filling a lot of forms for the past year, but I never get anything, so I don’t know. Is that fine to be asked or put it in the legitimate side or not?

**P320**

P320: Okay, I think this is quite legitimate, because I’ve seen Amazon emails before, and they usually send stuff like this to you when you’ve just bought something. Yes, it also has the address, a shipping confirmation, and, “your order’s link,” which means you could click on that to check that it links back to your Amazon account. So, I’m going to go with definitely legitimate, especially because a TV would probably cost around £360.

Okay, this looks like phishing, because I don’t like the look of the email address, and there is no sort of logo from the student’s loan company, and there is no name at the bottom; it just says “yours sincerely”. I don’t like the look of that link, either. That doesn’t look like a legitimate link because it’s got loads of random letters and numbers and words, and it also doesn’t address the person it’s being sent to, which shows that it could be a computer instead of a human, so I’m going to put… Maybe number two.

Okay. I can’t actually read this. It’s quite pixelated. Let’s see if that works. Okay. Okay, this looks a little bit more legitimate than the last one, because I can see a Dell logo. However, I don’t like the look of the email address. It doesn’t look like a legitimate server. It says “mailto.raptnsonline” which doesn’t sound promising. “Dear valued customer”; it should probably say “Dear Helen”. And again, “The Dell team”, I’d want a name of the person to know it’s trustworthy; maybe a phone number as well so you can ring them, but none of that information is there, so I’m going to put number two, just because there’s a logo, but everything else seems a bit illegitimate.

Okay. I don’t like the look of this, because when you pay for your phone bill, they usually text you; I don’t think I’ve ever received an email. There’s also no name for attachment, which I don’t like. But the look of the email address looks quite genuine. But then again, there’s no addressed to “Helen”, so I think I’m going to put ‘two’.

[Background noise 00:04:37 – 00:05:13]

Again, there’s no logo, but there is an address to “Ms. Jones”, there’s also a link to the website at the bottom. I also like, the email address looks quite trustworthy as well, so I think… But then again, everything’s very spaced out, and looks… I don’t like all these links either. But then, there are two to… Okay, there are four steps, but one of them… There are two that are both “number two”, so that’s a bit untrustworthy, but the fact that there are steps to view instructions makes it more legitimate, so I think I’m going to go with ‘four’.

Okay. First, looking at this FedEx one, it looks quite genuine because you’ve got the logo. However, I don’t like the look of the email; it doesn’t look very genuine, and it has no relation to the company. It says “Fort Wayne”, whereas the company’s FedEx, which doesn’t make any sense. I also don’t understand why they would send you an email at half midnight, that’s odd for a company. They would usually work 9:00 to 5:00 if it was a human sending this email.

There’s also an error in the email: there isn’t a space between “hour” and the “dot” after “December 7th”, and there also isn’t much information in it as well which makes me think that a computer might have generated it, so I’m going to go with definitely phishing.

Okay. Okay, I don’t like the look of this, because… Okay. I don’t really know where this email’s coming from, it just said “your password”, but it’s not addressed to anybody, which seems quite a generic email. I don’t know who Shaun is; [where he’s based at 00:08:27]. It just says “Thanks, system administrator.” So, you would think it would say “Shaun” at the bottom there, which it doesn’t; it just has a general job. So, I’m going to put definitely phishing. There’s also no company logo or anything that would make it more legitimate.

Okay, this looks very trustworthy, because we’ve got the Barclays logo at the top, and we’ve also got a name of a person at the bottom, “David Brown”, so we know that we could possibly try to contact him if in doubt, so look for a David Brown at Barclays and see if he actually works there. There’s also one straightforward link as well, instead of a load of busy links. The only problem is, I don’t like the email. It should probably say “@Barclays” or something instead of “vnet”. However, I think I’ll put ‘five’, because it looks quite trustworthy otherwise.

Okay. Okay, first look at this, we’ve got a logo; but when you look at the email address, there are two Es in ‘finance’, which makes me think that it’s a sort of parody email address to kind of slip people up. So, some people might not notice that extra ‘e’, so think “Oh, this is genuine.” If they recognise the email address. But, with that extra ‘e’, it makes me think that it’s definitely phishing. I also don’t like the look of this “Please do not reply to this email.” At the end, that looks quite ‘spam-ish’ with all those stars. I think, “public services all in one place”, I don’t know if that’s the correct sort of motto for Directgov, so I’m going to put definitely phishing.

[Background noise 00:11:39 – 00:11:50]

Okay, this is definitely phishing, because in the “from” section it says “Gucci, Cartier and Rolex” which is kind of trying to trick the customer into thinking that they’ve won maybe a Gucci product, which is unlikely from Yahoo. I also think the email address looks very untrustworthy; it’s just a load of random letters. Again, the timing that this email’s been sent is quite… Oh, no, sorry. No, that’s in the morning, forget that. Yes, no address to the person receiving the email, and… Yes, I don’t believe someone would just give away a watch for free, that would just never happen. There’s also no legitimate company displayed on here, just basic info, so that’s definitely phishing.

Okay. This looks quite trustworthy. We’ve got the NatWest strip at the top, and I know that bank accounts do often send things, warn you that it will expire. However, the email address doesn’t look very related to NatWest. There’s no address to the customer, and there’s no name at the “Yours sincerely” section, so I think I’m going to go with ‘three’.

Okay, this looks very trustworthy, because at the bottom right hand corner there’s a copyright symbol with 2012 and Dropbox, so that looks quite trustworthy. We’ve also got the Dropbox logo at the top. There are also the Dropboxes in the email, which makes it very trustworthy, and we’ve got an address to “Helen”, which looks, again, trustworthy. So, I’m going to go with definitely legitimate.

Okay. A lot of these emails seem to have been sent at the exact same day and time, which is strange. Again, we’ve got an address here, like an actual, physical address, and we’ve got something at the bottom here about the Newcastle Building Society, I think it says, and the email address matches who it’s from. We’ve also got MasterCard with a copyright symbol next to it, and then we’ve got a logo, so I’m going to go with… Hmm. I think I’m going to go with ‘five’, because I’m getting a bit suspicious about that date, that it’s all the same.

Okay. This is very strange, because someone appears to be posing as the NUS, and I don’t believe that they would send a link like this to someone, it’s too long. It’s one, two, three, four, five, six lines long. Yes, the link’s far too busy for it to look genuine. However, the email address looks quite trustworthy. But again, there’s no address to the recipient of the email, and there’s no NUS symbol on it, no NUS logo, which, as I receive NUS emails myself, I know that they do include that, so this email just looks like someone trying to pose as NUS to scam students, so I’m going to go with definitely phishing.

Okay. Okay. This looks quite genuine, because there’s the PayPal logo at the top, and I receive stuff from PayPal. There’s just something about the font that doesn’t look right, I don’t know why, and sort of the way it’s set out doesn’t look quite right. The email address looks quite genuine, but I don’t know if PayPal is… Oh, PayPal Europe, hmm. I was thinking about .co.uk, I thought it might have been an American company, it might have said “.com”, but it does say at the bottom, “PayPal Europe”. So, that looks quite genuine.

We’ve also got an address to the recipient of the email, and they also appear to know the last four digits, whereas I think that a spam email might try to trick you into something with more numbers. Hmm, it’s hard. Again, this one’s sent at the same time as some of the others, and the same date, same year, same time. So, that makes me think there might be an infiltration of spam emails being sent all at once, so I think I’m going to go with ‘three’, just because I’m suspicious about that date and time being the same. But the email address looks quite genuine, and some of the things inside the email as well.

Okay. The first thing I notice here is the email address. It looks very ‘spam-ish’ because of all the random letters and numbers. I think they would have more of a professional-looking email instead of just random numbers and @yahoo.co.uk. I don’t think a recruitment company would put that many arrows next to a link, that seems quite aggressive. And “Adam French” doesn’t seem to have a job title at the end, and usually people at companies put their job title so that you can possibly look them up to check that they are actually a person.

Again, “Dear Applicant” is quite general, instead of “Dear Helen” which would make it more trustworthy. Also a few grammatical errors in this as well, which I don’t like.

There are a lot of spaces between things. Yes, it’s very depersonalised. I think if you were going to an interview it would be more personal, so I think I’m going to go with definitely phishing on that one.

Okay.

[Background noise 00:22:14 – 00:22:31]

Okay, I’ve definitely received an email similar to this, saying that there’s money for me somewhere over the country or the world, which it just wouldn’t happen. That money would go to the person’s family, not just a random person. They obviously wouldn’t just randomly choose you as a trustworthy person when he doesn’t know you. I don’t like the look of the email address. Why would the subject be confident? If you were in hospital with lung cancer, terminal lung cancer, you would not be worried about where…

You wouldn’t be worried that your money would be going to orphans; you would be so ill you wouldn’t be able to send an email like this, so I’m going to go with definitely phishing, just because I’ve also had personal experience of people sending emails like that, saying I’m about to inherit millions. It just would never happen.

This is definitely phishing because someone’s trying to pose as HSBC, and that is not what HSBC’s logo looks like in the slightest. And yes, email address doesn’t look legitimate. No. Don’t like it. It’s the logo that’s throwing me off; it’s not the right logo, so definitely phishing.

[Background noise 00:24:40 – 00:24:57]

Yes, this one’s definitely phishing. They’ve even put at the end “beware of scams”, so therefore it makes me think that it is a scam, because why would they feel the need to write that if the email looked trustworthy? You would never get an email asking you for a roommate. I don’t like this tab at the top at well that says “Please do not reply to this email.” It looks quite aggressive and ‘spammy’. Yes, I don’t like the look of that link either, it looks a bit busy. Very strange content. You would never send someone an email saying “We’re helping you find the right flatmate.” It’s just strange, so I’m going to put… It does say “Hi Helen.” So, hmm. I’m going to go with ‘two’.

Okay.

[Background noise 00:26:21 – 00:26:44]

Okay, this looks genuine, because this PayPal one… Because “seller” matches the “from” at the top, and “service@paypal.com” looks like the correct email address that you would use. I’ve also had loads of receipts and stuff like this before, and this looks very familiar. Yes, the email address from the seller is exactly the same at the “from” section. It’s also got the… Oh, ‘unconfirmed address’, that’s strange. Department of Psychology, Lancaster University, looks like the right email address as well, so I think I’m going to go with definitely legitimate for that one.

[Background noise 00:27:47 – 00:28:03]

Okay, this looks quite genuine, this Visa email, because of the email address. But then again, there are some grammatical… Oh, no. Oh no. Like the copyright at the bottom that says “Copyright verified by Visa, all rights reserved.” You’ve got the copyright symbols as well, which looks very trustworthy. There are no ‘spammy’ looking links, they’re all just simple ‘click here’ instead of loads of random letters which makes me think that they would take you to an obscure place. Again, this date, this day keeps popping up, I don’t know why. But yes, I think this looks quite trustworthy, for this I’m going to put maybe ‘six’.

[Background noise 00:29:16 – 00:30:05]

This is definitely, definitely spam. You would never get an email to a person that isn’t affiliated to a loan company just asking for money. It also doesn’t say “Hello, Helen.” It just says “Hello” which looks like a quite generic email that’s been sent to a lot of people. Yes. Strange content. The police would also deal with this. It wouldn’t be appropriate to say that you’ve had a “robbery attack” to a random email address. Yes, you would be contacting a loan company for something like this, not just a personal email address, so definitely phishing.

I can’t actually see this, the writing’s all blurry and small. eBay… I don’t like this, because there’s no eBay logo on the email, but everything else looks quite… Hmm. The email address looks familiar and trustworthy, and we’ve also got the copyright at the bottom which looks trustworthy as well. It also has the eBay link directly here, the genuine, that’s the genuine website address, ‘eBay.co.uk’, that’s definitely eBay’s genuine address, so the fact that that is in the one, two, three step of how to view your invoice is quite trustworthy, as well. But then again it says at the bottom “Protect yourself from spoof/fake emails” which is a bit strange. I think I’m going to go with ‘four’ for that one.

This is a very strange email address for this Gogglebox UK one. There’s no copyright at the bottom as well, or logo, which doesn’t look trustworthy, so I’m going to go with number ‘one’, definitely phishing.

Okay, this is definitely not Facebook. Again, no Facebook logo. But then again, they’ve got “Hi, Helen, the Facebook team…” and the links seem to go directly to Facebook links as well; but there’s just something about that email address and the fact that there’s no Facebook logos on the email or copyrights makes me think that it could possibly be phishing. So, I think I’m going to put ‘two’.

Okay, this eBay one looks more genuine than the others, but you have got a logo, but I don’t like the email address, it says “admin@eBays.com” Why would it say “eBays”? It would just say “eBay”. But then, we have got copyright at the bottom. It says it’s trying to suspend the account. I feel like eBay could do that. This is a hard one. I think I’m going to go with ‘four’.

So, HR recruitment team. Got some very questionable links here that match the “@igrasp.com” on the email, which is strange; it makes me think that it’s the same phishing server. Again, HR recruitment team, that’s quite a vague company to work for. Which company am I… It says “organisation send” I don’t know if I like the look of this. It doesn’t look like a genuine organisation, so I think I’m going to put a ‘three’.

Okay, there’s a Google one here. So, this one looks quite genuine, because we’ve got the Google logo at the top. We’ve got Helen’s profile picture at the top of the email, and we’ve got “Hi, Helen” as an address to the recipient. Yes, we’ve got copyright information at the bottom. I would think the email address looks quite genuine as well. There’s also quite a clear link to reset password instead of a random link that looks quite ‘spam-ish’. It also warns that “If this is you and you are having trouble accessing your account, please complete the troubling steps listed at…” which is supported at Google’s genuine website, google.com, so I think I’m going to go with definitely legitimate.

Okay. “Congratulations, you have just purchased an item from Gogglebox.” This looks quite similar to an email that we’ve already seen, which makes me think that it’s spam. And I don’t like the look of the email address. “ioffer.com”, there’s no copyright at the bottom as well, so I’m going to go with definitely phishing.

This Adobe customer care looks genuine; the email address looks trustworthy. It actually says “adobesystems.com”. Again, same date, 8th October 2013, 11:50:37. That date’s coming up quite a lot, as opposed to the others, which is strange. However, at the bottom we’ve got the copyright information, we’ve got the Adobe logo, we’ve got “click here” instead of click on a questionable link that’s very long. Yes, the links look quite genuine; they’re similar to what you’d see on genuine emails, so I’m going to go with definitely legitimate for that one.

Blizzard Entertainment. Hmm. “Greetings” – strange. This is a strange one. Again, there’s no company. I don’t know what… Blizzard Entertainment. There’s no Blizzard Entertainment logo. There’s a very questionable link here that’s very long and includes random letters and numbers and symbols, which makes me think that it might take you to a spam website. “We will send this package…” That’s strange. Why would they send that in an email? I’m going to go with definitely phishing for that one. Strange content involved. I don’t know what “Diablo” means either.

There’s a NatWest here. This looks very genuine, because of the email address and the logo being there; but there’s no copyright at the bottom. We’ve got “Chris Popple, Managing Director, Retail Banking.” So they’ve got a name and the job title of a person, which seems more believable. It also recognises that the account ends in 801, which is different to another email, so unless you changed your bank card, then…

Okay, that’s strange. Oh, that’s the account instead of the card. Hmm, maybe that’s okay then. Again, we’ve got links that would take you directly to the website instead of random long links that look ‘spam-ish’, so I think I’m going to go with definitely legitimate for that one.

Okay, PayPal. paypal@epaypal.co.uk – that looks very strange. I don’t like the look of that email, it looks a bit complicated. However, it says “Dear Helen Jones” and the correct email address is on the actual email. The PayPal logo looks legitimate; it’s got copyright at the bottom of the email. But again, 8th October 2013 11:50:37 – why have so many emails been sent at that time from all these different companies? So I think I’m going to put ‘five’.

Team at Blackpool Pleasure Beach. Okay, first of all, the link that they’ve sent for the survey has nothing to do with Blackpool Pleasure Beach, so I don’t like the look of that; same with who it’s from. It’s not from anyone at Blackpool. It also just says “The Blackpool Pleasure Beach team” instead of an individual person, and “Dear Pleasure Beach visitor” not “Helen”, which isn’t personalised enough. I’m going to go with ‘two’, almost definitely phishing.

DVLA.

[Background noise 00:46:16 – 00:46:30]

Info at [TFT]. We’ve got a postcode at the bottom, the copyright symbol. The link as well looks quite genuine, because it says “verification” in it, which is the content of the beginning of the email. We’ve also got a logo, which I think looks like DVLA’s logo. I think I’m going to go with ‘five’ for that one. It looks genuine but there’s something not quite right about it; maybe it’s the fact that it’s not addressed to Helen.

Okay. This is one from Lancaster. It looks like a genuine Lancaster email address. I don’t know who Ross Malcom is, which would have helped if I did know. “Faculty of Science and Technology undergraduate survey.” “We hope you enjoyed your first weeks at Lancaster.” Hmm. If Helen is PhD, why would she have been an undergraduate in 2013? Or fresher, maybe. It says “first few weeks”: you would have been a fresher, which is odd. But then again, Lancaster do send irrelevant emails out, so, hmm, maybe ‘five’.

**P321**

P321: \_\_\_[0:00:00] so what’s the \_\_\_? The email address is directgov@slc.co.uk, so @slc is not a governmental post address which means it should be .gov. Chances are this is a phishing email. "We have detected fraudulent activities going on with student loan accounts." okay, they wouldn't be asking you to update the database. No, this definitely is phishing. [mindphase.com 0:00:51] sounds very odd although .html seems a bit more legitimate. It was sent at 11:15am, that doesn't seem too bad. The subject is interesting because students \_\_\_[0:01:11] this season. That doesn't sound formal.

Next, so it's PayPal to Keith \_\_\_. With PayPal there's normally phishing scams. "Hello," so it's addressed to no one. When it comes to the hello, it's not hello person, which seems fairly odd. There's an eBay sign though which could just be copied and pasted. Transaction ID though and shipping details, RUSPS. Whatever it is, it's a watch for £149.14. "You sent a payment to an address at \_\_\_[0:02:20] Music," which doesn't sound like a watch company. It seems fairly normal though. I haven't used PayPal personally so I don't know for sure so it might be. I'd say it was more legitimate.

Next, so it's Philippe \_\_\_[0:03:01]@btinternet. It sounds odd, "Sad news, Philippe \_\_\_". This automatically looks odd; "Hello, I'm sorry for reaching you rather too late, the situation..." That automatically looks like phishing. I mean the first sentence, no one would send an email to a random person. It's sent to a Gmail account which means it's personal. They'd have to have that email address. "All we need is £1,850," that seems very odd. It's definitely phishing.

Next, okay, so Virgin Mobile, "Your mobile bill dated 8th October." There's no name for the attachment, that could be a sign of a phishing email. Normally, I'm guessing, Virgin Mobile don't send attachments in the bills because they'd normally have a website where you can deal with this. There's no link to that though. "Hello, the bill for your Virgin Media mobile is now ready..." is now, there's a spelling issue there or like a grammatical issue, "Hello, the bill for your Virgin Media mobile is now and ready to view."

They've got a link to send us an email. "Our team won't be picking up emails from this address so if you'd like to email us back, head over to our website to send us an email." It looks fairly phishing because there's a few issues with it but I wouldn't say it was definite.

Next, so Gary Cooper, it's @[aviso.ci 0:05:10], that automatically looks odd. I don't know what .ci is. The subject is confidence; "Hello, I'm Mr. Gary Cooper. I was born January 13th 1953 in London, England. I'm in a medical institution in Italy where I'm writing you. I suffer from lung cancer." It sounds okay so they're asking for something. It's definitely going to be phishing.

Next, so it's from Carla Craig and it's subject is "Apply \_\_\_[0:05:51]," so it's an Amazon one. "Hello, Helen Jones 1989," so it looks like it's log in, user name. I've seen Amazon.com confirmation emails and this looks fairly standard so whatever it is, they've ordered a large TV and the price is £359.99. It looks okay. I would say that seems very legitimate.

Next, so it's from Barclays. It's from Barclays online but it's not from the Barclays website "Important account notification. Click here to verify your account records." No, they would never ask you to do that so it's definitely going to be phishing.

Priority mail postal service, yet it's Fed-Ex and the Fed-Ex logo looks terrible. Tracking number, get postal receipt, "To receive a parcel please go to the nearest our office," again, another grammatical error, "and show this postal receipt, get postal receipt. Best regards, the Fed-Ex team." It seems okay I guess but it's too odd to get a postal receipt. "Our post driver was unable to deliver a parcel to you." Would they send an email for this? No, I think if you click on that get postal receipt, it could be a link to download seeing as it's from someone at fortwing.com, that's probably definitely going to be phishing.

Next, okay so it's from Dell, from TMS on behalf of Dell Inc. It's a weird app, Dell survey help. The subject is "Dell customer experience survey invitation. "Dear valued customer," junk email but it might not be phishing. "Thank you for your recent contact with Dell Support. To complete the survey..." Okay, yes, I wouldn't say it was phishing, it seems legitimate but it's just going to be a junk type thing.

I would be more certain if I was the person and I'd had some sort of communication from Dell. "To be removed from this list, reply with remove in the subject line or click here." That looks legitimate because it could just be junk email but it's not phishing.

Next, so it's from Plus Net Support, support@plus.net. "Your Plus Net Protect software is available to download." Again, I haven't used Plus Net as my service provider. "Dear Miss. Jones. Account user name, Helen Jones 1989," that looks fine based on the email address that it's been sent to; Helen Jones 1989. Helen Jones 1989 seems like a reasonable thing for the person to do.

"Follow the instructions to get your software up and running." Most internet service providers will give you some sort of internet protection so this doesn't look like they're trying to phish. It's got a reasonable phone number and the website looks fairly legitimate so I'd say this is legitimate.

Next, so it's from iOffer, "Seller received payment. Dear guest user," so you're a guest user but you've received a payment of some sort. "Goggle Box UK has received your payment regarding the item [History Man 1989 0:10:40], four part miniseries for ITV on DVD" It's from iOffer.com so it's not a doc zip file. The link that they're sending you too seems normal but why would you go to iOffer?

Automated emails normally happen when you get a payment online received. "Click below to view the status of your purchase." It would have been nice to have some sort of images from Goggle Box UK or iOffer from the website so it could be phishing but then again it could just be an old website. I wouldn't be too sure but it could be legitimate.

Next, so it's student finance. This one has got @directgov.uk, which is the normal website extension or email extension. "Student Update" is the subject. "This is a formal notification of an important account update and avoiding this payment." Why would they do that though? Surely they'd get in touch with you direct. "Click here to validate your information." There's no hello person/name so it just seems odd.

"Please do not reply to this email as this address does not accept incoming emails." Student Finance ER but that's Student Finance England. "Please fill the requested information in exactly as you filled it when you signed up for student finance." I can't remember, not having used directgov services for a while or student finance things. It could be phishing.

Next, so it's billing at eBay.co.uk. I don't use eBay. There's no logo but there's a copyright for eBay. I would have thought that eBay would send a logo in their email. "Your eBay invoice, " all the web addressed look legitimate though and there's no direct link that they want you to click on. It's all through eBay so I'd say that was legitimate but again, there should be an eBay logo.

Next, it's from NatWest but the extension is at \_\_\_[0:14:22].com. It automatically looks like phishing. "Log in to online banking and ensure your credit card is up to date. Your account will be disabled," so there's a threat there if you don't do something now. Banks normally wouldn't give you that sort of stress to do something, especially through email so it's going to be definitely phishing. It was sent on 8th October but your account will expire on 3rd June, definitely phishing.

Okay, nusextra.co.uk. "You or someone else entered this email address to change a password to reset your account. To continue to the password rest process please proceed to this link." It's from an nusextra.co.uk web address. I can't see the NUS logo but that seems like a reasonable thing and the web address it's sent from looks normal. I think it's the IP address. You can always check your IP address if you think it's phishing but I'd say it's legitimate.

Next, ah, from NatWest again, onlinebanking@information.natwest.com, "Your latest statement is available online." I don't use NatWest but these are normal I guess for monthly statements. The website links at natwest.com/your statement. There could be a hyper link underneath that looks different but "In your account ending 801," so you could always check your bank account details if you're unsure but it looks legitimate.

From eBay again but it's @ebayz.com with a z, that's very odd. "Dear Valued eBay Member. Per the user agreement," this looks really odd. It's got the eBay logo on, eBay suspension. "To update your eBay records, click on the following link." Again, it's @ebay.com but it looks too weird and again, there's "Please update your records by 10th December," which is another stress on the time that you have to do it. It was sent on 10th December so it's probably going to be phishing.

From Dropbox, noreply@dropbox.com. that would be a hard email address to get; "Hi Helen, Dropbox needs to verify your email address before you can check folders." Dropbox do that normally if you were going to do that, based on my prior knowledge of using Dropbox; "Verify your email address." These are normally straight after you would do it so if you were using Dropbox for this purpose and you got this email, it wouldn't be a surprise. If this came out of nowhere then I would think it was phishing but it looks too normal to be that.

Next, so seantgranata@\_\_\_[0:18:24], "Your password expires in three days." Why is it from Sean T Granata though? "Upgrade web mail 13. System administrator," it should really sign it as Sean T Granata though but \_\_\_ University? I think it could just be that they visited the university but why would the website - I couldn't say for sure but unless you know yourself if you visited \_\_\_ University before this and you've had some sort of service then it might seem more legitimate.

Next, so HR recruitment department job application form. "Dear applicant, thank you for your interest in our new role we have opened. My name is Adam French and I'm the HR Manager. Once the file is downloaded please ensure you double click the application form to be able to open the file and fill out the application form." They say application form an awful lot and it's in capital letters, "Yours sincerely, Adam French. Please click the link to download the application form."

They don't specify the new role. What is this role? Hrdepartment@yahoo. There's no sign of what the actual company is. "Please do not hesitate to contact me by email," that seems different to normal but normally they'd give the email address there. "I'd like to inform you you have made my shortlist." No, this seems too weird, too personal but broad personal.

Next, it's from Facebook, @facebookmail.com. Facebook contact email address confirmation. There should be the Facebook logo if there was a Facebook related thing but the website addresses look fine. "To confirm your contact email address, follow the link below; try copying and pasting it into your browser," so that should remove any odd hyper link underneath. That looks fine. "If you did not enter this address as your contact email, please disregard this message." Normally you would say the opposite if it was phishing so it's definitely legitimate.

Next, so it's from [Caxton FX 0:22:12] cards via \_\_\_.co.uk. "There's and conditions update. Changes to the terms of conditions of you Caxton FX prepaid Master Card. Please take the time to read your updated terms and conditions which are available." I don't know what Caxton FX is. If I had some sort of credit card from them I'd know but this would be interesting. It is only terms and conditions \_\_\_[0:22:40]. Everything else looks fine. It's got an address of the place so you could always check them out online if you were unsure.

Next, "Gucci, Cartier, Rolex., get ready for your luxury fix," no, I don't want to have that, definitely phishing. "Good day, give your loved one a luxury watch today. Good luck," why good luck? "Click here," no, too many clicking.

Next, easyroommate.com; "You have received a message from Graham \_\_\_[0:23:27]," \_\_\_ I don't know why people would send you a phishing mail from that. "Beware of scams, do not send money by Western Union," so they're warning you about suspicious scamming. The easyroommate.com website looks fine, based on the fact that I've used it before. "Click here to see the messaging profile." This is normally what they look like.

Next, security verified by Visa. "Dear valued customer, your credit card has been suspended because an error was detected on your credit card information. The reason for the error is not certain." They should know, it's an error. "Security reason, we have suspended your credit card temporarily." I think I've had one of these type of emails before and it looks very dodgy. "To lift the suspension click here and follow the steps to reactivate your credit card." That's not how credit card systems work. "If it's not resolved in 72 hours we will be forced to suspend your credit card permanently." They would call you directly.

Next, iOffer again, "History Arund1981; Congratulations, you just purchased an item from Goggle Box UK. Click here to cancel the transaction. You should receive an invoice for payment and instruction shortly." Because this came up before and it was very similar, it looks like these would make sense to go together, the other iOffer email. I haven't used iOffer so I don't know but it looks very legitimate, based on that fact though.

Next, Blizzard Entertainment; [Diablo Free Account 0:25:46]. "Greetings. It has come to our attention that you are trying to sell your personal Diablo Free account." What is that? I don't know what that is. "If your account passes the checks successfully we will send this package to dynamicbattle.net." \_\_\_ account is. If I didn't I would think it was very weird. "Please open this connection," it looks technical. "\_\_\_ the account," it just looks like whoever got this email is trying to use a service that's very specific. They wouldn't try and target general people with this. Illegitimate maybe.

Next, accounts.Google, suspicious sign-in prevented. "Hi Helen, someone recently tried to use an application to sign into your Google account," so it's giving you the IP address, location Italy. "Someone has tried to access your account." It seems reasonable that Google would send you this and it's got Helen Jones and the [Avatar-y 0:27:21] image so you'd know explicitly if this was your Google account and even more so if you went to Italy and logged in, it wouldn't seem too odd. I don't know whether Google send you these emails so it looks legitimate.

Next, "Your card is about to expire," from PayPal. "Update your card details with PayPal. Visa Delta Electron ending 1234," that looks odd because not many card numbers end in those exact numbers but PayPal would probably send you an email to explain this. "If you have received a new card, please link the card." There's a safety advice link there. I don't think a phishing email would have that link in. Apart from that ending in 1234, I'd say it was legitimate.

Next, PayPal again. "Helen Jones, view your recent transactions now. Log in now." PayPal logo is not normal. "View the online version." I don't think phishing emails look that technical so legitimate.

Next, Adobe Customer Care, it's adobeemail@mail.adobesystems.com, password reset information. It's a warning that someone has tried to access the account. Someone has hacked Adobe. That seems odd. "Too many newsletters? Click unsubscribe or better yet..." There's a lot of information that a phishing email wouldn't have. Read online as well, so maybe it's just a warning that they want you to reset the password so you could always do it online, you don't have to go through the email. You don't have to click any of the links. Legitimate.

Next, HSBC. The HSBC logo looks not like the HSBC one. It's @hsbcbusiness, "HSBC income fund is blocked. This is to inform you that the business account with us has been blocked for receiving payments. \_\_\_[0:30:34] security system. Please click here to begin to resolve the issue." Why is to begin highlighted as well? "Please forward to the authorised signatory." There should be more information on a HSBC email I would say. "You can always log into your business account if you weren't sure directly through the HSBC website if you have that account."

HMP \_\_\_ job alert. It looks like if you've signed up for a service, this would be something. iGrasp is some sort of thing "Psychological assistant, job search. "To cancel your job alerts click here," so iGrasp website again. It looks alright if you've done that sort of thing before.

Next, no subject. "Pleasure Beach, Blackpool visitor survey. Thank you for visiting the Pleasure Beach Blackpool recently," so you might have given your email address to them. If you know you were in the Blackpool area and you know what Blackpool Pleasure Beach was and you went there, then you'd know it was legitimate or not.

Next, DVLA DFT, Department for Transport, okay. "Important update required. We are currently upgrading our database and all drivers are required to update and verify their driver licence details." They wouldn't do that. The website address looks fine. There's a post code but no proper address. It looks very weird to have that. "Drivers that refuse to upgrade his or her details in two weeks," again, there's pressure on time, "Will lose his or her driver's licence," licence with a capital L, "will have to take a fresh driving test," no you don't, no one does that. Phishing email.

Next, r.malcolm@lancaster.ac.uk so because it's an @Lancaster web address or email address, that's very legitimate and exact. Survey Monkey is a well known website and Ross Malcolm. There's a lot of information there that seems normal. If you're part of Lancaster University, especially science and technology, you'd know.

**P323**

P323: This email says it's from Adobe. It says it's 'an attacker that's illegally entered our network and may have obtained access to your ID and password. Currently have no indication that there has been unauthorised activity on your account.' You have to click a link to create a new password. I know this sounds really stupid, but it's got the Adobe log on it. Let's have a look who sent the email. It says it's from email@mail@adobesystems.com, so it's got a legitimate email address, but there's a link to click. 'If you have any questions you can learn more by visiting our customer alert page, which you will fine here'.

I'd still be weary because you're asked to click an actual link. 'Please visit to create a new password'. (Whispers) I'm really not sure about this one. I'm going to go for either a three or a four, probably a four. Okay, 'Dear guest user, \_\_\_ your payment'.

[Silence 0:01:58 - 0:02:19].

Yes, I'm not too sure about this one either. There's no logo on it. It could be real, but it also could be fake. A very short email, but then I suppose you're not really doing very much. You just have to click on a link to view the status of your purchase. That sounds a bit suspicious, 'view the status of your purchase'. Maybe a three. I'm always a bit suspicious, to be honest. I'd rather not click on any links just in case. Dropbox. 'Dropbox needs to verify your email address before you can share folders. Please verity your email address by clicking the link below'. It's got an official email, official logo. Yes, I think this one might be legitimate. It's very short, but then you're not really having to do very much. You're just having to click on the link to verify your email address. I'm going to go with five here.

Okay, Google. 'Someone recently tried to use applications on your Google account'.

[Silence 0:03:40 - 0:04:05].

It looks quite official because it's got official time. These are quite hard. I'm not sure. I'm really not sure. I think I'm going to go with a four again.

Let's have a look at these next ones. Ooh, this one looks fake. 'I'm sorry for reaching you rather too late due to the situation of things right now. My family and I…'

[Silence 0:04:44 - 0:04:57].

Yes, this is definitely phishing. It's a note from Philippe regarding an attack by unknown gunmen and they want some money. All we need is £1850. Definitely phishing.

NatWest. Ooh, cancel. Cancel. Computer keeps going wrong. This is from NatWest. There's the official NatWest logo on it.

[Silence 0:05:41 - 0:05:59].

I think this one is probably legitimate. You can never be sure. I think I'll give it a five. It looks very official. The computer keeps going wrong. I don't know what it's doing. Cancel.

Visa. 'Your credit card has been suspended as an error was detected in your credit card information'. I think this one is fake because I think they might ring you for something like this because it's quite important. It just says 'click here'. No, it just says 'Dear valued customer'. It doesn't actually say Helen's name on it. You'd imagine they would say the person's name. It says this thing about 'if it's not resolved within 72 hours we'll be forced to suspend your credit card permanently as it may be used fraudulently'. I don't think they'd do that. I think I'm going to go with a two. I think it looks like phishing to me, but I can't be sure.

See, again, this is one from HSBC. Again, they're not saying 'Dear Helen' or they haven't introduced themselves. It just says 'a business account has been blocked. The account will be disabled if you ignore this message'. I don't think they'd do that. It just says 'click here'. It's very vague. It's very vague. I think this is phishing. I'm going to go with definitely phishing.

Okay. 'Your bill for Virgin Media is now ready and available to view'.

[Silence 0:08:13 - 0:08:34].

I think this one might be real, but they haven't named the attachment. It probably makes it more likely that you'll open it, so it could be fake. All you really have to do, you have to go over to the website to send an email and then you can send an email on a link as well. I don't know. They haven't got a logo on it either. It just says 'hello'. It doesn't say a name. It doesn’t say 'hello customer'. Maybe a three, a two or three, because they've got an attachment but they haven't put a name on it. I'll just go with a three.

[Silence 0:09:19 - 0:09:33].

This one is from Caxton Cards. 'I just want you to read the updated terms and conditions'. It's got Helen's name on it, Helen's full name. It's got a logo. It's got an email address and it's got their address. I think this one is probably legitimate. I think I'm going to give it a five.

[Silence 0:09:59 - 0:10:12].

This is Facebook. 'To confirm your contact email address follow the link below'.

[Silence 0:10:20 - 0:10:36].

It's addressing Helen by name. It says it's from Facebook. 'To confirm your email address follow the link below. If you didn't email this address as your contact email, disregard the message'. I think this might be real. I think I'll give it a five.

This is from Student Loans. 'Message for all students receiving grants and loans from Student Loans Company. Fraudulent activity is going on with Student Loans' account'. I don’t think that's likely to happen. The link, it says 'mineface.com'. It doesn't look like that kind of link that Student Finance would use. Maybe a two or a three.

PayPal. 'You sent a payment of something to Keith [Perli]'.

[Silence 0:12:07 - 0:12:23].

Okay. This is just a PayPal receipt. You don't actually have to click on anything I don't think, unless you want to. If you've got a question you can go to PayPal. This looks fairly legitimate. I'll go for a five.

[Silence 0:12:46 - 0:13:06].

I think this one is phishing. It's about, 'you're trying to sell personal Diablo account'. I've never heard of them. Then the link that they've given to verify the account ownership is a bit odd as well.

[Silence 0:13:29 - 0:13:41].

Ah, but then it says 'if you've already authenticated your account, please disregard this automatic notification'. It's not like they're making you click on it, whereas if it was phishing they'd want you to click on it. I don't know.

[Silence 0:13:58 - 0:14:08].

Not sure. I'll give it a four, a three or a four. I'll give it a four. Computer keeps going wrong.

[Silence 0:14:20 - 0:14:32].

Okay, so this is from Amazon. It addresses Helen by name. I think this is probably real. You don’t have to click on anything unless you want to manage your orders. It's got her name on. It's got her name on and stuff. Yes, I'll give it a five I think.

I think this one is fake. It's about a Gucci watch or something. 'Yahoo and Gmail users, click here. Give your loved ones a luxury watch today'. There's no introduction to it whatsoever. It's just really short and one link. I think this is phishing. I'm going to give it a two I think.

Ah, so this one again, it's about Google box UK. Oh, it's the history man again. This has been in one of the other ones, from iOffer.

[Silence 0:15:45 - 0:16:00].

It's just she's just purchased an offer. 'Should receive an invoice with payment and shipping instructions shortly. Made a mistake, click here to cancel the transaction'. It's very vague and there's no proper logo to it. It's just the fact that it's actually saying 'made a mistake' because obviously if she hasn't ordered it she'll want to click there. I think this might be phishing. I'm going to give it a two.

Easyroommate.

[Silence 0:16:42 - 0:16:54].

Addressing Helen by name. It's a very long link, but you might expect that I guess. Probably legitimate. I'll give it a five.

[Silence 0:17:16 - 0:17:26].

Okay. Plusnet Protect. I think this is probably legitimate. It's got Helen's last name. It hasn't got a logo on it.

[Silence 0:17:48 - 0:18:06].

Yes, it's got a load of instructions about what to do. I think I'll go with five.

Okay, so this one supposedly is from NatWest, but the header is a bit odd. It says NatWest, but then it's got in brackets '[uup@dankertone.com 0:18:29]'. It just says 'your online account will expire today', but it doesn't say why. Then 'if it's not performed within 24 hours your account will be disabled'. They'd never do that in case you didn't get the email within 24 hours. I'm going to go with phishing. One.

Okay. Gary Cooper. This one is phishing. One.

[Silence 0:19:15 - 0:19:29].

Okay, so this is from Student Finance. It's got an official email address. It's generic to all students. I think this one might be legitimate. I think I'll go with five.

Okay, so this one just says 'your password will expire in three days. Click here to validate your email'. I think this one is phishing because it doesn't even say where it's from. It's just system administrator. I'll go with definitely phishing.

Okay, so this is from recruitment, JobAlert. 'A job which matches your alert criteria has been published on our website'. It's a job for a psychological assistant. It's a bit vague. It just says 'job, psychological assistant. Grade, psychological assistant'. It looks quite genuine. I'll give it a five.

Okay, so this is NUS. 'You entered this email address to change the password of an NUS extra account. To continue the password reset process, proceed to this link'. It's a bit vague. I think it might be phishing, but I'm not sure. I'll go with a three.

This one is from PayPal. 'Your card is about to expire. Be sure to activate your new card with your bank first'. I think this one might be legitimate because it's got the PayPal logo. It also says 'if you've already updated your PayPal account with your new card details, please disregard your email'. I think if it was phishing they'd be trying to do everything that they could to get you to click on that link. I think I'll go with four. It's got the official PayPal address thing on the bottom as well.

Something else from PayPal. 'Log in to see your monthly activity and recent transitions'. Oh, it actually says 'how do I know this is not a phishing email? Emails from PayPal will always address you by your first and last name'. Oh, okay. All the other things that I've seen from PayPal, I'll just have to watch it's addressing her by her first and last name. 'If you're concerned about the security of this email, type paypal.co.uk into your browser and log in that way'.

Yes, I think this is legitimate then because it's actually saying about it being spam/phishing. The others probably weren't legitimate because none of them have said about phishing. I'll give it a five. Actually no, I should probably have given it six. Ah. I don't know if I can go back. No, I can't go back. Never mind.

'Your parcel has arrived at the post office. To receive a parcel, please go to our nearest office and share this postal receipt'. Not sure about this one because it says 'priority mail postal service', but then it's got a weird address. It's actually got a tracking number. Ah, I'm not sure. A three or a four. Maybe a four. No, three actually.

Okay, eBay suspension.

[Silence 0:23:50 - 0:24:06].

'Your eBay account has been suspended due to concerns we have for the safety and security of the eBay community'. Why would they do that?

[Silence 0:24:16 -0:24:26].

They haven't said why.

[Silence 0:24:28 - 0:24:49].

I think this one is probably genuine because they've explained the situation quite clearly. It's got a logo on it. They've given an actual date rather than saying 'oh, if this isn't done within the next day'. Either a four or a five for this one. Maybe a four. You can't be too cautious.

[Silence 0:25:18 - 0:25:39].

Okay, so this is from HR recruitment department.

[Silence 0:25:42 - 0:25:57].

It looks quite official, but it just says 'our new role we have opened'. It doesn't say what it is. Well, actually it does say what it is later on. This might be genuine. I think I'll give it a four.

[Silence 0:2613 - 0:26:25].

eBay. Okay, so this one is from eBay. It looks quite legitimate because it's got a proper address on it. It's got an invoice number on it.

[Silence 0:26:38 - 0:26:48].

Then it's got something on the bottom about learning to protect yourself from fake emails. These ones have probably been left until last because had I have seen these ones first then I'd have known that the other ones weren't genuine. This one is probably legitimate. I'll go with five.

Dell. This is completing a survey for Dell.

[Silence 0:27:17 -0:27:28].

This one looks really genuine because it's explaining a lot about the survey and it won't be used for sales purposes, how to contact them if you want to contact them. Probably a five.

Barclays. 'We have detected unusual activity in your account. This may be the cause of logging into online banking from several IP addresses. \_\_\_[0:27:58] [limit] your account \_\_\_'. Barclays quite often text. They've texted me before rather than emailed me when I've spent more money than they thought that I would. I don't think they'd send an email like this. They'd address you by either name or- hmm. I don't know. There's just something about this email. I don't think they'd ask you to click a link either. What they've done with me, they've texted me and I had to say yes or no. I think this one is probably phishing. I'll go with two.

Blackpool Pleasure Beach survey.

[Silence 0:28:58 - 0:29:13].

I think this one looks quite genuine to me because it's explaining that the answers are anonymous, confidential. 'Information provided will only be used for research purposes, won't be passed onto anybody else', etc. I think I'll say four or a five. Probably a four because there are some that have looked more legitimate than this and I've given a five, so I'll give that one a four. God, the computer keeps going wrong.

DVLA. 'We're currently updating our database and all drivers are required to update and verify their driving licence details'. They've spelt 'their' wrong. It should be T-H-E-I-R. Yes, the grammar in this isn't very good. 'Drivers that refuses to update his or her details' - oh, that's ridiculous - 'within two weeks of receiving this verification will lose their driving license'. There's no way they'd do that. Definitely phishing. Actually I'll go with a two just in case, not a one.

Okay, so this is from Lancaster University, Faculty of Science and Technology undergraduate survey. 'Welcome to Lancaster. We hope you've enjoyed your first few weeks at university'. This looks like the kind of email that they would send. I think I recognise the name Ros Malcolm as well. I don't know why. I've probably got this.

[Silence 0:31:05 - 0:31:17].

This was addressed to Helen in 2013 when she'd be doing her PhD I think rather than undergrad degree, but they could have just made a mistake or the details could have been changed. It looks like a SurveyMonkey survey. Loads of people at the uni use SurveyMonkey. Yes, I think this is legitimate. I'll give it a five.

**P324**

P324: Okay, first email. Well my feeling about this is that the email address looks potentially legitimate because it’s at like a URL that’s the direct URL of the company, but at the same time, the use of exclamation points in the subject make it seem unprofessional, as does the grammatical error of capitalising all of the words in the subject. Also the link that they ask you to click is at a URL that is nothing to do with the company SLC, and the fact that the company name Student Finance England does not correspond to the letters in the abbreviation SLC makes me believe that this is definitely phishing.

So, again, we have a legitimate looking email address, but an email subject that does not look legitimate. They’re using the Visa logo, but at the same time, you’re receiving an email to say that your card has been suspended, whereas really you should be receiving this sort of email one from your bank, and they should probably be giving you a phone call or some other sort of notification, not via email. The link is not clearly marked, so it’s not easy to tell where it’s going to lead you, so I would be suspicious about clicking on it. Additionally there is this time limitation of 72 hours, and about permanent suspension of your credit card. Well, you should not be receiving anything like this from Visa themselves, you should be receiving it from your bank, so I’m going to say that’s definitely phishing as well.

So this is very clearly phishing from the beginning. The email address refers to three companies, whose websites are not referenced within the URL of the email address. There is incorrect grammar, and there is just an advertisement for giving someone a luxury watch with a bunch of links that, it’s not clear where they lead, so this is definitely phishing again.

So this one looks… Hmm, it’s difficult to tell if this is legitimate. The first thing I would imagine would be whether I have actually intended to make this payment to somebody. I’m not clear about the PayPal policies about the fact that you’ve got an email from [service@PayPal.com](mailto:service@PayPal.com), but an additional- The actual email address, so the email title, or the sender’s name is service@PayPal.com, but the address that’s attached to it is someone’s specific address, the address of the person that you’ve sent the payment to. I’m not really sure what PayPal policies are, so I’d be a little bit suspicious about this, but it does look precisely like the PayPal format of emails. So I’m not totally certain about how truthful this email is, and whether it’s phishing or not. The only thing that kind of alerts me to it is the lack of coherence between the title of the sender and the sender’s actual email address, so I’m going to move towards phishing, but I’m not totally certain.

So again I’m not totally certain about the legitimacy of this email. There is a link to a website, it’s clear where the link leads. I guess it doesn’t look like a- Usually on job websites people, when they send you links, they’ve got the title of the job inside the link, which isn’t here, which would be a little bit of a flag raiser to me. In addition to the fact that I don’t understand why you have www2, or www5, but I know that these types of links for whatever way they do the redirection or whatever, tend to be associated with more suspicious things. So I would be a little bit suspicious of this email if I’d never used this iGrasp.com website before. So again, I’m leaning more towards phishing in this email.

So, there is an add for a survey for Dell. The email address from which the survey has been sent is not a Dell email address, but it could potentially relate to like a survey company that has been hired by Dell. I’m not certain that the email address looks legitimate, simply because it’s got multiple parts to the email address, you think that if they’re a legitimate company they’d have a more direct email address, for example, [Dellsurveyhelp@TNSonline.com](mailto:Dellsurveyhelp@TNSonline.com), rather than redirecting through additional mail signifiers.

So if I read this email… Again, the link looks a little bit suspicious, it’s not a very direct link. If it were, for example, attached to a company that I was more familiar with, like Survey Monkey or something like this, maybe I’d be a little bit less suspicious of it. It would also depend on whether I had recently actually contacted Dell about an issue that I was having. So there is a link to support.url.dell.com and some other web pages associated with Dell. They’ve got more information about TNS down at the bottom, and they’ve got some information on additional programs. Even though the link seems a little bit long and dodgy, I’m not totally certain that this is phishing, so I’m going to suggest that it’s potentially phishing, but I’m not certain.

So next email. I absolutely recognise the email address from which it has been sent. Then the link is extremely long, but you do often get these kinds of links when you have requested a password change. It looks suspicious that the IP address is everyone’s home IP address, you know, 192.168.1.whatever, but maybe that just refers to the fact that it was a computer in your network that requested it, and it’s likely that it would be your computer. So I’m leaning, simply on the basis of the recognisable and direct email from which this was sent, going to suggest that it is legitimate, but I’m not totally certain because of the extreme length of the password change length, although it does lead to the NUS Extra website, which is a legitimate website, and the fact that it was requested. Yes, again, I’m not totally techy, so I’m not totally sure about the fact that the IP from which it was requested was one within your own network. Maybe that’s a good thing. It’s leaning more towards legitimate in this case.

So this is absolutely definitely phishing, because it purports to be from NatWest, but you’ve got grammatical errors in ‘Login to online banking,’ you’ve got un-needed capitalisation, you can’t see where the link is, you’ve got a threat that’s time limited, and the email address it’s sent from is nothing to do with NatWest at all, so it’s definitely phishing.

So here, this is also definitely phishing. You’ve got an email address from someone that, okay, maybe someone’s US university email address has been hacked into and emails are being sent from it, but you’ve got a threat of a password expiry, which is nothing to do with the email address of the recipient, which is at a totally different university. You’ve got some link to a web mail upgrade that looks completely dodgy, because there are multiple components, and a domain, .me that’s not always associated with legitimate websites, as you normally have the more general ones, .com, .co.uk, [.e 0:10:45], .net, .org, so I’m going to say that this is definitely phishing.

So I am uncertain about this one, but leaning a little bit more towards- No, now that I’ve looked at it, I’m thinking that this is phishing, even though it’s a direct.gov.uk email address, I’m wondering if there has been some sort of messing around with that, because it says [Student Finance E 0:11:26] and surely they should be able to get them to write Student Finance within their own email address. The thing that really changed my mind is that they have a sentence that says, “Please fill the requested information exactly as you filled it when you were signing up for student finance,” then a period, then a lower case ‘O’ for “or your payment will be suspended because of failed account verification.” This is the sort of thing that you really wouldn’t expect to receive an email about if there was some sort of need for a huge update you’d expect to get some sort of letter or phone call in addition to this kind of email, which is not really from a legitimate looking email address even though the website seems legitimate. It’s strange to me how they can manage that, but really it doesn’t look legitimate to me. You’ve got a link that you’re not sure where it goes unless you’re able to hover over it. Yes, there are grammatical errors, we have, “Due to a recent update in our database, We require all student” – no ‘students’ – “To update their account information to ensure you receive your scheduled payment,” so this is almost certainly phishing, absolutely.

Okay, this is legitimate. The email address comes from NatWest. Hmm, almost certainly legitimate. So they’ve got a segmented email address, but you can possibly see that this would exist, from the bank. The only link they’ve given you is a ‘contact us’ link, they’re not asking you to update any information. They’ve got some links to the NatWest website itself, but of course the ‘contact us’ is a hidden link, or a concealed link, but that’s fine, given that the other ones are up to date. They’re not asking you to change details, they’ve in fact said they’ll never contact you and ask you to provide your security details, so it does seem- I’m going to lean that this is definitely a legitimate email.

So, first red flag, you’ve got an email sent via another server, well, it’s an orange flag, maybe not a red flag. You’ve got emails, or you’ve got links to an email address that’s a direct email address, but you’ve also got a concealed link, it’s supposed to be to updated terms and conditions, which I would definitely hover over before clicking. They’ve definitely got some information down the bottom here about registration number with the Financial Services Authority, which you could use to look this up, and they’ve got a legitimate looking phone number. They’ve not asked you to provide any sort of information, or anything like this, so despite the orange flag of the emails being sent via a different server, I’m going to suggest this is likely legitimate.

So, red flag one, “Dear valued eBay member,” instead of, “Dear Helen Jones.” You’ve got admin@ebayz.com, not eBay. They’re suspending your account, letting you know via email, but not giving you a name. They’ve got a link that again has got many components, so is likely to lead to something a little bit dodgy, even though it’s actually an ebay.com link. So yes, definitely this is, just on the basis of the email address from which it has been sent, this is definitely phishing.

So this looks like a legitimate email. You’ve got something from an iOffer website, which presumably is some sort of deals website, or some selling website. You’ve got a guest user, so it’s obvious that they haven’t written your name, but that’s because you haven’t given those details. The link within the email just gives you a link to the status of your purchase, to the website. So again, it’s got multiple components, but you might expect this on a mutual selling website. So really what would flag this up to me as phishing or not, is whether I’d actually purchased this item on this website, but I’m leaning towards this email being legitimate.

So red flag, an HR recruitment department that has a Yahoo email address rather than one for themselves, and the recruitment department doesn’t make any references to any company, even within the email address. Even if they were a small company that happened to have a Yahoo email address, they’d have something like HRDepartment\_companyname. A company would never say, “I am glad to inform you that you have made my shortlist,” it’s the shortlist, they don’t make these personal statements. Grammatical errors, lack of spaces between full stops and words. The introduction of the person’s name comes later than the part where they’re telling you that you’ve made the shortlist. You’ve got a big link that says, “Please click here to download the application form.” They’ve got a huge number of symbols pointing towards it to really draw your attention to it, perhaps before you even read the email. It tells you to double click the application form, which is probably some sort of zipped program that is going to install itself. Yes, so this is absolutely definitely phishing.

So, this is legitimate. It’s from Dropbox, it’s from a direct email address @Dropbox, you’ve got a link that’s concealed, but given the email address the email has come from I would suggest that this is a legitimate- Yes, especially if I’d recently signed up for Dropbox.

So, Blizzard Entertainment. So, a bit of a flag, you’ve got something from Blizzard Entertainment, but it’s from [Battle.com 0:18:16] website, so I don’t know much about Blizzard, but if the company was a subsidiary of a company called Battle, or if Battle.com was some website associated with that company, I’d be a bit more comfortable, but I have no familiarity. So you’ve got a link with multiple components, I’m not really sure where it’s going to direct you. You’ve been told that your account is going to be suspended, and you’ve got this time limit, you should immediately verify your account ownership. They’re saying that your account needs to pass a check in three days, “If you don’t submit it we have the right to freeze your account.” I’m not really… I’m not sure about this one. “Please open this connection.” This could be legitimate, but I would be cautious about it, just because you’ve got Battle.com not BlizzardEntertainment.com. Unless the Battle website is some component of playing Diablo 3. I don’t know. I’m leaning towards this being legitimate, but not leaning very heavily.

Again, “Dear Barclays account holder,” not, “Dear Helen Jones,” [Barclaysonlinesupport@bnet.com](mailto:Barclaysonlinesupport@bnet.com), that’s not a match, bnet is nothing to do with Barclays, so no, absolutely not. You’ve got a link that’s concealed. This is phishing, absolutely.

Okay, Adobe Systems email, the title matches the email address. Your password reset information, “May have obtained access to your Adobe ID.” So the password reset actually looks legitimate, because it’s linked to Adobe.com. I’m not certain. I would lean towards this being legitimate; what flags it with me is that it’s Adobe.com/go/passwordresetuk presumably it should be something like www.adobe.com/login or something like this, where it would bring you to a page where you can reset your password anyway, no matter how you access it. Maybe they’ve set up a special support webpage, given that everyone seems to have to change their password. So likely legitimate, not wanting to say definitely legitimate.

Okay. So this is a legitimate website, Accounts.Google.com, you’ve got some attachments, which would flag something with me, but maybe it’s because you’re not reading your email on an HTML enabled platform, and often what happens in non-Gmail accounts, or non-HTML set-ups is that the images don’t get incorporated into the email, they get included as attachments. So orange flag, yellow flag.

Oh yes, you’re reading it on your Lancaster email address, so this makes sense. They’re giving you the information about the login, they’ve got something that tells you that you should reset your password. You’ve got links to Google, there is one link that’s concealed, the reset password link, I would suspect that Google would not actually give you a link for going to reset your password, but would tell you to visit mail.google.com so this is potentially phishing, but not definitely phishing. I would have suspicions about receiving this email but I would not necessarily disregard the email off the bat, I would just look into it further and probably just go to mail.google.com and reset my password anyway.

Right, so they’re addressing you as Ms Jones, Plus Net Support, [support@plus.net](mailto:support@plus.net), this looks good. They’ve got portal.plus.net makes sense, given that it’s plus.net that’s emailing you. So I would suggest that this is legitimate. The links are all highly visible, it’s a legitimate company email, title matches email address. I don’t have any suspicions about this.

Just loading. It’s still loading. Still loading. Okay I’m going to skip this one because it’s failed to load. Right. I’m just going to answer on this one there is nothing visible, I can’t click anything. Here we go, okay. “Issue one, please enter this question.” So this is the Priority Mail Postal Service, [DTF.193@FortWayne.com 0:24:40] doesn’t match the email title, or who it purports to be from, which is FedEx. I don’t know, does FedEx have a parent company called Fort Wayne? I doubt it, they’re a big enough company to have their own website. So, errors, “Your parcel has arrived at the Post Office at December 7th” – full stop, no space – “Our post [rider] was unable to deliver the parcel to you.” It’s not the real FedEx logo, it’s not the FedEx colours. They’ve got a link that’s concealed. “Dear customer,” not, “Dear your name,” so yes, this is definitely phishing. Okay.

This is- Oh yes, a very standard form of phishing about someone leaving you money, and it’s going to be total bullshit- Excuse me, that’s not professional language. It’s going to be totally incorrect; I mean, no one ever contacts you this way, these are very, very well established scams, so this is definitely phishing.

Okay. Now this is an email that is very similar to one that was in previously that was a text-only email. This one is an HTML email, it’s got a- Hmm. Now, email address looks legitimate, but they’ve got something about receiving an invoice, whereas normally with these websites you can pay directly. Shipping instructions. Maybe this is the way that you get to work on these websites, I don’t have any experience of this kind of person-to-person selling, usually it’s via PayPal, it’s not invoiced. They’ve also got a link to directly cancel a transaction, that doesn’t seem… That seems like you’re told that you’ve got a transaction that is nothing to do with you, you panic and you want to cancel it, and then they get information. Additionally, it’s iOffer, but the company is Google Box, so I’m going to suggest that this is likely phishing. In fact, I would not respond to this email, so I’m going to say it’s definitely phishing.

So, HSBC, HSBC website. So the email address and title look legitimate, but they’re telling you that the business account has been blocked. You’re receiving this as an email, and you’ve got a concealed link, and they haven’t said, “Dear whoever,” so, hmm, I would be very suspicious of this, I would not click anything on this email and I would contact HSBC directly, because I wouldn’t expect to be receiving emails from them about this sort of thing, I would expect phone calls. It’s a shock, you know, “Incoming funds blocked,” it’s to instil fear, so no, phishing.

Okay, you’ve got an email from PayPal, and it’s a legitimate PayPal address, telling you that your card is about to expire. But I would have suspicions about whether PayPal would actually care about this sort of thing, or whether they’d really have access to that information. But I can see this being fundamental to their business model, to be able to do this sort of thing. The email looks legitimate, the kind of information that’s in it doesn’t seem super legitimate to me, I would expect that you would simply have an issue next time you had to pay via PayPal. I mean, you never do it automatically, they always give you something to review, so I would suggest that this is potentially phishing.

Now, here we go, [PayPal@e.paypal.co.uk](mailto:PayPal@e.paypal.co.uk). The ‘e’ is a little bit suspicious. But it’s just a PayPal statement. They’re telling you that you can login via PayPal.co.uk and not have to click this link, so that’s comforting, but it looks like standard PayPal email, but this e.paypal.co.uk would get my back up a little bit. So probably not phishing, but could be. I’d probably just go to PayPal.co.uk instead of clicking any of the links in this email.

So, Virgin Mobile, they’re sending you a zipped file, that is immediately suspicious to me. It looks like the structure of an email that you’d receive from Virgin, but why is it \_\_\_[0:30:10]@virginmedia.com, why isn’t it ‘bills’ or ‘statements’ or something? There is an attachment there and it shouldn’t be there. Essentially this email is trying to get you to view that attachment, so that is definitely phishing I’m afraid.

Facebookmail.com. No, that’s not Facebook, this is phishing. Email looks legitimate, but the email address does not. Again, this would all be tied to my recent behaviours.

Right, [billing@ebay.co.uk](mailto:billing@ebay.co.uk), this looks like a legitimate email address. You’ve got an invoice. Okay, so it’s telling you that you’ve got an automatic- Okay, so I can understand in the previous email why PayPal would tell you that your card was about to expire, because they’re doing automatic deductions from your account. So, let me see. Right, so they’re not sending you links to any weird places. Everything is very clearly available, and the links are to ebay.co.uk not ebay.co.uk/alphabetsoup so I would suggest that this is not phishing, that this is a legitimate email.

So, [Frank@EasyRoommate.com](mailto:Frank@EasyRoommate.com). You’ve got a lot of links. Now, I can understand why the link within the email is so strange, because obviously on these websites they have huge amounts of content that is constantly changing, so it does look okay, but presumably here, the highlighted link here, and the other link, should be exactly the same. I don’t know how you could be redirected to different ways. Usually what I would expect to do is be told to login to my account if the above link doesn’t work, that there would be some sort of system in that case. So I’m suggesting that this is a scam, this is phishing, but I’m not 100% certain.

So, can’t see the email address, but maybe that’s an Amazon policy to conceal it. Usually you would expect that this sort of email would come via Amazon, not from Carla Craig, you would get it so that the seller would be able to route their contact with you through Amazon, so this raises my hackles and I’m going to suggest that this is a phishing email. It looks like a legitimate Amazon email, but you shouldn’t be getting it from Carla Craig; you should be getting it from something to do with Amazon, I’m afraid this is almost certainly a phishing email. I probably would login to my Amazon account directly, just to check the information, but I wouldn’t do it via this email.

Okay, here we go, you’ve got someone pleading with you for help; someone who is not related to you, someone who is not connected to you, asking for money. You’ve probably never had contact with this person before. So I’m going to say that this is definitely phishing. That person should have gone via the police anyway, it’s just not legitimate.

Team@BlackpoolPleasureBeach, [Surveys@AspectMR.co.uk 0:34:48], not really matching up there. They’ve got a Pleasure Beach visitor survey, so maybe again it’s a case that someone has been employed, Aspect MR have been employed by Blackpool Pleasure Beach to do this survey. Again, my feelings about this would be based on whether I had recently visited the Pleasure Beach or not. Then you’ve got quite a long email address, or quite a long URL, but you would expect this sort of thing in relation to these kinds of surveys where there are many, many of them hosted on the same website. The email is well written, so I would suggest that this is not phishing, but it’s not totally legitimate either, because you’ve not got contact details for the company, contact details for Blackpool Pleasure Beach, not got information about how they got your email address, so I’m going to lean towards the middle on this one, I’m afraid.

Okay, DFT.co.uk, well it’s from the DVLA. Incorrect spellings, [there/their/they’re instead of there/their/they’re 0:36:10], “Drivers that refuses,” time limit with two weeks, blah, blah, blah. This is almost certainly phishing. It’s not legitimate.

So, got a legitimate email address, Lancaster.ac.uk, you’ve got a Survey Monkey survey, which is a trusted survey host. You’ve got the offer of a prize, but given that it’s from a university and it’s a Survey Monkey link, I would say that this is legitimate, and yes, I would see this as a legitimate email, although it could be someone from within the University trying to get my information by getting me to answer questions on Survey Monkey but I would obviously adjust how I answered, or not answer if I saw a question that was illegitimate.

**P325**

P325: ‘From Billing@Ebay.co.uk’. ‘EBay inbox notification’, ‘Helen Jones’, ‘Invoice number’, ‘Automatically generated E-mail.’

‘Your invoice, from a period from June 16, 2013, is now available to view online.’

‘PayPal has an automated E-mail, and automatically deducted...’

Hmm.

‘EBay, your recent payments...’

[Background noise, 0:00:48-0:01:06]

Legitimate. Yes.

Oh, Dropbox. So, I have to think out loud. ‘Subject must verify E-mail address.’

‘Please verify, The Dropbox Team.’ Hmm.

Just checking the design of it, because I use Dropbox quite frequently. And it looks quite legitimate. I would definitely verify my E-mail address if that came to me.

Oh, ‘Barclays account number,’ ‘Detected unusual activity in your account. This may be because of logging into online banking. To access the online profile validation form, click on the following link.’

The number’s the account. ‘To access the online...’ ‘Click on the following link.’

Hmm. I don’t trust this. But I’d probably click it and then see where it takes me to. If it asked for more details, I won’t put my details.

But it doesn’t look like a phishing E-mail. I’ll put a ‘Two.’

‘Caxton FX.’ ‘Changes to terms and conditions.’ ‘Please take time to read.’ ‘Recommend...’

‘If you have any questions, we will be pleased to help.’ Hmm, not phishing, because it’s not really asking me for any information. So, that.

‘Thank you for your interest in our new role. We’ve carefully reviewed your CV.’ ‘Full time and part time position.’ ‘Average...’ ‘Touch up your application form with directions and instructions.’ ‘Once the file is downloaded...’

And then, ‘If you have any queries...’

Why would it be a phishing E-mail when it’s coming from HR? But this HR department E-mail is not really that professional-looking. And it’s Yahoo. Unless I’m trying to work for Yahoo. But then, that looks really odd.

‘Don’t let go.’ ‘This formal notification is for an update in our student...’ ‘And avoid missed payment...’ ‘It’s therefore requested...’ ‘Student finance,’ ‘Or your payment will be suspended.’

So, there’s a full stop after ‘Finance’, hmm. Why would a payment be suspended because of failed account verification? That’s quite intense. I don’t know how Direct.gov works or Student Finance works, but that does sound wrong.

And they spelt ‘Student Finance’ wrong in the E-mail. Got you.

Don’t laugh, Helen, this is not funny. This is serious business.

‘Dear candidate, a job which matches your online criteria...’ ‘Paste into your browser...’

‘Good luck with your job search,’ who the hell sends that? What HR recruitment team does that? ‘HMPSRecruitment@igrasp.com’, that sounds really dodgy. Were you grasping? Hmm.

‘Follow the link,’ ‘Click the following link or paste it into your browser and search for vacancy number...’ Hmm.

‘Greetings, it has come to our attention that you are trying to sell your personal Diablo 2 accounts. This conflicts with DUIN terms of agreement. If this report proves to be true, your account can and will be disabled. It will be ongoing for further investigation by Blizzard Entertainment employee.’

‘If you wish to not get your account suspended, you should immediately verify your account ownership. Please open this connection.’ Hmm. Dotcom WoW?

‘If your account passes the check successfully, we will send this package to you in the following three days’ time. If you don’t submit...’

Diablo 3, Blizzard Entertainment, 2013. I don’t know what to say. This is very sad, that you’re going to freeze my account. Diablo 3 account in the subject heading. From Blizzard Entertainment.

Why would you greet me with, ‘Greetings’? That’s very, very unprofessional when you’re trying to freeze my account. So, definitely phishing.

EBay. ‘Admin@ebayz.com’. Definitely phishing, without a shadow of a doubt. Unless they’ve changed their E-mail address recently.

‘HSBC’. ‘Mail to info@HSBC-business.co.uk’ ‘Subject: HSBC incoming funds block.’ ‘HSBC, the world’s local bank.’ This all looks very different.

‘...Has been blocked from receiving payment, attempted error log-ins were detected by our security systems’, ‘Account will be disabled, please click here to begin to resolve the issue.’ ‘Please forward to authorised signatory.’

Hmm. Definitely phishing.

‘Service@paypal.co.uk’, ‘Update your card details,’ ‘1234 [is back 0:10:09],’ ‘Please update your current expiry date and current security code. ‘Be sure to activate your new card with your bank first.’ ‘If you have received a new card, please link the card, if you have already updated your new card details, please disregard this E-mail.’

‘Yours sincerely, PayPal.’ Hmm, it’s pretty legitimate, I would say, because it gives me the option to update and not update if I’ve already done it, I think.

‘Activate your new card with your bank first.’ Why so much information? I don’t know. I’m going to go for, ‘Four’, because it does look legitimate in terms of spelling, but...

But then again, these little squares. Hmm. I’m going to put, ‘Two.’

‘I’m sorry for reaching you...’ ‘Are too late,’ ‘Due to a situation everything’s right now’. Hmm. ‘\_\_\_[0:11:50] incident,’ I think definitely phishing.

‘Hello. The bill for your Virgin Media is now in ready to...’ ‘Is now in ready...’

‘Balance will be taken out.’ ‘Our team won’t be picking E-mails, so if you like...’ So, definitely phishing. Why would it be a no-name attachment, silly?

‘Your latest statement is available online.’ ‘Onlinebanking@information.natwest.com’ ‘Just logon.’ ‘Logon’? Isn’t it ‘Log on’?

‘If you need more help with understanding your statement, visit our statement area.’ ‘Our statement area,’ that sounds really unprofessional.

‘With your online banking, remember you can also set your “Act Now” alerts to prevent missed payments.’

‘We’re here to help, we’d also like to remind you about security. We’ll never contact you and ask you to fill our your security details. Please contact us.’

‘If you need more help with understanding your statement, visit our statement area at Natwest.com/yourstatement’, Ah. Hmm, ‘Managing Director, retail banking.’

The links all look fairly correct. ‘Natwest.com/online’. ‘Statement for account ending 801...’

I don’t know how a Natwest statement E-mail would look like. But it does seem like...

It’s definitely phishing, because it says, ‘Visit our statement area at Natwest.com/yourstatement’. It should be ‘Visit your statement area.’ ‘Logon’, there should be a space between ‘Log’ and ‘On.’ Maybe. Maybe not.

Oh, why? This doesn’t look...

Very fishy. ‘You or someone else entered this E-mail address to change the password of an NUS Extra account.’ Phew.

‘Your online account will expire today, on the 3rd June, 2013. Please log in to online bank, in this case...’ Oh, different font. ‘This process is not performed within 24 hours, your account will be disabled. In case this process is not performed...’

That’s very harsh, so that’s fake. Oh, and the E-mail address is fake.

‘Ioffer’, ‘Noreply@ioffer.com, via ioffer-mail.com’ ‘Dear Guest User, Googlebox UK has received your payment regarding the item under ‘History Man, 1981 mini-series.’ ‘Mini-series’? ‘Rare TV on DVD’? ‘Ioffer’, wow. This doesn’t look legit.

Don’t really want to click on that.

‘Dell Survey’ ‘Help@NAIL2RatmailTNS-online’ ‘From TNS on behalf of Dell Incorporation’ ‘Dear Valued Customer, thank you for your recent contact. At Dell, we’re committed to our delivering the best Customer Experience to our customer.’

Why is it, ‘Customer’ and ‘Experience’ both capitalised? ‘Valuable feedback regarding your experience of Dell Support will help us improve our internal processes and provide better service to you.’

‘To complete this survey, please click on the web address below.’ By, ‘If that does not work, copy and paste the entire web address into the address field of your browser. This survey should take about five minutes to complete. We look forward to your feedback. Sincerely, the Dell team.’

The E-mail doesn’t look legitimate, and the link does not look legitimate, so definitely phishing.

‘Hello, I’m Mr. Gary Cooper.’ ‘Was born...’ ‘I’m in a medical institution in Italy where I’m writing you.’ ‘I’m suffering from lung cancer in terminal phase. Doctors have asserted that my days are numbers. Therefore I will kindly leave you my fortune to good use.’

Wow, how very nice of you.

‘Especially for a charity...’ ‘Primarily provides support to orphans, destitute and homeless. I have no heir apparent and my situation...’

‘I chose you as...’ ‘At least I hope to follow now, as I will count on your good faith to carry out this work and better. Could you contact me..?’

Oh, Gary Cooper, you are desperate. If you were born in London, England, you would have better grammar than that. And what’s that mail to, ‘GNB@Eviso.ci’? Hmm, I wouldn’t trust you, Gary Cooper.

‘Yahoo and Gmail user, click here.’ ‘Good day, Gabrial left one a luxury watch today,’ definitely phishing.

‘Your password will expire in three days. Click here to validate your E-mail.’ Hmm, ‘Upgrade-webmail13.html’, doesn’t look legit. ‘S.Grenata2@wash-col.edu’? What password is this? Am I in the same education, the same uni as you? Am I at Wash-Col? But even then, that link has got nothing to do with Wash-Col.edu. So definitely phishing.

‘Hi Helen, someone recently tried to use an application to sign into your Google account.’ ‘1989@googlemail.com.’ ‘We have prevented a sign-in,’ ‘Hijacker trying to access your account.’

‘If you do not recognise this sign-in attempt, someone else might be trying to access your account. You should sign in to your account and reset your password immediately.’

‘If this was you and you’re having trouble accessing your account, complete the troubleshooting steps listed at support.google.com/client-login.’

This seems real. Legitimate. Because it doesn’t give me a link to reset my password. It just told me to sign into my account and reset my password immediately. Through whatever means.

But, ‘hijacker’, hmm. I don’t know. ‘9th of September 2013, 10:13,’ Location, Italy. So I would definitely change my password with any means, but not clicking that.

‘Your application.’ ‘Someone recently tried to use an application.’ How do you know it was an application?

And, why would you have Google.png and profilephoto.jpg as an attachment? I don’t know. I’m uncertain. I’m going to go number ‘Three’, actually.

Hmm. ‘Recently entered a new contact E-mail address.’ ‘Follow link below.’ ‘Try copy and pasting it into your browser.’ I don’t like this copy and pasting malarkey. ‘If you did not enter this address as your contact E-mail, please disregard.’

‘Facebook Mail,’ ‘Notification+OFCDRD1’, hmm. Looks fishy.

‘Detected fraudulent activity.’

[Background noise, 0:23:12-0:23:27]

‘[InsLC.uk]’, ‘Minephase.com’, hmm. It should really have ‘Student Loans Company’ attached to this link. Or Direct.gov, but there’s nothing like that, so it’s definitely phishing.

‘Hello from PayPal, log in now to see your monthly activity and recent transaction’. ‘View online version,’ ‘Paypal@...’ Oh, can’t really see it. ‘Paypal@e-Paypal.co.uk’, hmm. Pardon me.

Now, ‘How do I know this is not a phishing E-mail? E-mails from PayPal always address you by your first and last name. If you are concerned about the security of this E-mail, type...’ ‘And log in that way.’ Hmm.

‘How do I know this is not a spoof E-mail?’ ‘Spoof or phishing E-mail tend to have generic greetings such “Dear PayPal Member”.’ Wow. So you must be real.

Nah, still don’t buy it. And why is it, ‘E.paypal.co.uk’?

Don’t buy it, because why would you need to remind us how to look out for phishing E-mails? Idiot.

‘Hello, HelenJones1989, thank you for shopping with us. We thought you must be informed that we shipped your item, and that this completes your order. If you need to return any goods from this shipment or manage other orders, please visit your orders on Amazon.com.’

Okay, that’s good.

‘Your estimated shipment date is...’

‘Your order was delivered to HelenJones1989, Department of Psychology.’ Phew, that’s an expensive TV.

‘Returns are easy. Visit our online return centre.’

‘From Carla Craig, regarding an item waiting on delivery today.’ Oh, ‘Sold by Trenter.’

‘\_\_\_[0:26:43] is acceptable...’

‘Paid by cheque.’ Mmm. ‘Shipment total.’

‘Total before tax.’

‘Order number.’

I’d say it looks quite legit.

‘If shipment has no associated tracking number, the client may not be available.’ Why is shipping not available for Helen Jones?

Think it looks okay. But I’m not going to put it as definitely legitimate.

‘Important password reset information.’ ‘Mail.adobesystems.com.’ ‘As we announced, we recently discovered an attacker illegally entered our network and may have obtained access to your Adobe ID. Currently have no indication that there has been unauthorised activity.’

‘Please visit adobe.com/go/passwordreset.’

‘On any website where you have used the same user ID and password.’

‘Please be on the lookout for suspicious E-mail offering scams.’

‘We deeply regret any inconvenience this may cause you. We value the trust of our customer, and are working aggressively to prevent these types of events from occurring in future.’

‘If you have any questions, you can learn more by visiting our customer alert page, which you will find here.’

‘Adobe Systems Incorporated.’ Okay, ‘Unsubscribe.’

Hmm. Mmm.

[Background noise, 0:29:31-0:29:43]

Hmm, Adobe Customer Care. I think it’s okay, but still don’t trust it fully. ‘Three’ or ‘Four’. A ‘Three.’ I’ll give it a ‘Two.’

‘FedEX.’ ‘Parcel has arrived.’ ‘Our post rider was unable to deliver a parcel to you.’ ‘To receive the parcel, please go to the nearest our office and show them this postal...’

Ah, wrong spelling, I mean grammar and spacing between the full stop and ‘Our.’ And ‘Priority E-mail postal office.’ You’ve got a funny E-mail.

‘Please do not reply to this E-mail. Follow the link below to your account to reply.’

Oh, ‘Easy roommate.’ Hello, Graham. ‘Click here to see the message and the profile. If the link above does not work, just copy and paste this URL into your browser. Regards...’

‘People that do not send many...’

(Laughter) ‘I@Westernunion.’

Oh, Frank. At Easyroommate.com.

‘Hi Helen. Click here to see the message and the profile. If the above link doesn’t work...’

Hmm. ‘UK.easyroommate.com.’ Hmm. I don’t know. It does look quite legitimate. But it should really tell me to log in to my website.

I’m going to give it a ‘Four’.

‘Send a payment to Keith. Approximating these at 100.’

‘You haven’t included a note.’

‘Shipping address, shipping details.’

Hmm.

[Background noise, 0:33:06-0:33:24]

I think it’s legitimate.

Hmm. ‘Update my information.’ ‘To lift the suspension, click here and follow the steps to reactivate your credit card.’

‘Suspended’ doesn’t need to be capitalised.

‘Your credit card has been suspended. Please update.

The subject heading, it just doesn’t sound right. And why is there an exclamation mark? Definitely phishing, because it wants my attention.

‘User Name, Helen J. Thanks for choosing Plusnet. Follow the instructions. Go to portal, log in, follow onscreen download instructions.’

‘If you’ve already got security software installed, this will be uninstalled automatically for you.’

Wow, that’s quite dangerous, right?

‘For more information, see our help pages.’

But the E-mail is correct, ‘Plus.net’.

‘If you need more help, use the help assistant, help.plus.net or call us.’

Hmm. ‘Thanks for choosing Plusnet Protect, powered by McAfee.’ Still Plusnet.

‘In those cases, if you’ve already got security software installed, this will be uninstalled.’

I don’t like the fact that it will uninstall automatically, so it should be phishing.

Oh. Can’t see any of the logos.

For that reason, I don’t know. ‘Just purchased an item from Googlebox UK.’ ‘I-offer Mail.’

I’m just going to go ‘Definitely phishing’, because I can’t see the pictures. And I don’t know what Googlebox UK is.

‘Please...’

‘Dear Pleasure Beach Visitor.’

‘TeamBlackpoolSurveys@S-PatMR.co.uk.’

‘To enter the survey...’

‘If you could spend a few minutes completing the questions, your views are important to us.’

‘Pleasure Beach Blackpool Team.’ What’s this KH numbering? Hmm. Who is S-PatMR.co.uk? Hmm.

It didn’t really say that I’m doing a survey through S-PatMR.co.uk, so I’m just going to say, ‘Phishing.’

‘DVLA are currently updating our database, and all drivers are required to verify their...’ (Laughter) Definitely phishing.

Can’t spell. And ‘DFT.’ Who is ‘DFT.co.uk?’ Idiot.

‘Dear Student, welcome to Lancaster. Hope you enjoy your first few weeks.’

‘When you came to Lancaster Uni and how you found it. Please...’

‘To give your feedback and to be entered into a draw to win one of three \_\_\_[0:37:51], complete a short survey.’

‘This survey is only open to current first-year undergraduates in the Faculty of Science and Technology. Survey will close on 20th November.’

‘Queries, contact Ross Malcolm, Lancaster.ac.uk.’

You all seem legitimate. So I’m going to say, ‘Yes.’ And the link seemed legitimate, Surveymonkey.com. But there’s a forward-slash-S, which I don’t know what the ‘S’ means.

But ‘University Undergraduate Survey 2013’ seems legit.

**P326**

P326: So, this one is you win [honours 0:00:05], you win. So you enter this address to show you the password of an NUS Extra account. ‘To review the password…’ \_\_\_.

Hmm. I would say it was definitely phishing. I’m not sure, actually. Because, put the address, but the length, email address is too long.

Yes, I would say maybe ‘Two’ because I can’t see the logo, that NUS logo. And this action was requested from the IP address, so I cannot get the sign. I would say, ‘Two.’

An eBay suspension. ‘We regret to inform you that your e-mail address has been security code found…’ ‘You will not run into any phishing…’

I would say it’s definitely phishing, because the e-mail address is a little bit strange. Because they have ‘CGI1’ before ‘eBay.com’, so, yes, and why did the e-mail address from the sender is, ‘Admit@ebayz.com’? It should be ‘ebay.com’ only. Why is that at the end of the ‘Y’?

So yes, I would say definitely phishing.

Hmm. I would say, ‘Tracking number’, I would say “Five”, maybe. Definitely legitimate. Because it doesn’t require me to enter or give any personal ID, credit cards or something like that. So just the e-mail to inform me that I have to go to the nearest Post Office.

Hmm.

[Break in conversation, 0:04:00-0:04:24]

I would say definitely phishing, because it says about my [Mobile group] but there is also an attachment for no name, and it’s a .SLP file. It’s not normal to have .SLP files from the company, and they usually use PDF files, and there is no name for the attachment, so it is very suspect-able.

I don’t know. PayPal. It’s a statement, and ‘Log in now.’

I would say the e-mail address from the sender is a little bit weird, because, ‘No.e.paypal.co.uk’ should be, like, ‘Paypal.co.uk’. Because it asked me to log in, so if I put my password and e-mail account, they might be knowing my password.

So I would give that a ‘Two’, because yes, it has the formal PayPal logo and it looks pretty formal. So, ‘Two’.

Hmm, it’s a job application, and I would say definitely phishing, maybe. No, it’s not. Really not. ‘Please click here to download an application.’ I would give it ‘Five’, because it seems like there’s nothing involved with money, so hmm.

Yes, I would say, ‘Five’ for that.

[Break in conversation, 0:07:28-0:07:50]

Hmm. I think, I would say it’s definitely phishing, because it is not secure to upload the security code. And normally you just have to fill in the security code every time when you press ‘release’. Yes.

Hmm, I think this is definitely legitimate, because yes, there is no money involved, and the address from the sender is quite normal. There’s nothing suspicious.

And yes, they have the logo of Dropbox as well, so I would give a ‘Six.’

What’s this? ‘Someone recently tried to use an application to sign into your Google account. We prevented this sign-in attempt. This was…’ \_\_\_[0:09:35]

It’s so difficult. I would give this a ‘Six’ because, but they have two journal attachments. I’m not sure why they give me the attachments, because if I need to change my password I don’t need any attachments.

Then I will give it a ‘Five’, because there are suspicious files, and yes. ‘Five’.

This one. ‘Upgrade the mail.’ ‘Validate your e-mail’. ‘Upgrade.’ I think I would give it ‘One’ because the address is not related to the sender. It seems like it’s from an educational institution, and the link is about upgrading the mail. So I would give it ‘One.’

Hmm, ‘An attempt to log in was detected by our security system, and this account will be disabled if you ignore this message.’ Hmm. ‘If you are not authorised…’

I would say, hmm.

[Break in conversation, 0:12:20-0:12:33]

I would say it’s definitely phishing, because, is it? ‘If you ignore this message,’ but maybe…

I would say, ‘Five’. Because I only look at the e-mail and I haven’t clicked into here to begin to resolve the issue, so if I look for that and know that I have to give my password, then I would say it is definitely phishing.

But if I click into the link and they just teach me how to resolve the issue, maybe give me the phone number to call to the bank, then I would say it’s quite legitimate. So I would give it, ‘Three’, though.

[Break in conversation, 0:13:46-0:14:01]

Hmm. What’s that? ‘All students receiving grants and loans from the Student Loans Company. We have to…’

Hmm. I would give it, ‘One’, maybe.

\_\_\_[0:14:30-0:14:37]

Because the link is quite weird, it’s ‘Myface’ and it should be something related to student finance, and the e-mail address from the sender is not government at the end of the address. It’s ‘SLC.co.uk’, so it might be not official. So it’s definitely phishing.

‘You just received a message from Grandpa in \_\_\_[0:14:34].’

I would say, yes, I think it’s legitimate, because it’s related, the e-mail address from the sender is related to Easy Roommates, and the link also has the Easy Roommates, so it’s fine.

‘Bidding eBay.co.uk’. I would say it’s definitely legitimate, because it’s only telling me about the invoice and bidding. And yes, there is no money involved. Yes, there’s money involved, but it didn’t ask me to send any money, or put forward any personal identity or credit card passwords, so it’s fine. It’s ‘Six’.

Yes, and hmm, from \_\_\_[0:16:59]. I think this one is also, ‘Six’, legitimate, because it’s only an e-mail invoice, and yes, it’s \_\_\_. Yes, it’s fine. I’ll give it, ‘Six’.

Mmm, ‘Change to determine…’

I will give it ‘Six’ as well, because it’s only to remind me of the updated terms and conditions, so it’s just a statement, really. So it’s fine.

Hmm, I think it’s fine as well, because it just reminds me that Google’s [boss route 0:18:09] has received my payment. And yes, and the e-mail address and the link is also related, it’s I-offer, so it’s fine.

‘Recruitment’. I would say it’s also fine, because it doesn’t ask me to give in any personal identity. So it’s fine.

‘Important password reset information.’ I would say, hmm.

[Break in conversation, 0:19:10-0:19:28]

I would say, “It’s fine.” It’s definitely legitimate, because the address which asked me to reset and create a new password is, ‘www.adobe.com’, so it belongs to the company, so it’s fine.

I can’t read the words, it’s so small, but I think it’s fine as well, because this only asks me to complete a survey, so it’s fine.

[Break in conversation, 0:20:27-0:20:39]

I would say it would be, hmm, I would give it, yes, I would give it ‘Six’, because if I just bought the software, then I would know this e-mail would come, but if I didn’t buy it, then I wouldn’t click onto it, so it depends.

Okay, just say I have just bought the software, so I will give it a ‘Six’.

Hmm. This I would definitely choose, ‘One’, because I don’t know, it’s like your advertisements but it’s very close, and yes, I think you’d get some virus. So I’ll give it ‘One’.

I would give it ‘One’ as well, because there’s no Facebook logo, and the address is very weird. e-mail address from the sender, it’s ‘Notification of…’ something I don’t understand. So it’s not official, I think.

Hmm, I’ll give it ‘Six’, though, because it’s only an invoice, so it’s fine.

[Break in conversation, 0:22:46-0:23:08]

I would give it a ‘Six’ as well, because, yes, because if I’m trying to sell my personal [Dynamo 0:23:30] free account, it’s only to inform me that I can’t sell it. So it’s ‘Six’.

‘Securities…’ I would give it, ‘One’. It’s definitely phishing, because the e-mail address is so weird. It’s ‘UUP@DiWickedLoan.com’.

And I don’t know that my account would be expired, bank on that account. So it’s, ‘One’.

Yes, it’s ‘Six’ as well, because it’s just a shipping confirmation, so it doesn’t equal anything. So it’s fine. I would give it, ‘Six’.

Hmm. Well, if my credit card has been suspended, the bank might call me or I have to go to the bank in person, so yes, I’ll give it, ‘One’.

‘I am suffering from lung cancer in terminal phase…’ Hmm. ‘Click on to \_\_\_[0:25:34].’

Well, hmm. I would give it, ‘One’, because it’s so weird. Yes. Why does this guy have any relatives? I have to fill in my last name.

Yes, I would give it, ‘One’. I don’t know this guy. So.

‘Your latest statement is ready for you,’ oh, well, it’s so difficult to tell with this one.

Hmm. I would give it, hmm. I would give it, ‘Six’, because the e-mail address from the sender is ‘Natwest.com’. It’s fine, I think, yes.

[Break in conversation, 0:26:56-0:27:14]

Yes, I would say definitely phishing as well, because yes, if, yes, I would give it, ‘One’.

[Break in conversation, 0:27:44-0:27:55]

Oh, it’s ‘One’, definitely, because the address from the sender is ‘Support@GreenNet.com’. It should be Barclays, isn’t it? Yes.

And, yes, if there’s any unusual activity in my account, the bank might call me several times before taking any action, I think. Or maybe at the same time, so…

I’ll give it ‘Six’, because the address from the sender is quite official. It’s ‘.Goverment.uk’, so it won’t be any weird thing.

It’s only a survey, so it’s fine. I give it a ‘Six’ anyway.

[Break in conversation, 0:29:00-0:29:18]

I will give it, ‘Six’ as well, because the link that I have to click is even with the ‘Government.uk’, so it’s fine, it’s official, I think.

Hmm. Well, I would give it ‘Six’ as well, because the address from the sender is from Lancaster University, so it’s a student from the university or staff from the university. And it’s just asking me to give my feedback, so it’s fine. I give it, ‘Six’.

**P327**

P327: Alright, definitely phishing. ‘Click here’, that’s a definite sign. Okay, I have got PayPal emails before, and I think that is how it’s supposed to be. Yes, it’s definitely legitimate. Amazon. No, Google \_\_\_[0:00:55] UK. Yes, this is fine, I guess. Okay, moving on. ‘\_\_\_[0:01:16], because \_\_\_ card information, to [renew] your \_\_\_ and follow the steps in order to \_\_\_.’ Hmm, okay, yes, this seems legitimate, I guess. They’re not asking for any information. Okay, scam, scam. I’ve got these emails so many times before. No, definitely a scam. Okay, yes, this happens, this is legitimate. They’re not asking for anything else, so… [No, that’s not it 0:02:17]. Why would they expire an account? It’s not phishing, it seems. ‘Log in’, so yes. I don’t think this is phishing. Okay, the wording on this email seems to be too professional for it to be a phishing scam or something, so I’m going to go with number six, definitely legitimate.

‘\_\_\_[0:03:14] [email].’ Hmm, never been suspended before, but this seems legitimate enough. They’re not asking for any other information. Okay, I guess this is fine. They’re at least asking for us to not send money, so I’m going to go with four. Not totally convinced, but yes, it’s fine. Hmm, this seems fine too, I guess. Okay, this is kind of like Facebook. I’ve got these emails myself. [Okay 0:05:26], they don’t ask… No, they do ask for a password sometimes, the [NUS], but \_\_\_ [seems] super fake. I’m going to go with ‘phishing’. Three, I’m on the fence with this one. I don’t think this is the right email. I’m going to go with ‘phishing’, because Google \_\_\_[0:06:24] UK would have sent the email on its own, and it will link itself, it will do something, showing something, and the message is a section, and that’s not right, I guess. [Calls are being recorded 0:06:54], \_\_\_. It’s fine, I [think it is]. I’ve never received \_\_\_[0:07:15] before. I guess that’s fine. I guess that’s fine, it’s \_\_\_ professional. \_\_\_[0:07:41], yes. ‘\_\_\_ your account ending 101-something’. That’s what they do. I’m going to go with ‘phishing’ on this one. No, that seems kind of shady. Okay, phishing. This is clear phishing because, ‘Please click here to download application form’, that is not something they would ever [ask for 0:08:48], yes. \_\_\_. ‘\_\_\_ [entertainment]’.

No, they would never send me an email like this. Oh wait, [they might]. Let me just see, yes. Three, not so sure about this anymore. No, I think this is a scam, because they shouldn’t mention the bank account. I’m going to go with three on this one again. No, this site is not [coinciding 0:10:14] with the email address, I guess. No, this isn’t [right]. Okay. ‘\_\_\_ account number \_\_\_, [1989]. Thanks for choosing bla bla bla.’ McAfee, oh God. No, I’m going to [give that as scam 0:10:38]. No one does that. Okay, ‘\_\_\_. Thank you for your \_\_\_. [Case number] okay, \_\_\_, okay.’ No, I’m going to take that as legitimate. Okay, so \_\_\_[0:11:05] [scam like this] so many times, and \_\_\_ this one, they’re just phishing. Alright, so, ‘\_\_\_ used the applications, \_\_\_ Google \_\_\_.’ Alright, this seems fine. I’m not going to \_\_\_[0:11:30] this as phishing, because it’s no good. ‘\_\_\_.’ Hmm, I guess it’s fine. I’ve never had this before, though. Oh, good. ‘Your password has been…’ They’ve given the tracking number. That’s fine, [I guess 0:12:00]. Why is the website different from the sender? I don’t know, let’s put that as a four. Invoice number, yes. This seems fine. Okay, this seems fine too, I guess, though I have no idea what a \_\_\_[0:12:59] [flex card] is.

Oh, no. Oh, no, no. Never. Oh, I guess it could be, one second, because the [site] coincides with… The email address coincides with the site. I’m going to go with ‘legitimate’ on this one, I guess. Why would they..? Yes, okay, seems fine. Oh, Amazon. Yes, okay. I have got emails that are just these, so I guess these are completely fine. Yes, legitimate. I’ve got emails that are just these. Why is it from \_\_\_[0:13:52]? That’s \_\_\_. ‘\_\_\_, thank you for \_\_\_.’ Oh, I guess this is fine. They aren’t asking for anything personal, just a survey. No, this is a governmental site. They say .co.uk and not… Yes, it should be governmental, I guess. I’m not convinced, so let’s… This is a phishing scam. ‘Welcome to \_\_\_[0:15:02].’ Oh, yes. I’ve got these emails. Okay, since I’ve got the exact same email, I \_\_\_ [survey]. I’m going to use this as a \_\_\_ [legitimate].

**P330**

P330: [Set the first up 0:00:04]. Direct Gov. From \_\_\_, so their email address looks legitimate. [It's legit to do with an update], so view. 'This is a formal notification of an update. Due to a recent update of \_\_\_, we'd like to update your account. Click here to validate your \_\_\_. Fill in the requested information [exactly as you find it].'   
  
I think legitimate, because… Oh, no, finance E. An extra E. So it's phishing, because why would they email you to validate your information? DirectGov doesn't do student finance, I don't think. So definitely phishing.   
  
PayPal. From PayPal.com. PayPal \_\_\_[0:01:13], whose email address is approximating \_\_\_. Yes, that looks okay. That looks pretty legitimate. 'Please do not reply to this email. For assistance, log on to your PayPal account and click Help.' So there's no [links for it 0:01:40] to try to get anything. So I'd say legitimate for that one.   
  
\_\_\_ mail to info@hsb. 'HSB incoming funds blocked. \_\_\_ business account with us has been blocked \_\_\_[0:02:00].' This is a typical phishing one. It's got a link in it to resolve your issues, and banks tend to do that. I think banks tend to ring you, and go in.  
  
Visa no reply, and verified by Visa.com. 'Your credit card has been suspended for this update.' Again, there's another link in it, so it makes you feel like it's phishing to try to get your information off you. Also, the fact that suspended is also in capital letters seems a bit strange. It's not very good grammar, and \_\_\_[0:02:54] in capital letters.  
  
Adobe customer care, email@mail. Yes, '\_\_\_ may have obtained access to \_\_\_[0:03:16]. To prevent an \_\_\_, we have reset your password. \_\_\_ change your password.' That seems legit. They are apologising for what's happened. It's also got a pretty good unsubscribe link at the bottom, which normally, if it's a phishing one, it'll have a couple. I'm not completely satisfied with it, so I think I'll go for a four.  
  
eBay suspension. admin@ebay is with a Z, so I have a feeling that that one will be phishing, because eBay's email address is definitely eBay. Yes, that's phishing.

[Break in conversation 0:04:27 - 0:04:40]

service@paypal. At least the email is the same [for both]. They've just noticed that it's about to expire. But at the same time, you wouldn't really want to click the link to update your card. But it does say, 'If you've already updated your PayPal account with your new card details, disregard the email.'   
  
So it seems like they're trying to get you to just re-sign up. It's a bit like the other one. I think I'll go for a four, because I think it's legitimate. No, I'll go for a five. Four. I think it's legitimate. The email address looks good, and it's a similar thing to PayPal. Just the fact that they're not telling you to go on your account, and they did before.   
  
iOffer, no reply. 'Congratulations, you've just purchased an item from Gogglebox UK. This is an automated email. Please don't reply.' No reply iOffer. It says there, 'Click below to pay,' which makes it seem a bit dodgy. Because surely, if you'd bought it, you've already paid. I'd say a two for that one. It seems quite dodgy ground. If I hadn't been on iOffer, then I definitely wouldn't think I'd ordered anything from there. The email doesn't seem very convincing.   
  
Another PayPal one. Paypal@e.paypal.co.uk. They do send ones [to show you 0:07:01] your recent transactions, but how do I know this is not a spoof email? \_\_\_[no greetings and such, just 'Dear PayPal] \_\_\_.' Emails from PayPal always address you by your first name, but they've got quite sophisticated over the years. So I don't think it necessarily means- [It does have a lot of 0:07:25], 'How do I know this is not a phishing email?' which strikes to the contrary.   
  
It doesn't seem too phishing, but there's a lot of mention of not phishing, which worries me.   
  
Plusnet support, support@plus.net. It's talking about some software to upload.

[Break in conversation 0:08:01 - 0:08:15]

You go to there, 'log in with your account and user names.' So [they'd have] your private stuff. I've never had a Plusnet email, so… They've got some numbers to ring. I'll give it a five. I think it's legitimate.   
  
Oh yes, this is one of these ones. Yes. It's BT Internet P \_\_\_[0:08:57]. Oh yes, of course, a classic Nigerian prince one. Yes, that's definitely phishing, because that is not really what happens.   
  
'Re item waiting [on 0:09:21] delivery day. Shipped your item. This completes your order.' That looks pretty legitimate, but it's got no email address from Amazon. \_\_\_[0:09:44] [Carla Craig], which is strange, but… It knocks down the legitimacy. Also, 'ON' in capital letters. \_\_\_ has no associated delivery tracking in there, which is strange for something that's £15.00 shipping. 'Returns are easy.' They start with capital letters \_\_\_[0:10:16] returns centre. I think it would be three.   
  
Dell. 'Dear valued customer,' so not addressing you by your name, which seems [weirdo]. dellsurvey@helpmailto[RAP].tnsonline.

[Break in conversation 0:10:42 - 0:10:56]

'The results of our survey will not be used for sale purposes. Individual responses will be combined.' Privacy protection. 'To be removed from this list, reply with 'Remove' in the subject line, or click here,' and it looks like phishing. Normally, it would say, 'To unsubscribe…' \_\_\_[0:11:26].  
  
From [Sgrenata] to [washcol.edu]. 'Your password will expire in three days. Click here to validate your email.' Mmm. The email is not from Washington College Education, so maybe. I'd say a four. But your password expiring, it doesn't seem likely, but it could be one of those new reset passwords. I think we'll go for a four.   
  
NatWest. Onlinebanking@information.natwest.com. 'Hi, your latest statement…' then it's just giving your account number ending… 'Just log on to see more information on your account. If you need more help understanding \_\_\_[0:12:40]. We will never contact you asking you to provide your security details.' \_\_\_ just said that \_\_\_, so I would think that's legitimate. I'm not 100% certain, but pretty certain.   
  
Nonameforattachment.zip thanks@virginmobile.com. 'The bill for your Virgin Media mobile is now ready to review. The balance of £16.94 will be taken by direct debit on or immediately… [My team will be 0:13:17] picking up emails from this address. No, I don't think that's very true. The nonameforattachment is quite suspicious. It should at least say, 'Invoice,' or 'Bill.'   
  
'Subject suspicious sign-in preventing.' Noreply@accounts.google.com. 'Someone tried to use \_\_\_[0:13:50] to sign into Google account. We prevented it, in case it was a hijacker.' There's a lot of attachments attached to this. I have a feeling that's phishing. Also, the fact that they emailed the Lancaster account with a Google mail issue suggests something's a bit strange.   
  
[Blank 0:14:26]@easyroommate.com. 'You have mail. Log into your account to reply. Committed to finding you the right flatmate. Do not send money via Western Union.' No, of course not. I think that's phishing. 'Click here to see the message and the profile,' and stuff.   
  
HMPS Recruitment. 'Dear Candidate, a job which matches your \_\_\_[0:15:02] criteria has been published on our website.' HR recruitment team. Strange that the grade is the same as the job. So I don't think that's quite right.   
  
[Gary Cooper 0:15:31] in a medical institution suffering from lung cancer. Yes, 'Kindly leaving my fortune to good use.' Mmm. 'With no heir apparent. Contact me with your full name to complete the procedure.' Yes, that's phishing.   
  
Barclays online support. 'Dear \_\_\_[0:16:05].' Yes, 'Click here to verify your account records.' Support@vnet.com. I don't think that's true, because it's not come from a Barclays email. Vnet doesn't sound anything to do with Barclays. I think that's phishing. I'm not 100% sure, but…   
  
hrimprovementdepartment@yahoo.co.uk. 'Dear Applicant, thank you for your interest. \_\_\_[0:16:43] attached the application \_\_\_.' Yes, I think that might be phishing. It's asking you to download an application form, without it being… Just the attachment seems strange.   
  
'Yahoo and Gmail user, click here. Good day. \_\_\_[0:17:11] [you've just won a luxury…]' That's definitely phishing.   
  
Dropbox. 'Dropbox needs to verify your email address before you can share folders.' Yes, I think that's legitimate. noreplydropbox.com. Verifying your email address is pretty standard.   
  
\_\_\_[0:17:33] Entertainment. 'It's come to our attention… If you don't wish to get suspended…' Well… I think that might be a phishing one.   
  
'There have been changes,' from [noreply@battle.com](mailto:noreply@battle.com). \_\_\_[0:18:00] of [entertainment]. Also, 'If you had already authenticate or your account,' doesn't really make any sense. I wouldn't think it would send that out like that.   
  
eBay invoice. billing@ebay.co.uk. Yes, automatically generated one. 'Don't reply.' They're not asking you to do anything; just, 'If you want to view your invoice…' They haven't asked you for anything. It's probably legitimate.   
  
FedEx. \_\_\_[0:18:56] with no space. That's strange. Oh yes, @dtf.9193. Yes, I don't think that is legitimate, really. Also, the tracking number is different to the order number, which is not unusual, but strange. And, 'Dear Customer;' no name, even though it's post, so they should know your name.   
  
NatWest. Oh well, okay. uup@[dankytaiwan 0:19:41] doesn't sound like a NatWest email account. Obviously, you've got to log into your online banking, which will take you to some kind of NatWest fake site.  
  
SLC. directgov@slc.co.uk. 'Students, be web safe, [just using 0:20:03]… Students receiving student loan company…' No. 'Student loan company' changes into 'Student financing' at the end. 'Fill out your information securely.' I don't think so.   
  
\_\_\_[0:20:23].com. I think that's a phishing email. 'You or someone else has entered this email address to change the password of an NUS extra account,' with a really big link. 'To find out about the address-' No reply. That seems quite legitimate, but then if… I'm not too sure on that one \_\_\_[0:20:57]. It doesn't really seem like the normal thing they would send.   
  
Caxton FX cards. 'We recommend you to retain a copy.' \_\_\_[0:21:29]. 'Please take time to read your updated terms, which are available here.' They're not really asking you for anything. I'm not so sure on that one. It seems more legitimate than phishing, but I'm not 100%.   
  
Facebook. notification@facebookmail.com with some strange letters in the middle. I think that's phishing.   
  
noreplyioffer.com. This is the same one: '\_\_\_[0:22:18] received a payment.' You can click to view the status of your purchase without being asked to pay for it. It says, 'You've paid. You're a guest user.' I'm not so sure on that one, but it seems a bit strange.   
  
surveys@\_\_\_[0:22:49]. So it's just a survey after visiting Blackpool Pleasure Beach. \_\_\_ subject, which seems unusual. 'Everyone taking part will be entered into a draw to win season passes giving unlimited entry to Pleasure Beach for a whole year.' It doesn't look like any unusual grammar or anything. There's nothing to suggest that it is Pleasure Beach. There's no header or anything, so it does seem unusual.  
  
dvlainfo@dft. I don't think that's how the DVLA work. I don't think you would lose your licence and have to take a fresh driving test. They certainly do not do that.   
  
\_\_\_[0:24:15] Lancaster. 'Dear Student, welcome to Lancaster. We hope you have enjoyed your first few weeks.' SurveyMonkey. They're always sending SurveyMonkeys, so I'd say that's legit. [Property of 0:24:30] science survey 2013. It was sent in 2013. 'Enjoyed your first few weeks.' It was 8th October, so possibly. Yes.

**P331**

P331: Firstly, then, hello [John 0:00:18]. You recently entered the new contact email address. To confirm your new contact email address, follow the link below, and then there is available link. If clicking on link doesn’t work, try copying and pasting it in your browser. If you did not enter this address as your contact email please disregard this message. Take a look at link. \_\_\_[0:00:44].

You have recently entered a new contact email address. What does that mean? Wait, so, clicking the available link and then entering your name and password is, like, the easiest way to get your get your Facebook [followed 0:01:10]. So I would rather not [do] this. Facebook mail dot com. That does not sound exactly legitimate, the email address they send it from, and I just put one because the email is definitely phishing, definitely illegitimate.

No reply, no extra dot co dot uk. No reply. Okay, that sounds like a [legitimate 0:01:49] email. That’s a bit long link. You or someone else entered this email address to change the password in \_\_\_ dot com. To continue the password reset process, please proceed to this link. Hmm. Create a new password \_\_\_[0:02:11] extra. Cars dot [nosextra] dot co dot uk. It’s \_\_\_. Hmm, interesting. I’m trying to find, like, a pattern or something in the link, or to spot that the link is fake.

For example, some phishing links might not say [‘double, double, double’ 0:02:46], dot something, but just two doubles. And you might overlook this if you’re in a rush or something, and then you get phished. But this link is too random and long to be analysed or something, I cannot see anything.

[Silence 0:03:07 - 0:03:32].

Four. Five, okay, five. Five. I just can’t find anything. And the address \_\_\_[0:03:46] nosextra dot co dot uk seems okay. Yes it was five and not six, because I had some doubts. Okay, next email. \_\_\_[0:04:11] Your latest statement is about \_\_\_.

[Silence 0:04:12 - 0:04:38].

Okay, this is definitely not phishing. First, from NatWest and then \_\_\_[0:04:51] actually is in [arrows] so we have this contact or something. And then there is no way to \_\_\_ you actually get \_\_\_ there are just simple links. So this makes me think that the last email was phishing, definitely illegitimate. No reply, I offer \_\_\_[0:05:20], I offer mail, okay. You’re a guest user, \_\_\_ [we’ve] received your payment regarding this item. Click below to review the status of your purchase. Thank you.

I offer this \_\_\_. I offer messages. Mini-series. Why does mini-series? Why is there? Is \_\_\_[0:05:57] mini-series? And what is global \_\_\_? Maybe it’s a site, maybe not. I offer sounds cheap, sounds like phishing. I offer messages. But if it’s just a link and then you just check your payment and you don’t write any additional data, how bad could it be? Virus? Maybe it’s a virus. Okay. So this mail’s phishing. This I would give [three 0:06:56], because I’m not sure.

Actually, I give two \_\_\_[0:07:10]. Lots of phishing through PayPal. [Series] at PayPal. Approximate \_\_\_ 100 \_\_\_. What... From… Hmm… This seems like it’s not phishing. I’m just looking through the email, the whole structure looks legitimate. There are different colours, there are relevant links and then there is, like, the sort of invoice is looking legitimate. Shipping countries...

[Silence 0:08:33 - -0:08:46].

This is legitimate. You actually… Actually, I don’t see that this is legitimate, I believe. Because, actually, they don’t require from you to make any action, you just read it and, if you don’t take action I don’t think you can catch a virus or anything, so it’s legitimate. There is no way this email will hurt you, just be reading it, I believe.

[Silence 0:09:20 - 0:10:05].

Okay. So, someone tried to sign in to your Google account. Hmm. But, why would they prevent the [signing authent 0:10:26]? It could have been you, right? If you used the right password and correct data and everything, why would they prevent him to log in, yes? It was just you, they don’t know it was someone else.

[Silence 0:10:43 - 0:11:09].

If you do not reply to this [sign authent 0:11:13]. Weird. This is phishing. This is phishing because they ask you for a password, things like that, and, in my opinion, I don’t believe that they should be preventing something, whatever they think, it’s phishing. No name for attachment zip. Thanks [and 0:11:45] and Virgin Mobile. Is that the correct \_\_\_? Virgin Mobile \_\_\_[0:11:52].

[Silence 0:11:52 - 0:12:15].

This seems like phishing because it’s too cheap, plain. There is not, like, a red strip saying Virgin or something, and \_\_\_[0:12:31], I would say one.

[Silence 0:12:37 - 0:13:06].

Oh. Wait, this seems legitimate but I just have a problem… In most cases, if you have already got security software installed, this will be uninstalled automatically for you. Why would they uninstall all security software? I mean, you could have 50 security softwares, there is no problem it would interfere with one another, in my opinion, of course. So, this is phishing, all of it seems \_\_\_[0:13:42]. I’m not sure. Plusnet Protect, yes, okay.

It seems legitimate, but I don’t like this sentence so I’m giving it two instead of a one. Hello Mr [Gary Cooper 0:14:04]. Hello, and Mr Gary Cooper, yes, okay.

[Silence 0:14:10 - 0:14:38].

Can you contact me your full name and your phone number? How can someone do you harm if he knows your phone number and your full name? Maybe he’s trying to get your number? Right, so this is definitely phishing. There is no reason for [he’s 0:15:07] meant to give you his \_\_\_, especially to you. What are you saying \_\_\_? It was relevant to the receiver.

[Silence 0:15:25 - 0:15:50].

Oh, okay, okay, okay. So they give the full name and phone number and then they ask for a bank account. But this email would not actually hurt you until you give your bank account, yes. Email \_\_\_[0:16:07] outlook, ID, \_\_\_ Skype. What? Okay, okay. This is phishing, I would say this is phishing although it would not hurt you to give your name and number. But then you might, maybe something will happen. It’s just complete nonsense.

Dropbox\_\_\_[0:16:31]. Dropbox needs to be\_\_\_. Please verify your email address by clicking on the link below. Verify your email address, verify your email address \_\_\_ how does that happen? You click the link and then what does it do? What happens after that?

[Silence 0:16:50 - -0:17:02].

Okay. So, this is extremely easy to see if you verified your email address because I think you should actually make a request for your email verification. And why is this email so short? Although [it seems 0:17:30] legitimate and it’s from no reply from Dropbox dot com. So, given the tasks that [there are] phishing emails, I’m always inclined to believe that someone is phishing but, if I had received an email like this and it’s relevant to me, I would say it’s definitely legitimate yet it’s [social 0:18:08] so I give it a five instead of a six \_\_\_.

[Silence 0:18:13 - 0:18:25].

Get postal receipt. Why [get 0:18:35] postal receipt? I think if you click on the get postal receipt, this would open a new link and that’s phishing, because they could just put their receipt as an attachment to this email they are sending you. Fedex, is that their logo? Purple and red and the email of the sender [DTF] dot 193 [for when]. Yes, phishing. I give it a one.

[Silence 0:19:14 - 0:19:42].

The paper actually remind you if your card is about to expire? \_\_\_[0:19:49].

[Silence - 0:19:49 – 0:20:08].

Okay \_\_\_[0:20:10]. Please note \_\_\_ reply to this email [following] the link below \_\_\_ to reply.

[Silence 0:20:16 - 0:20:35].

[Frank 0:20:53] \_\_\_.

[Silence - 0:20:56 - 0:21:21].

Do they send [you 0:21:21] messages..? So, he sent you a message in this website which is easy roommate dot com and UK \_\_\_. The links actually look like this. Again, I’m looking at the link and then we have, like, source and easy \_\_\_[0:21:45] internal \_\_\_ contact application \_\_\_ application. Interesting. Maybe look at that link is not the right way to go, assuming that the links have been created for the purpose of this task. And [this 0:22:07], even if [they] are supposed to be phishing, maybe they’re not legitimately phishing link but, yes, okay.

But I believe, yes, anyway. I believe it should be easy roommate dot co dot uk and not uk easy roommate dot com. But maybe that is just [returned 0:22:31] because maybe there is an easy roommate site that looks like this in the UK. I have no knowledge, I am not from the UK, but I would say this is a two. I see no reason. Subject, you have mail. Subject, okay. The subject annoys me a lot, you have mail. That’s not a legitimate subject. This is phishing.

I don’t know would it hurt you and how they would benefit if you click this link, but I give it a one because I don’t like the subject. \_\_\_[0:23:22] obligation for [HR], okay, HR recruitment department, HR dot [dep] \_\_\_ yahoo dot uk. Okay, so, HR departments now have emails from yahoo. Sure. Please click here to download application for… Yeah, right. Again, I have not the email but this is completely phishing. Again they have, sort of, attached the application form and their email address is absolutely, what’s the word? Yes, it’s not legitimate.

\_\_\_[0:24:23]. Mail to dot \_\_\_. Okay, so this is [a legitimate] email address. \_\_\_ that the business account with us has been blocked for receiving payments.

[Silence 0:24:45 – 0:25:03].

When? When was it blocked? \_\_\_[0:25:12]. More information before I click the link. Your whole business account was blocked and they [can’t] write you four lines of text, I don’t think so. It, as a whole, there is not much to say that it is phishing so I would say, okay, I’d say one. You can’t just block your business account and receive four lines. Email, it should be longer, more information. [Gucci 0:25:56], Cartier, Rolex. Okay, you received an email from Gucci, Cartier and Rolex.

Okay, this is definitely phishing. Good, they give me a lot \_\_\_ luxury \_\_\_. Not in a million years. That was absolutely phishing. No, it was not even an email it was \_\_\_[0:26:30] or a joke. It was \_\_\_. So this is an email but [is] no reply at verified by Visa dot com. Maybe, no reply. Why \_\_\_ at verified by Visa? Why isn’t it just Visa or something like that? Maybe that’s an actual site \_\_\_[0:27:05]. Let’s read the email.

[Silence 0:27:05 - 0:27:21].

No, no, no. Okay, they suspended your credit card information. The reason for the error is not certain but, for security reasons, we have suspended your card temporarily. How can they suspend your credit card for, sort of, uncertain or unknown security reasons? They will get sued for that. How could they link your finances if they are uncertain? An error. Again, I think there should be more information about this error. At least when it occurred, or something like that.

Click here to leave this \_\_\_[0:28:13]. And then after [the click] there are three, sort of, arrows which you could normally see in the pirate sites or phishing sites. Yes, okay, I give it a two because it seems kind of legitimate but there are things that are phishing. Okay, yes, I will give it a two. Click here. Maybe it’s legitimate. Okay. I’ll give this one a three, okay, a three, because the ‘click here’ kind of, maybe, is not that phishing after all, erm, I’ll give it a three, that’s what I believe.

Dear candidate, a job which matches your \_\_\_[0:29:06] criteria \_\_\_. Reference, psychological assistant \_\_\_ organisation. Send. Great. Psychological assistant. Good luck with your job search. HR recruitment team at [i dash grasp] dot com. [HBMS] recruitment. Okay, see, that’s what they’re talking about. [Double, double, double 0:29:30], twenty-one dot [i grasp]. No, that’s not what I’m talking about. There are legitimate websites with such links.

Or is it just ‘double, double, double’, [two 0:29:52]? Okay. Organisation, send. I’ll give this one a three because I’m uncertain and I’m more inclined to think that it’s phishing because I believe the link should be ‘double, double, double two’ not ‘double, double twenty-one’.

[Silence 0:30:27 - 0:30:47].

Support at [vignette 0:30:49]. What is vignette? Is there such a site? Vignette? [David Brown] security assistant, [Major Bradleys]. Why would he sign your email? Which is only if it’s just a standard email. Okay. So it seems legitimate but…

[Silence 0:31:19 - 0:31:32].

[And there is a 0:31:34] limit that you’re [going] to, sort of… Okay, I will give this one a five, because [the] link, they don’t suspend your account or something. Your password will expire in three days. No. No. Upgrade with [mail HTML 5 0:32:13] dot [mead]. No. This is phishing. [Tanks] system administrator. ‘S’, ‘G’, ‘R’ \_\_\_ [Moscow] dot [EU]. This is phishing. I give it a one. Dear valued customer, complete the survey, mail to \_\_\_[0:32:39]. I’m just reading the email.

[Silence 0:32:48 - 0:33:26].

Okay.

[Silence 0:33:26 – 0:33:39].

They have-They are saying, for a copy of \_\_\_[0:33:41] privacy policy go to \_\_\_ dot com, slash privacy. So this inclines me to think that, erm, this is a legitimate email, because you can go and read the privacy policy although, if it were a phishing email they could just write that down. I don’t think anyone would care to check the privacy section of their website. And, yet again, what is this [wrap two 0:34:17] dot \_\_\_ dot com slash ‘S’ dot [SA].

Did this email, mail to dot [wrap DNS] online. Okay, so the email address of the sender and the website address of the link, of the survey, seem phishing. Yet overall it seems, kind of, legitimate, so I’ll give it a two instead of a one. Okay. It’s completely legitimate. From [Carol Creek 0:35:05], no email address.

[Silence 0:35:06 – 0:35:27].

Yes but you will get [to clicking 0:35:31] just your orders but [there are zero] links for that. Okay, and they [shipped it] and this at nine o’clock, nine thirty, so it’s, so it will arrive tomorrow.

[Silence 0:36:00 – 0:36:12].

I think this is legitimate, although it’s from Carol Creek and the subject is [red dot item waiting for delivery 0:36:19] today. Your estimated shipment date is… So they ship your item but your estimated shipping date is 21st. Alright, there is something phishing about this, although I don’t think clicking your orders would hurt you. I will give it a four because it says that they have shipped your item yet your shipment date, your estimated shipment date is tomorrow.

Why would they say that in an email? They said they have shipped your item and [why 0:37:15] they ship it in the morning? Normally items are shipped in the evening, I believe, and they’re out for delivery in the morning. So I give it a four. It seems legitimate overall yet \_\_\_[0:37:40]. Directgov, okay, this seems really fishy. Student finance with two e’s, no. No. Why? No, no. Definitely phishing. I give it a one. \_\_\_[0:38:14] visited \_\_\_. Oh, okay, okay.

You see…

[Silence 0:38:30 - 0:39:14].

\_\_\_[0:39:14] mobile [authenticate] in the form of email. No. This is definitely a virus and \_\_\_ is [dot net] not \_\_\_ dot com. The email address should be dot net. Yes. And this \_\_\_[0:39:40] auto indicator or something, yes. This is so phishing. One. Congratulations, you just purchased an item from Google \_\_\_, [‘The History of Men’] mini-series. \_\_\_[0:40:00] that’s how you write \_\_\_ you should receive an email \_\_\_ shipping \_\_\_ made a mistake.

They already see this email? \_\_\_.

[Silence 0:40:17 - 0:40:38].

I give it a three because it does not directly ask you to make an action but it seems like it’s phishing, yes. Important \_\_\_[0:40:54] information.

[Silence 0:40:54 - 0:41:11].

Okay. Email at mail dot \_\_\_[0:41:17] systems. Maybe that’s the email address they chose, maybe that’s it. Read online. Okay, I would normally give this a six because it seems extremely legitimate but I don’t like the email address. Generally I don’t assume that anything is… Okay, okay, that’s six, okay. It seems legitimate. It seems legitimate. Invoice number…

[Silence 0:41:59 - 0:42:11].

Yes, definitely legitimate, everything about it is legitimate. They say how to, [if 0:42:21] your invoice without a link, everything is absolutely legitimate here, about this email.

[Silence 0:42:25 - 0:42:50].

No, no, no, no. No, no, no, no. Yes, \_\_\_[0:43:06] every single stone, yet I still have [an] access to a device that can send emails yet I have no access to a device that an complete a phone call. I don’t think you can ever find yourself in a situation like this, phishing. And there are 105 more reasons that this is phishing. This is a no.

[Silence 0:43:33 - 0:43:46].

Your valid email [member 0:43:47]. \_\_\_ situation at eBay dot co. No, no.

[Silence 0:43:52 - 0:43:02].

No, no, no, no \_\_\_[0:44:04] this link they’re looking back. Definitely phishing.

[Silence 0:44:07 - 0:44:20].

[This mail 0:44:20] link, Directgov at [SLC] dot uk, [SLC] uk \_\_\_ company, yes.

[Silence 0:44:30 - 0:44:41].

[Mindphase 0:44:41] dot com. What? We give the [ticket fraudulent] activities going on with student loans. [Fraudulent]. You just give a loan and they pay it back. If someone pays back more it’s not fraud, if he pays less it’s not a fraud. A fraud is if someone takes a loan from you not legitimately and this is your problem, not the student’s problem. How could someone engage in fraudulent activities that are concerning a student loan?

Impossible, I believe and hope. Definitely phishing. Be web safe this season. The subject it outrageous, erm, [gang stone 0:45:48] ethics change to the terms and conditions of your \_\_\_ prepaid MasterCard.

[Silence 0:45:52 - 0:46:03].

Okay. This seems legitimate. [Sounding 0:46:13] \_\_\_ legitimate. Six. PayPal [log in now] \_\_\_ dot PayPal dot co uk. ‘E’. Maybe it’s the ‘E’ in the [email address] stands for electronic or something. But why is the name PayPal? At PayPal? Maybe I’m giving too much attention to… Hello [Jules 0:46:48] your recent transactions now [Helen Jones] you recent \_\_\_. And then the subject is outrageous, thinking, doesn’t it say recent transactions or transaction number, and then the number of the transaction.

Log in now. Why would you log in? You could just click a link and… Okay, \_\_\_[0:47:26] seems extremely [legit] but, I don’t know, I have some doubts about the subject, big doubts.

[Silence 0:47:42 - 0:47:56].

How do I know this is not a spoof email? Spoof or phishing emails tend to have generic greetings such as ‘Dear PayPal member’. Oh, so that emails that started with ‘Dear Valued Member’ were all phishing. Find out more. Yes, but if that’s so, why is the subject..? Okay, I will give it a five. I’ll give it a five. Again, the subject is fishy.

[Silence 0:48:35 – 0:49:03].

I don’t think \_\_\_[0:48:05]. I don’t \_\_\_ and then it’s you \_\_\_ no, phishing, phishing. \_\_\_ and the mobile banking team. No, phishing. Mobile banking \_\_\_ doesn’t look right and the email address of the sender doesn’t look okay as well.

[Silence 0:49:27 - 0:49:55].

This seems like a legitimately… No, not legitimately. This mail’s phishing but it looks like it’s a legitimate spam email. So it’s not actually trying to hurt you, just to get views on a page or something, so I’ll give it a two instead of a one. No, no, no, no, no. Driver’s licence details. Drivers that \_\_[0:50:51] that you used to \_\_\_, these \_\_\_ waiting [three] weeks his or her driver’s licence. Yes, sure, yes. Even if that’s so, there are people who don’t have access to computers and you need not have access to a computer with email address that you should check regularly in order to [put this 0:51:15] driving licence.

So they take that out the way from you just based on an email, that’s not alright, that’s definitely phishing, it’s not even a one, it’s a zero or minus one. It’s extremely phishing. \_\_\_ Lancaster. Okay Faculty of Science [and 0:51:41] undergraduate survey. Dear student…

[Silence 0:51:43 - 0:52:22].

Dear student, why didn’t they send it to the Lancaster address? Why did they send it to the Gmail address? Just based on that I would give it a three because I’m uncertain. Because if they can send it to a Gmail address they can send it to a Lancaster dot ac dot uk address as well. Yet the whole reason that they’re sending it to a Gmail address instead of the Lancaster address. I would say that emails from universities tend not to look like this, three.

**P332**

P332: ‘Dear guest user, \_\_\_[0:00:01] sees your PIN.’ That’s definitely phishing.

[Silence 0:00:11-0:00:28]

Actually, we’ll put four. It doesn’t look too fake. Oh right, this is definitely phishing. ‘Hello, I’m Mr Gary Cooper.’ The spelling is not even right. The grammar is not even right. You always get emails from people trying to leave you money and it’s never even real.

[Silence 0:00:57-0:01:11]

Yes, that’s definitely- Dell definitely looks legitimate.

[Silence 0:01:14-0:01:28]

Yes, that’s definitely legitimate. It’s got things at the bottom.

[Silence 0:01:30-0:01:49]

I don’t know, that’s the same as the first one. Oh God. I’ll put three, just because I’m not sure.

[Silence 0:02:06-0:02:23]

That is definitely phishing. ‘Find out more about this IP address,’ they don’t say that.

[Silence 0:02:36-0:02:49]

That looks quite real, not that I’m even sure that- oh God, I’ve clicked the wrong one. Not that I was even aware that you could have an Adobe Reader account. That is definitely fake. It’s trying to sell an account, a games account, why? Right, okay.

That’s definitely phishing because banks don’t email you, because even when they phone, they give you the option to ring up. That’s definitely phishing because Visa just make cards. I’m sure we all- they don’t do anything. That’s definitely phishing. It doesn’t look official, there’s no email, logo or anything like that.

That looks quite real. Actually, I don’t know. That email looks a bit dodgy for Facebook. No. Do NatWest email? I don’t know. That looks definitely legitimate. Yes, that definitely is Amazon, not too bad. That looks quite legitimate as well, because they \_\_\_[0:04:57] usually send you an email, but I’ve never had an email. I don’t know. That one’s phishing.

[Silence 0:05:05-0:05:18]

That looks legitimate. Why would people send a phishing email for a fake job? I mean, why would people spend… I don’t know actually, because then if you download the application form, it might be a virus. I’m going to go with legitimate, anyway.

[Silence 0:05:40-0:05:54]

Student Finance definitely don’t even email you. [No one 0:05:59] wants you to give out your details online. Again, PayPal don’t email, because they don’t want you to give your details out. Actually, that FedEx one looks alright, because you’ve got nothing really to lose from that, unless you open the postal receipt and then it was fraudulent.

‘Your password will expire in three days. Upgrade \_\_\_[0:06:33].’ Who even is this person? What, even, do they want? That’s another one of them, like, Nigerian things who email you saying, “I’m a millionaire, I’m leaving you all my money.” That’s definitely not. ‘I was wondering if you could help us with a [click 0:06:55] loan?’ No.

[Silence 0:06:57-0:07:10]

No, that’s definitely phishing as well. I’m sure if you’ve got a bill for a mobile phone, that they’d just text you instead. They wouldn’t just send you an email, it’s a bit weird. That’s definitely a fake eBay email because it says @ebayz, with a Z. Oh right, that looks legitimate because Dropbox is quite reliable.

I get these all the time. Then again, yes, that’s not an email to PayPal, approximatingdz@mckenkmusic, it doesn’t send you an invoice from the person, it sends it from PayPal. It’s a PayPal thing not an other- no, that’s wrong. ‘Good day, give your loved one a watch.’ That’s fake.

Oh right, that’s quite legitimate because you do get job alerts over email. No, because I’m sure Student Finance send, like, letters. They don’t send emails. That looks quite real, so I’ll give that a five. That doesn’t look real. That looks like one of those fake, like, Vanquis cards or Black cards or whatever they are that they keep trying to get you to get. That looks alright, but I’m not entirely sure, so I’m just going to put that as a three to be safe.

That’s phishing because NatWest, again, would send letters for online banking. Barclays, phishing, they don’t send emails about unusual activity, they’d ring you. Oh, that’s legitimate because I’ve had that one before. A Pleasure Beach survey. That is definitely fake because you have to renew all your driving licence details over the post. Can’t do it over the internet, it’s not reliable. That’s true, because they send module feedback things all the time.

**P333**

P333: From [HMPSrecruitment@i-grasp.com](mailto:HMPSrecruitment@i-grasp.com) job alert. “A job that matches your alert criteria has been published on our website. Please click the following link or paste it into your browser and search for the vacancy reference number listed below. \_\_\_[0:00:28] send \_\_\_good luck with your job search, yours sincerely, [0:00:36] recruitment team.” It seems pretty legit. Hmm. I-grasp, I’ve never heard of it. Just because you’ve never heard of it doesn’t mean it does not exist. There are so many job alert [0:01:05] and everything. So, yes, I’m pretty sure it’s legit. Give it a four? Yes, four. Pretty sure.

NatWest. Ha, this is definitely phishing, because NatWest, UUP@ \_\_\_[0:01:26], players! “To continue your online banking,” they never say this. Definitely phishing. Student finance@direct.gov.uk, “Student update. This is a formal notification for an important account update. Due to a recent update in our database we require all students to update their account information to ensure you receive your scheduled payment and avoid mispayment. To update your account information, click here to validate your information. Sincerely, Student Finance England.”

One thing is that it’s .gov.uk, but it also has @direct.gov.uk, but Student Finance has a double E and I’m pretty sure that Student Financee, Financer would make sense. Let’s see. Oh. All in one place, Direct Gov. Hmm. I have no idea. I don't receive student finance. [Studentfinancee@direct.gov.uk](mailto:Studentfinancee@direct.gov.uk) but if it’s @directgov.uk. Hmm. I would say I’m not sure. So either three or four. No. Where it’s financee, I’m not confident with that. I’d say a two.

“Priority mail postal service, DTF.193.com.” That is such a dodgy email. “Our post-rider,” grammatical error. “To receive a parcel, please...” Why would you put a comma next to it? Definitely phishing. Hmm. “Helpful banking, your latest statement’s available online.” Ah, this one is definitely legitimate. Yes. NatWest. Caxton FX. Via statutory.co.uk. Why would you send it through a different email? “Changes in terms and conditions for your Caxton pre-paid MasterCard. Please take the time to read your updated terms and conditions, which are available here.

We recommend that you retain a copy of the updated terms and conditions for your records. Here to help, call on and we will be pleased to help you.” I think this is pretty legitimate because it’s just saying that your... Read updated, usually if they ask for information about your card then it’s a scam, so five. PayPal, “Please update your card expiry date as soon as possible. You should activate your new card.” Yes, this is the one that’s so annoying to get from PayPal. Definitely legitimate. “You or someone else entered the email to change the password of a user account.”

Yes, this is legitimate. I’ve heard this one before, [frank@easyroommate.com](mailto:frank@easyroommate.com). Yes, it’s legitimate. Barclays, support@vnet.com. “We have detected unusual activity on your account. This may be because of logging into internet banking from several IP addresses. To reduce the risk of unauthorised access, we’ve decided to limit your account until you complete these steps. Click here to refer your account.” I don't think this is real because support@vnet. It should be Barclays. Definitely phishing.

Mail to [info@hsbc-business.co.uk](mailto:info@hsbc-business.co.uk). “Incoming funds blocked. Just to inform you that business account with us has been blocked from receiving payments and attempted error logins were detected by our security system and this account will be disabled if you ignore this message. Please click here to resolve the issues. If you are not an authorised signatory, please forward to the authorised signatory.” Hmm. HSBC-business.co.uk. No. It’s definitely phishing because if they block your card they’ll say, “Call us.”

\_\_\_[0:07:52]. “Your password will expire in three days. systemadministrator@\_\_\_.eu. Yes, legitimate, but \_\_\_This person is probably a student. \_\_\_[0:08:13] this doesn’t seem right. [Ofcvdvr1@facebookmail.com](mailto:Ofcvdvr1@facebookmail.com), definitely not, “Enter the new email address, confirm you have,” blah, blah, blah, “If you do not, take a look at... If you have any questions...” Hmm. But notification plus but facebookmail. Everyone has a Facebook mail these days. I would say it’s closer to being legitimate.

\_\_\_[0:09:01] Diablo 3 account@\_\_\_.com. “You’re trying to sell your personal account and you may not... You are in the terms of agreement. If this proves to be true, your account can and will be disabled. It will be ongoing for further investigations. If you wish to not get your account suspended, verify your account ownership. If your account passes the checks, the system will send the package down in the form of an email. Three days after receiving the email if you don't submit your information we have the right to freeze your account.

This is to protect the safety of your account. You must work together with us. We are determined to crack down on all the behaviours destroying games. If you have not already authenticator your account,” definitely phishing. “If you had already authenticator your account.” Oh, come on. eBayz, when they put a Z you already know it’s phishing. It’s lies.

“Verified by Visa.com.” Huh? Oh, this is definitely a phishing one. I don't even need to read to work this. E.paypal.co.uk. Oh, well, they don't really send you that. “Visa transaction now.” No, they don't have E dot. Definitely phishing. “Philip \_\_\_[0:10:42]. My family had a trip visiting Manila, Philippines. Everything was going on fine when...” Oh, come on. Every time. Definitely phishing. Gucci, Cartier, Rolex, bull. That’s not real. “Can you give your loved one a luxury watch today?” I think not, definitely phishing.

Noreplyaccounts.google.com. “Suspicious sign-in prevented, 2 September, [noreply@accounts.google.com](mailto:noreply@accounts.google.com). Someone recently tried to use... Sign-in to your Google account. We prevented sign-in attempt in case this was a hijacker trying to access your account. Please review the details and sign-in attempt. If you do not recognise then reset.” Yes, pretty legitimate, so I’m marking it a five.

“Hello, I’m Mr Gary Cooper. Was born in... I am suffering from...” Ha, sob story, bye-bye. This is phishing. “Dear Guest User, Google Box UK has received your payment regarding the item.” Yes, legitimate. This is not. [Service@paypal.com](mailto:Service@paypal.com), but why does it say ‘approximate-adz’? It’s not... But... Macuser.com, payment \_\_\_[0:12:49] [service@paypal.com](mailto:service@paypal.com). Alright, okay, that’s why. So, legitimate. “Adobe customer care.” [Email@mail.adobesystems.com](mailto:Email@mail.adobesystems.com). “We have obtained your access to... There has been... Choose your password.”

Hmm. “An attack illegally entered... Obtained access to your ID and password. We currently have no indication there has been unauthorised access to your account. You have to reset your password. Please visit to create a new password. Google password reset.” Hmm, it seems legitimate. Let’s put a five. “\_\_\_[0:14:08] the United States. \_\_\_. Yes. I think it’s okay. \_\_\_@virginmobile.com. “The bill for your Virgin Media Mobile is now ready to view. So if you’d like to email us back, head over to our website.” Yes.

[Ebayinvoice@ebay.uk](mailto:Ebayinvoice@ebay.uk). Yes. If it asks you to sign-on that’s fine. Hrdepartment. This is so not real. Definitely phishing. No one uses \_\_\_[0:15:03].co.uk. SLC UK Direct Gov. “You can do this by... Update you...” Yes, quite legitimate. “\_\_\_ needs to verify your email address before you can share.” Yes, legitimate. “TNS on behalf of Dell at Dell Survey help.tns.” Ah, I don't think so, because it’s [dellsurveyhelp@mailtowabtnsonline.com](mailto:dellsurveyhelp@mailtowabtnsonline.com). Does that even mean?

“Please click on the web address below. If that does not work, copy and paste. The survey should take about five minutes to complete. We look forward to your feedback. A customer... Committed to delivering...” I have no idea. TNS. Oh, okay. mailto.wab.tns. Ah, it won’t open this. Koala Craig waiting on delivery today. Hello, Helen Jones, thank you for shopping with us. We thought you must be informed of your shipping and this completes your order. If you need to return an good from this ship...” Why would Karla Gregg send it to you? Amazon means Amazon not Karla Gregg.

Plusnet. Yes, this is legitimate. Plus.net. No. “Your software is available. Dear Miss Jones... Plusnet Protect. This is now ready for download.” This will be an install. Yes, legitimate. Ioffer.com. “You shall receive...” Okay. team@blackpoolpleasurebeach. “Dear Pleasure Beach visitor, thank you for visiting Pleasure Beach Blackpool recently. We hope you enjoyed your day here. We want to find out more about your views.” Why does it say RE? “This is the result of completing the survey and we hope to see you here at Pleasure Beach Blackpool again soon.

We will be grateful if you can login. Thank you for visiting Pleasure Beach Blackpool recently.” Hmm. team@blackpoolpleasurebeach. I don't know. Snap web host survey. Sent their email address, though. Hmm. Maybe three. Could be, could be not. DVLA.co.uk. “Our database... Refuse to update his or her...” Hmm. DFT.co.uk. DVLA, though, shouldn’t it be DVLA? Yes, definitely legitimate. I don't know. Lancaster, “To find out why you chose... Service...” Definitely legitimate.

**P334**

P334: So the email says, “Please take the time to read your updated terms and conditions, which are available here. We recommend that you retain a copy of the updated terms and conditions for your records. Here to help.” Terms and conditions.

I [do] believe that this is a legitimate email because it doesn’t require any additional personal details, it just… Actually, hmm. Sure, there is a link, which might be some malware or something. That’s a bit strange, but apart from that I think that it’s quite a legit one, and therefore I would give it five out of six.

Alright, so the next one is a [Diablo 3 0:01:10] account. “It’s come to our attention that you were trying to [set up a personal Diablo 3 account. As you may not be aware of this conflict with the \_\_\_. This \_\_\_ to [ensure your] account can and will be disabled. [There will be an] ongoing [for further] investigation by [Blizzard Entertainment employees 0:01:29]. If you wish to not to get your account suspended you should immediately verify your account ownership. Please open the connection. If your account passes the check successfully we will send a \_\_\_ dynamic [button] \_\_\_ indicator in the form of an email. In three days after you are receiving the email, if you don’t submit your information we have the right to freeze your account \_\_\_[0:01:55] to protect the safety of your account. You must work together with us to crack down on the behaviours that are destroying games.”

The fact that this is linked from a site that I am rather familiar, it should be a completely legitimate one, and it’s just regarding some possible fraud and Blizzard would like to identify that fraud. I don’t see anything wrong here, so I would go with six out of six.

Alright, next one is, “Just to inform you that the business account with us is being blocked from receiving payments. Attempted \_\_\_[0:02:49] login was taken by our security system and this account will be disabled if you ignore this message. Please click here to [be able to] resolve the issues. \_\_\_ authorised signature.”

Alright, so that seems a bit phishing, because it’s… It’s like too much hostile I think, this email, and this like… “This account will be disabled if you ignore this message.” It seems probably too harsh for an email that a bank would send. Hmm.

That seems a rather phishing email, but… Well, I think the language that is used here is not the language I would personally expect from a bank, so I’ll give it a two out of six.

Alright, the next one is from FedEx. “A parcel has arrived with the Post Office, or a [post rider 0:04:30] was unable to deliver the parcel to you. To receive the parcel please go to your nearest office and show this postal receipt. Best regards, the FedEx team.”

Hmm. Well… “Get the postal receipt.” That seems a bit fishy, but… Well, generally it should be the firm’s obligation to deliver the parcel, and not to tell you to go somewhere else, and that [links it 0:05:35]… It really seems rather fishy, so yes, I think that’s definitely phishing. The firm should do its best to deliver the parcel right to you, and not send you somewhere else, and that link is just too suspicious for me.

“You just received a message from Graham, an Easy Roommate member, click here to see the message and profile. If the link above doesn’t work just copy the URL into your browser. \_\_\_ helping you find the right [flatmate]. Beware of scams. Do not send money via Western Union.”

Alright, so… What’s written at the bottom, “Beware of scams,” is like, why would you write that? “Do not send money via Western Union,” why would one not send money via Western Union? That seems quite strange. “See the message and the profile…” [I find that 0:07:11] it says, “Please do not reply to this email,” and, “Forward the link [going to] your account to reply.” It is phishing, but like, in some aspects it looks legit, but not too much. I’ll give it two out of six.

Alright, so that’s from Google. “Someone recently tried to use an application to sign into your Google + account, it prevented the sign-in attempt in case this was a hijacker trying to access your account. Here is a review of the details of the sign-in attempt. If you do not recognise the sign-in attempt, someone else might be trying to access your account. You should sign-in to your account and reset your password immediately. If it was you and you are having trouble accessing your account, [complete the troubleshooting steps listed 0:08:19]. Your sincerely, the Google Accounts Team.”

Hmm. That’s an interesting one, and it looks rather legit to me actually. There are some attachments as well. Hmm. But… Well, the thing is that I have personal experience with that, someone entering my account, and I didn’t receive such an email. Well, generally I don’t know why there would be such a message, because you can go into your account from all around the world, and that looks kind of suspicious, but still… I would say that I’m 50:50, between whether that’s legitimate or a phishing one, so I would go with 3 out of 6.

Direct Gov. “This is a formal notification of an important account update. [Due to] a recent update in our database we require all students to update their account information to ensure you will receive your scheduled payment and avoid a mispayment. Update your account information. Click here to provide \_\_\_[0:10:29]. Please fill the requested information exactly as you filled it when you were signing up for student finance, or your payments will be suspended because of failed account verification.”

Well I think that seems a bit harsh, like, “Your payment will be suspended.” There could be numerous reasons for… But they want exactly the same [details], I mean, something could have changed, you could have informed the people who are in charge of that. So again, that seems like a too harsh email, and, hmm… Again, there is nothing written in the link, and the email is from Student Finance [E], but generally I don’t know if these emails are made up just for the purpose of the study, but that looks like, too suspicious, [with double Es 0:11:44], at least from my perspective, so I think that’s definitely a phishing one.

Alright. “Your account is about to expire. We noticed that your Visa Delta Electron is about to expire, please update your card expiry and card security code as soon as possible to avoid any interruptions to \_\_\_[0:12:08] PayPal. Be sure to activate your new card. If you have received a new card, please link the card. If you have already update your PayPal account with your new card details, please disregard this email.”

That truly looks like a quite legitimate- It’s like a message I would expect to receive from PayPal, so yes. “PayPal Europe, rights reserved…” Hmm. [Date card 0:12:43]. I don’t like these short links, they seem a bit suspicious, but apart from that it looks quite legit, so I’ll go with five out of six.

Alright, so the next one is from Barclays. “We’ve detected unusual activity on your account. It may be because you’ve logged into your online banking from several IP addresses. Due to the risk of unauthorised access we have decided to limit your account until you complete the steps here for access. Please note that these security measures are intended to protect our members’ accounts, we are sorry for any inconvenience.” Hmm. [[Support@bnet.com](mailto:Support@bnet.com) 0:13:31]. I’m not sure why you would receive an email from bnet, I guess it should be from Barclays, so that seems strange to me. Also, again, I don’t like some of these short links. But it’s like an email that I would expect to receive from a bank. It’s hard for me to say, so I’ll go with three out of six.

Dropbox. “Dropbox needs to verify your email address because you can share folders. Please verify your email address by clicking the link below.” Again, it’s a short link, but apart from that… I think I’ve received the very same message, so we’ll go with fix out of six. Yes, five out of six.

Alright, [NUSExtra.co.uk 0:14:35]. “You or someone else entered this email address to change the password of an NUS Extra account. \_\_\_ password reset, please proceed to the link, this action was requested from IP address…” And there is… Hmm. “Enter password of your NUS Extra account.” I’m not quite sure what an Extra account is to be honest, so that could be the key here. Hmm. I’m a bit stuck here; it’s hard to make sense \_\_\_[0:15:41]. The thing is that I would expect something at the end, like, “Greetings,” or like some indication of a person writing this message, like, “Your sincerely, David from Customer Support,” or something else like from the Support Team. Hmm.

There is an attachment, which is made unavailable, so it could be blocked automatically by the system as something potentially harmful to the computer, or the device you’re using. Yes, that seems like a bit of a strange email to me, I wouldn’t go with one, but I guess two would be fair.

Alright, it seems like- Alright, it’s [loaded 0:17:03] now. Okay, \_\_\_, “A job which matches your \_\_\_ has been published on our website, please click on the following link or paste into your browser and search for the vacancy reference. Yours sincerely, HR Recruitment Team.” “\_\_\_ job adverts, click here.” That seems…

The fact that I’m not native English, I’m not quite sure about the punctuation, but I do believe there are a couple of mistakes here, which you’re not supposed to receive from a recruitment team. Therefore that seems fishy to me, but apart from that it seems alright, and I might be wrong about the punctuation. I would go with two out of six, that’s my \_\_\_[0:18:31].

EBay invoice notification. Right, so it’s a bit hard for me to read this one, it’s like… “You’ve set up a PayPal account as your automatic payment method. Go to eBay and click on eBay…” Oh, it’s very hard to read that email; the letters are… I’m not sure if that’s from the monitor, or from the email, but it’s so hard to read that. Oh god. Hmm.

Again, I’m not sure if the letters and the font is due to the monitor or it’s how I’m supposed to perceive it, it’s so unclear and so hard to read it, but the language is something that I would expect from eBay to write to me. So I would go with 50:50 here.

Alright. “Congratulations you just purchased an item from [Google Box 0:20:18] UK. You should receive an invoice with payment and shipping instructions shortly. If you have made a mistake, click here to cancel the transaction. This is an automated email, please do not reply.” Alright, then there are attachments, which are made unavailable. “You just purchased an item from Google Box UK…” Hmm.

That’s an interesting one, but I don’t think it’s fishy. There is just a short link, which is a bit disturbing, but it says it is an automated reply, which seems legit to me. There are some attachments made unavailable, but overall it looks legit, apart from these things. I’ll go with four out of six.

“Your password will expire in three days. [Why would] your password expire? Click here to validate your email. Thanks, System Administrator.”

Again, I think that there is a punctuation mistake here, and also you receive an email from someone who has said his name, and at the end you have the System Administrator, and also we have a different link. So yes, that seems fishy, but… I won’t go with one out of six, I think two out of six would be fair.

EBay suspension. Alright. “We regret to inform you that your eBay account has been suspended due to concerns we have for the safety and integrity of the eBay community.” \_\_\_[wow, the whole community 0:22:35]. “[We may] immediately [show] warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide [authorisation] to you if we believe your actions may cause financial loss or [legal liability] to you, our users, or us. We may also take these actions if we are unable to verify your [aural identification] in any information you provide to us. Please take 5 to 10 minutes out of your online experience [in data \_\_\_] you will not run into any future problems with the online service.”

“Any future problems,” that seems fishy. Like, “Your account is suspended, if you take 10 minutes, everything will be smooth forever,” that doesn’t make sense. Also it is received from eBayz, which doesn’t make any sense. Again, there is a rather- No, I wouldn’t say it’s a short link, but the whole content seems so fishy and also it’s from eBayz, with a ‘Z’, that doesn’t make sense. I think that’s quite fishy. Also the logo, the logo is so old, I think that should be the logo for eBay in 2005 or something, not 2012. So I’d say that’s definitely phishing.

Right, so this is from [Adobe Systems 0:24:43], Adobe Customer Care. “To view this message in another language, please click here.” Alright, I’ve never seen such things, “To view this message in another language,” that’s definitely something to watch for. “We recently discovered that an attacker illegally entered our network and may have obtained access to your Adobe IT and encrypted password. We currently have no indication that there has been unauthorised activity on your account. To prevent unauthorised attacks on your account we have reset your password.”

Then there are only short links, but… Alright, so the dates, October 3rd and October 8th, they match, and that makes sense.

That seems rather legit, to be honest. Hmm. Apart from the short links. That is probably one thing that you will receive from Adobesystems.com. I’m not sure if you should receive an email from them, but the content seems legitimate, although it’s strange for a company like Adobe to be hacked. I’m in two minds about that, let’s go with three out of six, it’s hard to decide.

NatWest, “Your online account will expire today. If this process is not performed within 24 hours your account will be disabled.” I don’t think you should receive an email on the very same date, and the email is from [danketewan 0:27:28], so that doesn’t make sense at all, and there is just some short link. That’s definitely phishing for me.

Okay. “Your latest statement is available online. Your latest statement is ready for you online now, just to [gain and see] more information on your account. If you need more help in understanding your statement \_\_\_ [statement area 0:28:01].” With your online banking \_\_\_ you can also enter some things listed about it, and there is some information regarding contact. “We like to remind you about security. We will never contact you and ask you to provide your security details. If you are in doubt, please contact us. Calls may be recorded.”

That email is from information.natwest.com, so seems legit, and the whole content seems something quite legit. I cannot find even one thing that rings a bell, so I’ll go with six out of six.

Right, Plus Net Support. “Dear Ms Jones, your account name…” There is some software here, and instructions for how to [perceive 0:29:10] it. Hmm. Definitely, I honestly cannot see anything suspicious, it’s just an email with all the details, all the instructions, it’s [well structured], seems to be from a legit website, from a legit provider. Yes, I would say that’s definitely legitimate.

“Hello I’m Mr [Gary Cooper 0:29:48], I’m at a \_\_\_ institution in Italy where I’m writing you, \_\_\_ [Lancaster \_\_\_ office]. Therefore I would kindly leave you my fortune to \_\_\_.” Ah, another one that wants to make me a millionaire. That’s definitely phishing.

I wouldn’t expect someone to just contact me and give me a few million bucks. I have received so many of these emails.

“Hello, I’m sorry for reaching you rather too late, due to the situation of things right now. My family and I \_\_\_[0:30:31], how does that concern me? Everything was going along fine until last night when we got attacked by some unknown gunmen. Our money, phones and credit cards were thrown away. [In calling \_\_\_] it was a terrible experience, but the good thing is they didn’t hurt anyone or make away with our passports.” Okay, that seems like a pretty strange story. “I reported the incident to the local authorities and the consulate, but their response was too casual; we were asked to come back in two weeks, and for investigations to be made proper. Right now we are financially [struggling 0:31:15] due to the unexpected robbery attack, we are wondering whether you can help us with \_\_\_ to sort out the bills and get back home. All we need is £1850, we promise to refund you in full as soon as we return home, hopefully tomorrow or next. Write back now to let me know what you can do. Thanks, Philip.”

Alright, so that could be a message from a friend who was in trouble, although that story seems like… It doesn’t seem like something that would happen. I mean, an armed gunmen came and they took some valuable items and they leave you your passport and they don’t hurt anyone? That’s strange. Well, it definitely seems fishy, but there are no links, there is nothing suspicious in that aspect, but the story that the person is telling seems unreal, for me. It’s hard for me to believe that. I’ll go with two out of six.

Alright. Facebookmail.com. I don’t think you should receive something from Facebookmail.com. What is it? A notification for \_\_\_[0:33:18], I don’t think you should receive… There is a link. “You recently added a new contact email address, confirm your contact email address, follow the link below. \_\_\_. If you did not enter this address as your contact email, please disregard this message.” I’m not quite sure if I understand. Why would you disregard that email? I mean, if I’m not the person who has added this contact email, then someone else has, which means that someone has most probably logged into my account without my permission and knowledge. Also, the person who has sent [that] seems too strange, I don’t think Facebook would send you something to your email from that email. It should be Facebook.com at the end. It seems fishy. The only thing that I like is that the link looks legit, but apart from that, it’s quite strange. I would go with two out of six.

Alright, so it’s from PayPal, “Approximating 100”. Okay, that seems strange. The payment is to [Kate \_\_\_ 0:35:08]. Actually I’m using PayPal, and now that I think about it, I think I have received the very same email, though again the logo of eBay seems too [non-modern 0:35:47] for the year 2013. Also, I don’t think you should be receiving an email from that provider. But apart from that, everything seems alright, the links, the amounts, the whole structure of the letter. I’ll go with four out of six.

Alright, so this is something, ‘Security by Visa’. “Dear valued customer, your credit card has been suspended as an error was detected in your credit card information. The reason for the error is not certain but for security reasons we have suspended your credit card temporarily. We need you to update your information for further use of this credit card. To lift this suspension…” Hmm. Verified by Visa, again, the provider seems a bit strange, to be honest. Now that I think about it, why is the copyright from 1999 to 2012? I think it should be until 2013. There are a couple of strange things, also I don’t like the short link, but the text looks legitimate, but the things I mentioned make me go with three out of six.

Alright. “We have detected \_\_\_[0:37:32] for all students receiving grants and loans from the Student Loan Company. We have detected further \_\_\_ activities going on with the student loan accounts. Do this by clicking the link or copying and pasting to your browser, [directgov.\_\_\_.co.uk]. You will receive an email from Direct Gov and there is a link that will transfer you to \_\_\_[0:38:13].” That doesn’t make any sense.

It’s hard for me to say. Again there is the thing that there might be some punctuation mistakes. Yes, it seems quite fishy. Quite fishy. I’ll go with one out of six.

[“Dear Google Box 0:38:54] user, and Gmail user, click here. Good day, give your loved one a luxury [wash] today.” Oh, come on. It’s from \_\_\_, [lakers.com], like totally phishing.

“Dear [guest] user, Google Box UK has received your payment regarding the item.” Oh, I think I remember that title. “Click below to view the status of your purchase.” Alright. It’s hard. “This is an automated email, please do not reply.” The link is not short. Hmm. This one looks rather legit. Yes. Well, I don’t think I can find anything strange here, given the fact that I saw the previous email as well. Now that I think about it, that one seems legit. I’ll go with six out of six.

Alright, there is a PDF, which is strange. “Hello.” Shouldn’t there be a comma after ‘Hello’? “The bill for your Virgin Media mobile is now ready to view.” Now, it doesn’t make sense. Alright, “The balance will be taken by Direct Debit on, or immediately after, October 20th. Our team won’t be picking up emails from this address, so if you would like to email us back head over to our website to send us an email.” Apart from the fact that- The sender, Virginmobile.com, seems like a legit one. The short link and… It’s quite hard to understand what they are saying. I mean, it could be, again, as I said I’m not native English, so that could be the problem, but I think it could be written in a better way. Again, the provider seems legit, and actually what they’re trying to say seems like- Actually- Hmm… Yes, I don’t think that there is anything, apart from the fact that it’s from this provider that makes me say it’s legit. It looks quite like phishing but the provider seems legit. I’ll go with two out of six.

Alright, HR Recruitment. What HR department… Wow, that seems quite strange. Here are some links that don’t look professional at all, and there isn’t a \_\_\_[0:42:21] really, \_\_\_ that you’re going to receive from a human resources department, and 40 hours is like the same- I’m just looking at some random things, and I see like so, so many mistakes, and so many things that make me \_\_\_[0:42:48] it. Yes.

I think also they should call it ‘Dear Ms Jones’ and not ‘Dear Applicant’. I also see some punctuation mistakes – again, that’s what I think. Yes, I think that’s definitely phishing.

Alright, again from PayPal. [E PayPal], hmm, that’s strange. “Hello from PayPal, login to see \_\_\_[0:43:26] activity and recent transactions.” I don’t think that there is such a site at all, E-PayPal. I have had a PayPal for a few years already and I’ve never received such an email. I don’t think you should receive an email. There are again some quite fishy links, the provider seems strange. The content doesn’t look suspicious, but that’s basically the only thing I could say. We’ll go with two out of six here.

Alright, that’s from [Carol Craig 0:44:23]. Oh, if you receive an email from Amazon, it shouldn’t be from Carol Craig, it should be from Amazon. Yes. You definitely shouldn’t receive an email from Carol Craig. Again, the numbers don’t add up. You add 15 to £359.99 and it’s again £359.99, that’s really, really strange. Again, there are just some short links, like, I have bought from Amazon and I’ve never ever received such an email, that’s definitely phishing for me.

Right, that’s from Dell, and again the provider is Dell [Surveys Help 0:45:37] mail \_\_\_.TNS what’s that? Again there are some short links. “Thank you for your recent contact with Dell Support. At Dell we are committed to delivering the best customer service experience to our customers, \_\_\_ feedback \_\_\_ and your experience with Dell Support to help us improve. \_\_\_ survey, please go- Again, you should go to the Dell site, not to the site of like [Raptor.TNSonline.com]. I do not understand how otherwise- The person who sent you that would know that you have contacted Dell customer service. That’s the only thing that’s making me saying there is legitimacy in this email. I’ll go again with two out of six.

Alright. [Team] Blackpool Pleasure Beach. Well, that’s strange, but let’s see. “Dear Pleasure Beach visitor. Thanks for visiting Pleasure Beach Blackpool recently, we hope you enjoyed your day here. Everyone taking part will be entered for a draw to win season passes giving unlimited entry to Pleasure Beach for a whole year. Enter the survey [click below 0:47:38], \_\_\_ the Pleasure Beach Blackpool Team.”

There are a couple of things again, I think the punctuation is a bit strange. There could be some mistakes. Shouldn’t you receive not from surveys but from another place? It seems strange, but the content seems like something alright, and there is not a whole link. I’ll go with three out of six.

Alright. Right, “[DFT.co.uk 0:48:22] [and there is], “We are currently upgrading our database \_\_\_ driver’s license. [Print] your [license verification] with us, you are required to fill out the form in the link below.” Two weeks, that seems like… DFT.co.uk. \_\_\_ although, having a [gov.uk] link, that would seem legit, but, if you do not upgrade your details within two weeks that will be it? Come one, some people don’t even have access to internet, how would they do that? And [you would regard it] as a refusal, like, that’s definitely not the policy, and… No. I refuse to believe that this is legitimate, other than the gov.uk link, otherwise it seems like something quite… Not quite what would you receive from such a provider.

Alright, this is a message from [Lancaster]. “Welcome to Lancaster, we hope you have enjoyed your first few weeks at the university. We are interested to find out why you chose to come to Lancaster University and how you found the admissions process.” There is something about a short survey. “Please note the survey is only open to current first year undergrads in the Faculty of Science and Technology. [It will close] on November 30th.” I think I have received really, really similar emails, so I think that they are definitely legitimate, also the provider.

**P335**

P335: Alright, this one doesn’t say anything about needing any more personal information or anything like that, so it seems pretty legitimate. It doesn’t seem like they’re trying to steal any information or anything like that.

Yes, this one seems pretty legitimate, even though it’s quite a large amount of money being spent. It has been delivered to the correct address, rather than an address of anyone else, which would seem a little bit more suspicious. I’m going to put that at five.

Yes, nothing here about wanting any information or anything like that. It doesn’t seem like they’re trying to phish anyone, so I’ll put that one at five as well.

Hmm, this one you can tell is false straight away, because it’s not a real eBay email address. It has ‘Z’ at the end, and the fact that they have a link to click on seems a little bit fishy as well.

This one also seems a little bit fake, because it’s a fake email address. It’s not actually from FedEx. It hasn’t given any information about which Post Office it’s been delivered to or anything like that, which a legitimate email would, but at the same time, it’s not asking for any personal information. However, the link to get the postal receipt may be an attempt to give your computer a virus or something.

This one, again, seems fake, because the email doesn’t come from a Barclays account. It comes from somewhere called ‘vnet’. If it was a real Barclays email, obviously, it would come from an account that was from ‘@barclays.com’, and obviously, yes, that mixed in with them wanting to click on a link seems like it could not be a legitimate email.

Okay, this one seems a little bit strange, because it seems like the website is maybe a bit of a spam website. ‘ioffer.com’ doesn’t really seem like… You know, as compared to somewhere more reputable, like Amazon or something like that, it doesn’t seem like it could be a real, safe website. Then again, at the same time, it says that an invoice has been sent and all this kind of stuff, so I’m going to put that one as a two, rather than saying that it’s definitely phishing.

Right, okay, this one, the email itself seems pretty legitimate until you look at the email address that it’s been sent from. A real HR department wouldn’t have a load of random letters at the end, and he would say which company the department was from. It also wouldn’t have all the arrows pointing to the download of the application form, so I’d say that that one’s phishing.

Okay, I think I might… Yes, I think I should have put that the iOffer one was a little bit more legitimate than I thought it was, because this email seems to be quite legitimate as well, and this is also from iOffer. It’s saying that it’s received the payment, rather than asking for a payment or anything like that, so it does seem like this one might actually be real.

This one’s a little bit strange, because it’s from ‘epaypal.co.uk’, rather than actual PayPal, but at the same time, it does look quite legitimate. However, it does say at the bottom about it being a spoof email, all this kind of thing, which might seem like they’re, kind of, trying to cover their tracks a bit. I’m not 100% sure on this one, so I’m going to go for a three.

Okay, this one from Adobe seems quite legitimate. It’s referencing something that actually happened. It looks like it’s quite a legitimate email, and the link actually goes to the Adobe website, rather than anywhere else. If it’s from the Adobe website, then it’s not very likely that it’s spam or phishing.

Okay, this one from Plusnet also seems quite legitimate. It’s got a reference number, things like that. It’s got real email addresses for the Plusnet site. It’s also from ‘support@plusnet’. The only thing that I think might be a little bit strange is that it’s ‘support@plus.net’, rather than ‘plusnet.com’. I don’t know what the actual email is for Plusnet or anything like that, so I’m going to go for a four.

Okay, this one’s clearly a fake one. It’s pretty much, you know, like, the archetypal phishing email: Giving you a bit of information, spinning you a bit of a sob story, that kind of thing. Yes, this is quite clearly phishing, because it’s asking for full name, phone number, and from there you can get a lot of different stuff. I mean, they’ve already got your email address, so…

Yes, this one again is definitely fake. For one, online accounts on banks don’t expire, I don’t think. Also, looking at the address that it was sent from, it’s definitely not from the actual NatWest bank. Yes, this one’s clearly phishing.

The same with this one about the password expiring in three days. If your password for a site really was expiring, they would tell you which site it was, and it wouldn’t come from someone with an actual name. It wouldn’t come from [‘Sean T. Granada’ 0:08:23], it would come from the website that he worked for.

This Dropbox one seems quite legitimate, because this is the kind of thing that they do send when you first set up an account. It comes from a legitimate address, it comes from an ‘@dropbox.com’ address, so I’d say that this one’s legitimate.

Okay, this one’s obviously false. Oh no, no, okay. Never mind. This one seems quite legitimate. It’s been sent to the right place, all this kind of thing. The only issue is that it’s been sent to a different person, but then again, it has come from the real… Oh, no, this one’s more confusing. It says it’s from ‘service@paypal.com’, but it looks like it’s actually from the person that it’s apparently being sent to, so yes, it looks like it might actually be a phishing email, but I’m not 100% sure on this one, so I’m going to go for a three.

This one, I’m not too sure about. It doesn’t look real, it doesn’t have any of HSBC’s logos or anything like that. HSBC would not be called ‘hsbc/business’, surely it would have something to do with it being a bank. It just says ‘click here to begin’, it doesn’t show you a link to the actual HSBC website or anything like that, so I’m going to put that one as a two.

Okay, this NatWest one seems quite legitimate. It’s not asking you to click anywhere that does look like it might be something else. It’s asking you to click on the NatWest website, it’s not trying to hide it, the address of the website or anything else. The actual email address is from ‘information.natwest.com’. I’d say this one’s quite legitimate.

Okay, this one, ‘Verified by Visa’, obviously it is a real thing. However, the fact that there’s, like, an exclamation mark in the title, that kind of thing, I wouldn’t say… In the subject, even, I wouldn’t say that that’s been sent by the actual website. The fact that it’s got, again, arrows leading to, you know, where you should click and whatever, trying to tempt you into clicking that link. It doesn’t seem legitimate.

Right, okay, this one seems fake. I don’t know that much about Diablo or anything like that. I don’t know where it’s actually made by Blizzard Entertainment or anything like that, but the fact that Blizzard Entertainment uses a battle.com email address seems a little bit strange. The fact that it’s asking you to download something onto your phone also seems a little bit strange, so I’ll put that one down as phishing.

Okay, this one, I would say, seems pretty legitimate. ‘billing@ebay.co.uk’, that sounds correct. It gives an actual invoice number, an amount due, all this kind of thing. It’s not asking you to click on any strange places, it’s telling you to go straight to the eBay website, so I’d say that this one’s legitimate.

Okay, this one’s from ‘slc.co.uk’, which, at first, looks pretty legitimate, but then, when you look at the actual link that it’s asking you to click on, it’s [‘mineface.com’ 0:13:26], which doesn’t really seem like something that a Student Loans company would ask you to click on, so that’s phishing.

Right, this Dell one you can tell is fake straight away because of the email address that it’s using, and also because it’s asking you to click on a link that has nothing to do with the Dell website, so I’ll put that one as phishing.

Okay, this one, it seems quite legitimate, actually. It’s giving you a job that you’ll be interested in. The link corresponds to the email address. However, I’m not 100% sure whether ‘i-grasp’ is a real website or not, so I’m going to go and put a three.

Okay, this one, it’s from ‘nusextra.co.uk’. I don’t have an NUS Extra card, so I don’t know whether this is real, but the link that it sends you to is for nusextra.co.uk, so even though it’s a long address with lots of different characters and everything, it does seem quite legitimate. It’s told you what IP address it’s from, but then again, it is also asking you to click on the address [if you want 0:15:12], which I don’t think you can actually do, so I’ll put that as a four.

This one’s obviously fake. It’s telling you that you’ve won something for free. The email does not look legitimate, it looks like a personal email address, rather than a business one.

Okay, this PayPal one is quite legitimate. It says [it’s from… Same 0:15:45], is ‘@paypal.co.uk’, and the actual email address confirms that. It gives you an option to update your card, all this kind of thing. It’s got advice for safety, it looks like it’s a real email address.

This one, they spell ‘Student Finance’ wrong, so that’s obviously phishing.

No, Facebook doesn’t send you emails using this address, I don’t think, but I’m not sure, because it is linking you to facebook.com. Yes, I think I’ll put this one as five, because it is taking you straight to Facebook.

This one, again, is trying to play on sympathy to get you to send money, which obviously you would not get back, so that’s phishing.

Okay, it’s telling you not to send money to people. It’s been sent from an email address that actually corresponds with the website, so I’ll put that as a five.

Virgin Mobile would not send you something like that, I don’t think. They would also have ‘copyright’, other things, how to unsubscribe from the emails, that sort of thing, at the bottom, if it was true. The fact that they’re using a zip file seems a bit strange as well. Also, the fact that it’s ‘thanks@virginmobile.com’. Yes, I don’t think they’d use that address.

Okay, this one says it’s from Blackpool Pleasure Beach, and I think it is actually Aspect that runs Pleasure Beach, so that looks like it might actually be legitimate, yes. Yes, it’s got a survey, that kind of thing. “Only be used for research purposes,” and it’s got a number at the bottom that you can reference if there are any issues, so I’d say that that’s five.

This DVLA one is fake, because it’s not from the DVLA email address. Yes, I wouldn’t say that this is correct.

Okay, this one’s from a ‘lancaster.ac.uk’ email address, which seems quite legitimate. It’s a SurveyMonkey link, which is a legitimate website, and they’ve got a way to contact people if it doesn’t work out, so this one’s legitimate.

**P336**

P336: Okay, a little spelling mistake which always makes me think that something might be wrong with the email. It says, “To allow us update,” instead of, “To allow us to update.” And the web link doesn’t include anything to do with student finance, which makes it look like it might be fraudulent. Usually they might just say, “Go on to the website to enter your information,” rather than following a link, so I think that that is phishing, definitely.

[Break in Audio 0:00:49 – 0:01:10].

Okay, so this one could be legitimate because it has the name of the place in the web link, Grasp or i-Grasp, and it’s not asking for any personal information, it’s just asking you to follow the link to find out about a job. So I think this one is more than likely legitimate. I’m going to go with 5 because I’m not 100% sure, but I think it is.

[Break in Audio 0:01:51 – 0:02:08].

Okay, I think this one is phishing because usually if you order something it will say, “Dear,” and your name, because they’ve got your name on the database, whereas this just says, “Dear Guest User.” And usually they’ll give you a snapshot of your order and your order number and things like that. So I think this one is phishing definitely.

[Break in Audio 0:02:38 – 0:02:50].

Okay, this one is definitely phishing. It’s asking for account information and to follow a link to put the information in. Whereas if it was a real Direct Gov website they’d ask you to just go to the website manually rather than follow any links. And it gives an ultimatum that if you don’t do it payment will be suspended but if it was that important they would probably call to make sure that you do it or give you at least a few months’ notice to be able to sort it out, so definitely phishing.

[Break in Audio 0:03:33 – 0:03:52].

Okay, I think this one is definitely legitimate, it’s not asking you to follow any links, it’s just telling you to go on to your account and change your password if you haven't signed on in this location. So this one is definitely legitimate I think.

[Break in Audio 0:04:09 – 0:04:24].

I’m not sure about this one because it’s asking you to follow a link but it’s not asking you to put any information in or anything like that, but then at the bottom it says, “Beware of Scams,” which is something that someone would say if it was a scam to make you think that it’s not a scam. But I think it could possibly be phishing because it would just tell you to log on to your profile yourself to go and see the message. So I’m going to put 2 because I’m not 100% sure that it’s phishing but I think it is.

[Break in Audio 0:05:10 – 0:05:46].

Okay, this is probably phishing because if you’d applied for a job already you probably wouldn’t need to download another application form, you’ve probably already filled one out and they wouldn’t attach it as a web link, they would just attach it as a document, like a Word document or something to send back. Or ask you to go to a website again to fill something out yourself. And also, there are quite a few spelling mistakes and it’s not worded very well. So I’m going to say definitely phishing.

[Break in Audio 0:06:29 – 0:06:51].

I think this one might be phishing because there’s spelling mistakes again. It says, “The bill for your Virgin Media Mobile is now and ready to view,” which doesn’t make sense. And it says, “The Direct Debit will be taken on or immediately after the 20th October,” which is not how someone sending you a bill would write it.

And they wouldn’t say that they’re not picking up emails from this address either, I don’t think. And I think just the address, that it’s from ‘Thanks at Virgin Mobile’ is not very legitimate. If it was a bill it would probably have like something with a bill in it or something from Customer Services maybe. So I’m going to say definitely phishing because it includes a link to send them an email and you probably would follow that link instead of going on to the website manually. So definitely phishing.

[Break in Audio 0:07:54 – 0:08:23].

Okay, I think this is definitely phishing because it’s saying that if you don’t follow a link immediately you’ll have your account taken off you which is never really how it works, they would just tell you to log in manually and sort it out yourself. And also, again, it’s not written very well. There are a lot of grammatical errors so I’m going to go with definitely phishing.

[Break in Audio 0:09:06 – 0:09:19].

Again, definitely phishing. Telling you, “Your password will expire in three days,” and then, “Follow a link to change it.” And then it’s just signed, “System Administrator.” You don’t know who this is off, what password will expire, there’s nothing telling you anything about it so yes, it’s definitely phishing.

[Break in Audio 0:09:47 – 0:09:59].

Okay, I think this legitimate. They’ve got the invoice of what you’ve bought, the item number and the quantity so if you need to ring up you’ve got your item number there. And usually they do send you that before sending you your payment and shipping instructions like what it says, so it looks pretty legitimate to me. I’m going to go with definitely legitimate.

[Break in Audio 0:10:27 – 0:10:41].

Okay, I think this is maybe legitimate. Although it has a link to updated Terms and Conditions it’s not asking for any details. It’s not asking you to put in any details or anything, although if you were to follow the link it could ask you to put in your MasterCard details and then I would definitely know that it’s phishing. And it is signed off by the right people and the address and the email address looks sort of alright.

I’m not sure about this one; I’m going to go with 4. No, I’m going to go with 3 because I think it might be phishing but I’m not 100% sure, I don’t know about that one.

[Break in Audio 0:11:42 – 0:12:02].

Okay, this is definitely phishing. It’s just someone emailing asking for money and the subject is ‘Sad News’ which is not really what you’ll say for this. It’s quite a dramatic thing that’s happened to them, getting attacked and everything stolen. And if it’s someone who you’re going to ask for money you would probably try to call them and you would have heard about it yourself. Yes, so this is definitely phishing.

[Break in Audio 0:12:40 – 0:03:09].

I think this is probably legitimate, they’re just asking you to complete a survey, although they do have a time limit you have to fill it out by, which is a bit strange. Again, it’s one of those where if you follow the link and it starts asking for more details, like your bank details or your address or anything, then I would say it was phishing. But I’m not really sure without that. I’m going to say a five because I’m not sure it’s definitely legitimate but I think it probably is.

[Break in Audio 0:13:54 – 0:14:17].

Yes, I’m going to go with five. Okay, this is definitely phishing. Someone who is introducing themselves to you so you don’t know them and they want your name and phone number so that they can give you money, which is just too good to be true. Yes, definitely phishing.

Okay, I think this is definitely phishing as well because, again, if someone has tried to change your password they would just tell you to log on to your account to make sure that your password’s secure or change it or whatever but this is asking you to actually follow a link to change your password so I think it’s definitely phishing.

I think this is probably legitimate. A lot of the time companies need your email address verified before they can do various things. So yes, I think this is definitely legitimate. And also you’re just putting in your email address, which if it was phishing they’re not going to gain anything from, other than selling your email address to other people.

[Break in Audio 0:16:19 – 0:16:41].

Yes, I think this is legitimate. Again, it’s just sending you a payment transaction. It’s got all of the information on it, what you sent to them, that item number, price, quantity, and there’s no link to follow to put any details in or anything. There’s a link to follow to ask questions but that wouldn’t be anything that someone would put on if it was phishing. Again, the only other thing is an email address for the person you’ve sent money to, which you wouldn’t contact them anyway. If you thought this was wrong you would just contact PayPal. So I’m going to go with definitely legitimate.

[Break in Audio 0:17:39 – 0:17:52].

Okay, I think this is not legitimate. There are a lot of mistakes in the first sentence and the wording is strange, “We thought you must be informed that we shipped your item.” It’s not really how Amazon would word it. And, “This completes your order.” And although it has some information, like how much it was, what you’ve bought, there’s no item number, there’s no way to track it. There’s nothing to tell you where to go to ring them up if you’ve got any problems or anything like that, so I think this is definitely phishing.

[Break in Audio 0:18:44 – 0:19:05].

I think this is definitely legitimate, there’s no links. Well, there’s one link. I can’t tell if they’re links. There’s NatWest.com/online and NatWest.com/your statement. I think they might be links actually, which makes me think then that it is phishing because they wouldn’t give you the web address I don’t think, they would just tell you to log on to your online banking, they wouldn’t give you any links. So I’m going to say this is definitely phishing actually.

And then there’s also a link to, “Contact us,” and you just click the link and it’ll give you a number, which it wouldn’t do as well I don’t think, because those links could be leading to anything, not necessarily NatWest. Although I presume that the NatWest website is NatWest.com. I’m going to go with two because I think it is phishing but I’m not definite about it.

Okay, this one is definitely phishing. It’s telling you, “Your online account will expire today,” which online accounts, I don’t even think they do expire. And then you have to follow a link to continue using the banking, which it wouldn’t say, it would just say, “Log on to your online banking,” without a link. And then it’s also only giving you 24 hours to do it. So I think definitely phishing.

[Break in Audio 0:21:11 – 0:21:26].

I think this is definitely phishing as well. You follow a link again to update your card and this link will probably not take you to the PayPal website if it’s phishing. I think if it was legitimate they would just say, “Log on to your account to change your card,” without the link, so definitely phishing again.

Definitely phishing again. Following a link to update your credit card information, which just would not happen. You would have to go into whatever bank it is, I presume, to sort that out if your credit card had been disabled, so definitely phishing.

[Break in Audio 0:22:25 – 0:22:53].

I think this is phishing again, although it does seem legitimate. Just the way it’s written and things, it looks legitimate but it’s asking you to follow a link to change your password, which just always makes me wary. I just think that they would say, “Please log on,” or, “Please go to the website to change your password,” rather than following a link. So I’m going to say definitely phishing.

[Break in Audio 0:23:27 – 0:24:23].

I’m not sure about this one. Some of the wording is a bit weird, it tells you the amount that you need to pay for this invoice and then it says, “The amount deducted may vary based on recent payments or credits,” but that doesn’t seem right because they’d just give you an invoice for that month which wouldn’t change. So I think that makes me a bit wary. And then also following a link to log in but the link looks legitimate, just eBay.co.uk. And it says at the bottom, “Remember eBay will not ask you for sensitive personal information.” I’m not sure about this one. And then it also says right at the bottom, “Learn more to protect yourself from spoof [say 0:25:36] emails,” which is a bit weird. I’m going to put 2. I think it’s phishing, but again, I’m not 100% sure.

Yes, this is definitely phishing because it’s a bank asking you to click on a link to verify account details, which they wouldn’t do. Again, they would just tell you to go on to your Barclays account, on a website or phone them up or something like that. So this is definitely phishing.

[Break in Audio 0:26:18 – 0:26:35].

This seems like phishing because the grammar and spelling is really bad again. However, they’re not asking for any details but there is a link to get a postal receipt which may then follow on to ask for some details. And the email address is weird. You’d think it would have FedEx in it if it’s from FedEx but it doesn’t. Yes, I’m going to say it’s definitely phishing actually because they would have FedEx in the email address. And if they wanted you to pick it up from an office they would just say, “Go to our website to find your nearest office,” or something like that. Or they would actually tell you which office it’s at. So yes, definitely phishing.

[Break in Audio 0:27:32 – 0:27:52].

I’m not sure about this one. It does give your account user name, which if you know that to be right then you’d think that it was legitimate. Which I presume it is right. It does ask you to follow a link and log in with a user name and password but that wouldn’t lead you anywhere because you know that you’re trying to download security software so you wouldn’t try to download it if you didn’t know your user name and things.

However, if they’re giving you your user name and you might have thought that you’ve forgotten your user name then they’ve given it you, so you might just follow the link and say that you’ve forgotten your password or guess your password and then they’ve got information from you.

I’m going to say 4. I think it’s legitimate but with you having to follow a link to download something I’m not 100% sure. I’m going to say 5 actually because the email address looks legitimate as well, ‘Support at Plusnet’. Yes, I’m going to go for 5 because I’m not 100% sure but I think it’s legitimate.

[Break in Audio 0:29:38 – 0:29:58].

I think this is probably legitimate because although it’s asking you to follow a link it does say, “If you are concerned about the security of this email…” Although it wouldn’t say, “Type PayPal.co.uk into your browser.” And I don’t know what the actual PayPal website is, so I don’t know if that will take you to the right place or not.

[Break in Audio 0:30:25 – 0:30:42].

It says, “How do I know this is not a phishing email? An email from PayPal will always address you by your first and last name.” But it is easy for people to get hold of your first and last name these days so that’s not necessarily a good indicator that it’s legitimate. It does have your email address too. I’m going to go with five. I think it is legitimate but I wouldn’t follow the link just in case. I would just log on to the website myself. Yes, I’m going to go with five.

[Break in Audio 0:31:26 – 0:31:41].

Definitely phishing again. I can see that it’s from a bank and asking you to click a link to resolve issues with your account, which will probably go on to ask you for your account details and things like that. And it’s signed ‘Customer Business Unit’ rather than ‘HSBC Customer Services’ or anything like that. So yes, definitely phishing.

[Break in Audio 0:32:08 – 0:32:33].

I’m not entirely sure about this one. It’s asking you to follow a link to confirm an email address, which places do sometimes do that if you change your email, because then they’re sending it to your email that you’ve changed it to. But it does say, “If you didn’t enter the address disregard this message,” which is a bit weird because if you didn’t enter it then how have they got your email? I would think that was a bit weird.

I think I’m going to go with four because the link is Facebook.com, which is the link for Facebook. I’m going to go with five I think actually because, yes, the link is Facebook.com and they’re not asking for anything other than your email address. But I just think it’s a bit weird that they say to disregard the message if you didn’t enter the address. So a five.

[Break in Audio 0:34:01 – 0:34:34].

Okay, this is definitely phishing. I thought it wasn’t going to be at first because it was saying, “Go on to the website to sort out your information online.” But then right at the end it has a link to follow, which looks like a bit of a weird link. It has eBay in it but it’s got CGI1 as well, which I don’t think it would have. And it’s going into a lot of detail about the account being a cause of financial loss and it’s a bit weird because I don’t think they would do that. So I think this is phishing definitely, I’m going to go with one.

Definitely phishing. There’s no information other than, “Click here if you use [Yahoo and 0:35:36] email.” And then another, “Click here if you want a luxury watch.” And that’s just definitely going to lead you to something weird and it’s from an unrecognised email address, so yes, definitely phishing.

[Break in Audio 0:36:02 – 0:36:32].

I think this is probably legitimate, it’s just asking you to complete a survey from Visiting Blackpool Pleasure Beach, and it does say that you will be entered into a prize draw but if you follow the link and it asks you for an email address or any personal information then you don’t have to put it in if you don’t want to, you can always close the link down. So I’m going to say definitely legitimate.

[Break in Audio 0:37:05 – 0:37:22].

This is definitely phishing. The DVLA wouldn’t send you a web link to update licence details because not everyone has email addresses and not everyone uses the Internet that often, especially older people, so they would just send you a letter I think or something like that if you needed to do anything, so definitely phishing.

[Break in Audio 0:37:45 – 0:38:06].

I think this is definitely legitimate. It’s asking you to fill out a survey and it’s on Survey Monkey which is a legitimate website and it also has an email address of the person conducting the surveys so you can always speak to them if you’re a bit unsure. And again, although it’s saying, “You’ll be entered into a prize draw,” you don’t have to put your email address or any contact details, so I’m going to say this is definitely legitimate.

**P337**

P337: ‘Dear candidate, a \_\_\_[0:00:01] which most of you \_\_\_ published on our website. Please click to follow the link or paste it into your browser and search for the vacancy references listed below. [Yours sincerely]-’ well it’s from the recruitment thing, so I would say- ‘Good luck with your job search.’ I would say it’s a five, actually. Looks legitimate.

This looks a little bit more- it looks like an auto-mail. I wouldn’t say it’s that legitimate, actually. The fact that it actually gives you a website to download something, it could be a virus. I’ll say a two.

‘HSBC, the world’s local bank.’ I don’t think you usually, like, click to get into a different account. They never send you any sketchy emails like this from the bank. So I will say three. ‘Hello, the bill for- is now ready to view. The balance \_\_\_[0:01:30] head over to our website to send us an email.’

[Silence 0:01:37-0:01:55]

Why would you head to their website to send them an email? I’ll say a three, because I’m a little bit unsure whether it’s a legit website or not. It could be that they actually [aspire to address 0:02:16], but why wouldn’t they- this is sketchy. You would have, like, the full address already in the email, if you were to send them.

‘This is a message \_\_\_[0:02:32] from the Student Loan Company.’ That’s definitely sketchy. Amazon. I’ll say this is quite legit, five. Also, because I know that website. ‘Your card is about to expire. Update card.’ That could be, like, they’re tracking down your card details. But is this PayPal? Yes, I would say it’s legit.

I’ll say this is [legit 0:03:31] as well [as PayPal]. You don’t have to download a free app. I’ll go with a four for this one. ‘Dropbox need to verify your address \_\_\_,’ I think this is legit as well. I use Dropbox. ‘Your password will expire in three days, click here to upgrade it.’ Oh, this is a little bit sketchy.

Visa. I don’t think you can, like- usually you have your own password to do it, especially if it’s credit card. It’s quite important that it’s not, like, something- so I’ll say this is also a little bit suspicious. I’ll give a three. I’ll say this is sketchy and give it a three. ‘I’m sorry for reaching you rather too late to \_\_\_[0:04:37].’ Definitely sketchy.

I’ll say this is quite legit. ‘Greetings, it has come to \_\_\_[0:05:03] trying to sell \_\_\_.’ This is quite sketchy, so I’ll say a two. Dell, ‘Thank you for your recent contact, blah, blah, blah. At Dell, we’re committed to deal with the best \_\_\_[0:05:23]. To complete a survey, please-’ it’s a survey, so I’ll say it’s a five. ‘eBay suspension. Dear valued member, we \_\_\_ your eBay account has been suspended.’

[Silence 0:05:35-0:05:49]

This is, kind of, hard. Why would they give you an online experience and \_\_\_ your personal records if they already suspended you? I’ll say a three. ‘Dear customer, your parcel has arrived at the Post Office. To receive a parcel please go \_\_\_[0:06:08].’

[Silence 0:06:10-0:06:26]

Well, I’ll say a five. Barclays, I’ll say this is a two, it doesn’t look sound. ‘Password reset information.’ I’ll say this is quite legit. Woah, what kind of account is that? I’ll say two, looks a little bit suspicious. Even the mail address is blocked. ‘Dear applicant, thank you \_\_\_[0:07:03] like to let you know we \_\_\_ soon.’

[Silence 0:07:07-0:07:27]

I’ll say a three, it looks a little bit suspicious. ‘Hi Helen, here’s a new \_\_\_ email address \_\_\_.’ I’ll say this is quite legit. ‘Invoice.’ Yes, this is also legit, it’s eBay. NatWest, ‘[Don’t 0:07:53] use your online banking, please log in \_\_\_ today.’ I’ll say it’s a four.

PayPal, looks like a five. It’s by PayPal. It’s a confirmation that you got a payment through. Sometimes \_\_\_[0:08:23] Google. ‘Hi [Helen], someone’s trying to use \_\_\_ Google account. You do not \_\_\_ immediately, \_\_\_.’

[Silence 0:08:34-0:08:46]

I’ll say a three. I don’t know whether it’s suspicious or not. ‘Dear guest user, Google \_\_\_[0:08:54] receive payment \_\_\_, thank you.’ This looks very suspicious. I’ll say a two. ‘Hello, I’m Mr Gary Copper, I was born in January \_\_\_, suffering from lung cancer.’

[Silence 0:09:13-0:09:25]

Very suspicious, ‘Leave his fortune to her.’ ‘Hi \_\_\_.’ I’ll say a two, looks suspicious. ‘Your latest statement is available online.’ It looks legit. ‘[Direct Gov 0:09:44], there is a formal notification of an important account update, \_\_\_ click here \_\_\_.’ I will say a two, that’s a little bit suspicious too. ‘Good day, give your loved on a luxury-’ \_\_\_ definitely, commercial.

‘Dear Pleasure Beach visitor, Pleasure Beach Blackpool \_\_\_[0:10:08], click on the link below.’ Could be, so I’ll give it a four. It’s a questionnaire. ‘ \_\_\_ drivers are required \_\_\_ verify driving licence details.’ I’ll say a two, looks very suspicious. ‘Dear student, welcome to Lancaster. We hope you have enjoyed your first week \_\_\_[0:10:34].’ Sounds legit. \_\_\_.

**P338**

P338: So, \_\_\_.

[Break in conversation 0:00:05 - 0:00:17].

Definitely no. That’s phishing. [Mainly because it’s from] \_\_\_ something, but yes, \_\_\_ .co.uk, which seems [probably] not a real email address, so I would say phishing.

[Break in conversation 0:00:38 - 0:01:03].

Well, that’s a tricky one. [I don’t know]. The address seems right \_\_\_ website address \_\_\_ information. They don’t have even the same thing as – no, it doesn’t seem right. \_\_\_[0:01:24], [so that’s] phishing as well.

[Break in conversation 0:01:29 - 0:01:53].

Yes, that seems… Yes, that doesn’t [want to ask for any] information to give. [They're] just informing you that you will be paying something automatically from PayPal, so \_\_\_[0:02:13] [give] information to pay something, so that’s [a good email] \_\_\_.

Well, that is definitely not a real email, \_\_\_[0:02:40] [text email], that’s [PNG attached], so that’s not likely to be a real email \_\_\_ text instead of [attaching an image of] text, so phishing.

[Break in conversation 0:02:57 - 0:03:36].

Well, that email \_\_\_ [seems a bit awkward], but I'm not familiar with Blizzard [anyway]. Yes, it’s probably [a real email], because they don’t ask you anything from now, \_\_\_[0:03:54] oh, yes, maybe \_\_\_ [IDs] \_\_\_ account and then use that instead of you. I don’t know. Yes, maybe that’s not phishing, but I'm not very confident about \_\_\_[0:04:17]. Let’s say something halfway, like maybe just an eight.

Okay, so that’s definitely not a legitimate thing, I think. Oh, yes, [the email 0:04:43] seems right, but [there’s a big red thing], like, ‘Please do not reply to this email. [Follow the link below to your account to] reply.’ It’s a bit too [flashy] for a real email, I think. Yes, it might be true, so let’s say yes. Okay, yes, so it’s definitely \_\_\_[0:05:16] [to be aware of not] sending money from anything, so yes, maybe legitimate. Yes, it’s legitimate.

[Break in conversation 0:05:25 - 0:05:41].

That seems [like a real email], like the email address. Oh. Yes, that seems okay, and [they're not 0:06:03] asking [much] things, [like you have just] reset your password. \_\_\_ [will] ask your ID, because maybe the ID is \_\_\_ to the link. So, yes, that seems a legitimate email.

PayPal. Well, that seems like – yes, that \_\_\_[0:06:35]. A bill from eBay, like a bill from PayPal for an eBay payment. It is not even trying to ask for information, so, yes, that’s a legitimate email.

[Break in conversation 0:06:52 - 0:07:09].

Okay, so, that seems a bit awkward. (Laughter) Yes, \_\_\_[0:07:24]. They are just giving you as well the IP address from which it has supposedly been taken, so maybe you can just check that, that’s your IP address. They won’t do that. Oh, yes, maybe.

I don’t think they can take your IP address before sending you an email, so if it’s your IP address then it’s a good email, and [therefore 0:07:54] they won’t make a false IP address. Oh, yes, \_\_\_ [false IP] address \_\_\_ someone not you have done that.

Oh, actually, no, that’s fine, because it just \_\_\_[0:08:14] process if it wasn’t you \_\_\_, and if it was you, yes, then you know if it \_\_\_ or not \_\_\_, so that is a legitimate email.

[Break in conversation 0:08:26 - 0:08:44].

Okay, that’s likely to be a legitimate email, and they are not asking [much things], and the [email address] seems right. Yes, I think that’s \_\_\_[0:09:03] is legitimate, yes.

Oh. [That’s definitely not a real email like]. ‘Your password will expire in three days.’ Really? Does any password even expire [in time] \_\_\_? Yes, so that’s phishing.

So, \_\_\_[0:09:27]. [That just seem like false things], like @verifiedbyvisa.com. What the hell is that? It should be your bank, not visa.com or something. Yes, definitely phishing email \_\_\_[0:09:47], yes.

That’s just some kind of bill, \_\_\_ doesn’t ask you anything, so yes, \_\_\_[0:10:06], Yes, of course, thinking your account will expire today. Yes, I don’t think so. Accounts don’t expire, right? Just cards do, and then you get a new one \_\_\_. Yes, that seems really phishing. Oh, yes, and the email address, \_\_\_[0:10:31] .com.

Yes, that’s just [a bill] as well, so yes, legitimate.

\_\_\_[0:10:47]. Yes, that’s \_\_\_ just a bit of information, [shipping information], for the same TV. Oh. Yes, [that’s good, isn’t it, because they are not asking anything 0:11:07] from you, so that is legitimate.

Oh, yes, that’s an awkward address, but Facebook does awkward addresses to [get you] notified. Yes, that’s just like \_\_\_[0:11:32] Facebook account, so that’s not even logging into your Facebook account, so you don’t have to \_\_\_, [so that is legitimate].

Oh, that’s a tricky one. Yes, I think \_\_\_[0:11:54] email address, service@paypal.co.uk, and that’s likely that PayPal will warn you that your card is going to expire, because they know your expiry date on the card, because you send that. So, yes, that’s legitimate. Yes, there is plenty of information about PayPal on that. Yes, it seems right. That’s okay. Okay, no, that’s a good one.

\_\_\_[0:12:39] paypal.co.uk \_\_\_ [and it’s just like] why would PayPal do that anyway, like telling you to login to see what funds \_\_\_[0:12:55] [last month]. Yes, I think that’s phishing, probably.

Oh, yes, okay, \_\_\_[0:13:11] phishing, \_\_\_ about, “How do I know it’s a spoof email or not?” Maybe it’s not phishing. Maybe, but yes, \_\_\_ and they probably just want [you to logon to 0:13:32] PayPal’s database and have your name, [so anyway].

That’s just, “[What the fuck]?” There’s not even any content to make you click here, just, ‘Hey, click here.’ No, that’s phishing.

No, \_\_\_[0:14:04] [email address] doesn’t seem good. If it’s HR Recruitment Department they would have a website from the company you are going to work with \_\_\_ @yahoo.co.uk address. Yes, definitely not. \_\_\_[0:14:27]. No. That’s phishing.

That’s classical phishing, like, ‘Hey, I need some money. I will refund you.’ No. I don’t even know you.

Oh, that seems – oh, no, wait. ‘Incoming funds blocked.’ [Why would they block 0:15:21] incoming funds. They could have blocked outgoing funds, outgoing payments, but… Yes, I guess that’s phishing. Yes, plus HSBCs \_\_\_[0:15:39] definitely looks like bad quality [made], so, yes, probably phishing.

Oh, Barclay’s. Yes, [it’s an email 0:15:57] from Barclay Online, but the address is \_\_\_ .com. Yes, probably phishing.

[Break in conversation 0:16:11 - 0:16:23].

Okay, it’s probably just [a false thing]. I'm not familiar with England Student Finance, but unless it just logs \_\_\_ database, and you don’t have any backup, they wouldn’t ask everyone to go back and check their information, and update the information. No, that’s phishing.

[Break in conversation \_\_\_[0:16:50 - 0:17:03].

Well, \_\_\_. Oh, no. Okay. Yes, the address is [@fortwayne.com, which is unlikely to be \_\_\_ for FedEx, so that’s probably just \_\_\_ or something.

\_\_\_[0:17:23] @ebay.com. That’s phishing, \_\_\_.

That’s a classical [email phishing thing], when you just start using something, and that’s noreply@ \_\_\_[0:17:42].com. That is like the main address of \_\_\_, so it’s legitimate.

Well, (Laughter) this email address, @ \_\_\_ online.com. [What the hell]? Yes, you have to complete a survey before \_\_\_[0:18:09]. [Why would they ask that]? If they will want a survey they will just wait for it, so that’s phishing.

Well, that’s – oh, that’s \_\_\_[0:18:33]. I don’t know i-Grasp \_\_\_ [www21.igrasp], 21 \_\_\_, isn’t it? \_\_\_. It’s not \_\_\_[0:18:52] anything. Maybe you \_\_\_, but yes, \_\_\_. That’s probably legitimate.

Yes, I don’t like the attached \_\_\_[0:19:28], the zip. That’s quite likely to be a virus or something even, \_\_\_, but yes, that’s probably a virus, so don’t load this zip file. Okay, so, that’s definitely phishing \_\_\_[0:19:52] phishing \_\_\_. No-one does that, send an email to people \_\_\_.

Yes, that seems a real email. The email address is good. The format is quite good. They are not asking you to do anything. Yes, probably a good email. Legitimate.

[Break in conversation 0:20:23 - 0:20:40].

That seems like a real email, [and you] can just click on that link and [you just feel very awkward] \_\_\_, but the email address is good. \_\_\_[0:20:56]. Okay. That’s fine.

Okay, \_\_\_[0:21:13] driving licence \_\_\_ in England or something like that. (Laughter) Why would you have that? Plus, it’s the DVLA that’s writing to you, and it’s dft.gov.co.uk, the address. Yes, that’s probably just phishing.

Yes, that’s \_\_\_[0:21:49] from the university. [Yes, SurveyMonkey] would not make you download anything. No, that seems [a good] email. Legitimate.

**P339**

P339: \_\_\_[0:00:00] the email address. [“3.co.uk], yes, that’s dodgy. That’s okay I’m going to… That’s [sort of thing 0:00:20], ‘3’ makes me a bit worried. Also, the fact that it’s an email address, otherwise it’s not asking for much, so I’ll give it a five. Kind of legitimate, almost. I guess I get lots of these.

“Thanks, virginmobile.com.” Oh, look, just no name for attachment, that’s it. That’s completely legitimate. [Write that date 0:00:53]. Oh, so it’s saying nothing, but people would be very likely to click on that. Yes, yes, no, I’d go towards the phishing side of it. It looks very nice and official apart from the \_\_\_[0:01:12] attachment. There, it’s a virginmobile.com address. No, attachment is dodgy.

“Verified by Visa.com. Spend it, please update.” It’s going to \_\_\_[0:01:34], why does that look like a picture? “Because an error was detected in your credit card information. The reason [we’re not certain] is \_\_\_ information.” (Laughter) I’d check the credit card was suspended before sending that. “Click here,” it’s dash, dash, dash, is quite awkward. “\_\_\_[0:02:01], please.” I’d ring them, I guess. Yes, but is it phishing or not? It’s the dash, dash, dash and the ‘click here’ that makes me a bit worried. The ‘verified by Visa.com’. What the fuck’s ‘verified by Visa’? Yes, it’s phishing. It’s definitely phishing. ‘Verified by Visa.com’ is a \_\_\_[0:02:20].

‘service@paypal.co.uk’, I think I’ve actually seen this one. “It’s about to expire, please update your card expiring, date, security code, as soon as possible to \_\_\_ [options]. You have received a new card, please link the card.” Hmm, link like that? “\_\_\_[0:02:43] your PayPal [card]…” I wouldn’t click on the link, I’d go to the website if I got an email like this, although I ignore PayPal. Hmm, I don’t think this is phishing, but I’m not saying it’s definitely legitimate. Why? The fact that, like, bits are missing of the outside, that’s normal, that can happen, depending on the email address that’s getting it. Although, I suppose, at least \_\_\_[0:03:13] [email address], so that’s mostly legitimate but I don’t think it’s definitely legitimate. Why? Because I’m always suspicious of this.

Student Finance, ‘E’, definitely phishing. I mean, give it another go, but that’s definitely phishing, ‘finance, E’. “\_\_\_[0:03:36] [direct], we require all students…” Oh, there’s a comma and a capital letter. \_\_\_ would not do that. “Click here to follow the \_\_\_.” Yes, dot, “…Or your payment will be suspended.” Yes, that’s definitely phishing.

‘frank@easyroommate.com’, the subject, “You have mail”. “\_\_\_[0:04:10] application and \_\_\_...” Oh, my eyes. That’s just a website, I can’t tell if it would download anything automatically. “Beware of scams, \_\_\_.” Why, “Do not send money via Western Union,” Western Union is fucking safe to send money. I don’t know, this could be plausible, if you actually get something like that. I’m putting a four. It’s plausible but it’s not definitely phishing.

Any day now, next page. Thank you. [‘Boucheron 0:05:01], btinternet.com.” \_\_\_ dot, dot, dot \_\_\_. “\_\_\_ money first.” (Laughter) “\_\_\_[0:05:24] [two] \_\_\_ to come back and \_\_\_ [reply], \_\_\_ leaving in a few hours. I wonder if you can help us with a quick \_\_\_.” No, ‘boucheron@btinternet.com’. I don’t know you, you’re supposed to assume these emails are somebody you’ve known. Oh, sorry, all he needs is that much money to [shut down and go home 0:05:51]. Sorry, Philippa. The dot, dot, dashes in the subject make it seem like it is somebody that wrote it in a hurry, but it’s [actually] from that guy. I suppose if he was in, like, a stressful environment… I don’t know if I know he’s visiting Manila. Although, nobody said… No, it’s phishing.

“Hello…” Email from NatWest, I casually ignore every month. ‘information.natwest.com’. Hmm, “It’s for account ending [is ready 0:06:35] for you. Just log on to natwest.com online.” See, it’s not telling you that’s the right website. “Forward slash your statement.” It’s not asking anything of you, it’s telling you the correct website to log on to. Let’s put that email, that link \_\_\_[0:06:53] account. Right, that’s legitimate. [You’re] suspicious. \_\_\_ suspicious, natwest.com. I’m suspicious of the ‘information.natwest.com’, but otherwise I can’t see anything wrong with it. They’re not asking, they’re just telling you, and the web links we fine.

“HMPS Recruitment, [i-grasp.com 0:07:17], job alert. \_\_\_ published on our website. Please click the following link or paste it into your browser, search for the vacancy \_\_\_ listed below. Search for the reference \_\_\_ [below 0:07:36].” The links are too dodgy. I’ve never heard of i-grasp. Yes, this… Yes, the emails are requesting… If I’m requesting an email from this website, then that would not be phishing, that would be, kind of, legitimate, just poorly written. They’ve sent it via… But that’s what happened. Yes, [I’ve checked the times 0:08:09] before. I’d give it a five, just because the email addresses that you’re supposed to click on look a bit dodgy. I don’t know what ‘www21’ is. I might give it a four now, yes. If I was waiting for an email like this… No, four.

“eBay administration, ebayz.com”. ‘ebayz.com’, eh? That’s [silly 0:08:47]. “Regret to inform you, [this has ended], da, da, da, da, da, \_\_\_ suspensions prohibited. Take out five minutes of your online experience to update your personal… Out of your own \_\_\_[0:09:03] your personal records, we will not \_\_\_ future problems, yet you will still run into future problems, you should still run if something like this happens.” Again, if it were legitimate… “The 10th December.” This is 10th December that you sent me that, definitely phishing. Pushing people and it’s… Again, that email address.

It’s a [tiny 0:09:31] email \_\_\_ survey. [rap] \_\_\_ [online.com]. “Thank you for your recent contact, \_\_\_ regarding case number [Dell]. At Dell, we are committed to delivering a [pleasant] experience…” That is really tiny, glasses or no glasses, I wouldn’t even see that. “\_\_\_ feedback regarding your experience. To complete the survey, please click on the address below by… If it does not work, copy and paste,” that’s fine. \_\_\_[0:10:00]. No, that’s a [server maintenance] sort of email address. It’s a bloody survey, it’s not going to… But, it could ask you stuff. Yes, surveys can ask you stuff. Also, the link can be an automatic download. Definitely phishing. I’m really confident, phishing or not really legitimate.

Plusnet… Shit, what’s Plusnet? “Current username, thanks for choosing Plusnet [protect 0:10:33] \_\_\_. \_\_\_ to download, \_\_\_, go to \_\_\_ Plusnet, \_\_\_ HTML.” Log into that… Plusnet’s not… [McAfee] doesn’t \_\_\_ Plusnet, does it? I’m not caught with what McAfee is doing. “\_\_\_[0:10:56] security, this would be uninstalled automatically for you.” That’s very rare for… (Laughter) I feel ridiculously suspicious about this, and it’s got phone numbers. \_\_\_ be fake, that’s not it. The addresses look solid, and the fact that… Yes, but there would be un-tech savvy people who will need that information to legitimately do that, and if the user account name is correct… Yes, but that could just be stolen from the email address. If it’s powered by McAfee, why wouldn’t it be on the McAfee website?

\_\_\_[0:11:59]. I’m giving this one a two, because I don’t believe it’s real. Talk more to yourself, I don’t believe… The addresses look fine. If there was a completely different product of Plusnet that required an address that was named after it, which I suppose some companies do that. The HTML downloads, HTML, it’s quite likely, but the fact it says it would uninstall it for you, I suppose is something McAfee would do. It would be nice to inform you of this, but also, something that software tends to not do. Yes, two for phishing, because it might just uninstall your antivirus and not anything else, it’s unlikely.

Adobe… “Email adobesystems.com, customer care…” \_\_\_[0:13:06]. I like the logo at the end, that’s quite a nice touch. “To view this message in another language, \_\_\_ [encrypt your password]. \_\_\_ no indication that this \_\_\_. Please visit adobe.com, go to ‘password reset’ and \_\_\_ [UK 0:13:31] to create a new…” Underscore U… The ‘K’ is not part of the address, “To create…” I can’t tell, it doesn’t look good. “To create a new password, we recommend that you also change your password on any website where you use the same user ID or password.” That’s a very sweet one. Oh, ‘any website’. So, if they get your password here, then they’ll be able to use it on anything else.

They might think, if you’re that worthy of a target. “Please be on the lookout for suspicious emails.” I love those ones, if they are really suspicious, but I am in the suspicious mind-set generally, and now especially. That line at the end is like, “Yes, thanks for telling me that, people who are about to steal my information.” “We regret any inconvenience it may cause you. \_\_\_[0:14:20] address to \_\_\_. Working aggressively to prevent these types…” Yes, not going to do that. “Schedule automatically,” no, yes. The website looks nice, but adobesystems.com, I don’t think it is that. I think it’s just adobe.com

Next one, “Facebook notification, bla, bla, bla. facebookmail.com.” That’s phishing, I’m not even going to bother with that much.

“\_\_\_[0:14:52], confirm your contact…” Hmm, yes. I think that one’s phishing.

“iOffer, no reply, iOffer.com, \_\_\_ mail.com, \_\_\_ [received] payment.” “Dear guest user, [Googlebox 0:15:12] UK has received your payment regarding item [‘History of Man’] miniseries, \_\_\_ TV, on TV.” You would know if you had bought that. I can’t know if I have bought that. Some of these rely on… “\_\_\_ status of your purchase, thank you.” I have seen emails like these from sellers of Amazon, carrying on sending you stuff like that, and they don’t look amazingly great, but they’re okay. I don’t think this is phishing, “iOffer.com, [as it is 0:15:48] shown…” Do you know what? I think this is legitimate. Oh my God, if it’s not, tough. If I ordered something like that, then this would be completely fine.

“Mail to business.co.uk, \_\_\_[0:16:08] blocked.” Oh, joy. Is that even HSBC’s logo? “\_\_\_ business account with us has been blocked for receiving payments.” Which business account? I’m [wondering] what? Who am I? You aren’t telling me anything about me, you’re just sending a very standard email. “\_\_\_[0:16:27] [error] logins were detected by our system security. Click here to begin to resolve the issues, customer business unit.” Yes, they’re spelling ‘errors’… It looks unprofessional. Yes, this ‘\_\_\_[0:16:55] error logins’, that logo looks a bit shabby. It doesn’t look a proper \_\_\_ logo, which they would have, and they don’t tell you your name or a bit of your account number, which, yes, can be phished otherwise, but definitely phishing.

“[soc, directgov 0:17:10].” Oh, no. That’s not what… No, \_\_\_, ‘Student Loans Company’ would be ‘@directgov.co.uk’, not ‘directgov@soc’, and even if SOC’s the website, Direct Gov wouldn’t be the one sending you it, so no, that’s not right.

\_\_\_[0:17:30] [season], \_\_\_. This person’s been receiving a lot of phishing emails recently. “\_\_\_ is good, you know, with [students]. Find your updated database… To allow us your database, [fill out]…” You’ve already got all of my information. You literally have me by the tail. Like, my… I don’t know what the expression is. There is no more information that person could legitimately be expected to give if there were fraudulent activities. Oh, ‘\_\_\_[0:17:59].com’. Okay, you had my at ‘directgov@associate’, but that just… It’s, okay, got it, that’s phishing.

[support@[visa].com](mailto:support@[visa].com) from Barclays online. Oh, you don’t say? Oh, ho, ho. “[Your] Barclays account \_\_\_. We have detected unusual activity on your accounts. Maybe because of [logging in], bla, bla, bla. \_\_\_[0:18:19] [profile validation], \_\_\_ [link].” Hmm, hmm, hmm… That one looks very professional, as opposed to the other one. The logo’s still a bit ‘blergh’ but that might just be a case of the print screening. “\_\_\_[0:18:39] [convenience]. Dear Barclays account holder…” It’s the fact it doesn’t give you your name, that it would tell you a little bit more. Also, the ‘visa.com’, definitely phishing.

Dropbox, ‘noreply@dropbox.com’, that’s legit. “Please verify your email address, \_\_\_[0:18:54].” Yes, that’s legit. Just checking the lettering. Yes, that’s legit. Also, I think I’ve seen it before.

‘prioritypostalservice@421.com’, eh? Oh, please tell me more for when getting the wrong colours for FedEx. It’s not purple. Okay, “Your parcel’s arrived, our \_\_\_[0:19:22] was unable to deliver the parcel to you \_\_\_ and shall \_\_\_ the receipt.” No, you just need to go to the nearest Post Office with your information. You don’t need to get a postal receipt, with, like, your address, so… If you then wanted something on top of the fact that the address is wrong, and the tracking number is a phone number. Why would the tracking number have brackets? No.

Now it’s \_\_\_[0:19:47].com (Laughter) Definitely phishing. Online, accounts also don’t expire. Oh, it’s the mobile banking time. Well, if only ‘digital’ gets capitalised… No, yes.

\_\_\_[0:20:07] [rewriting]… No, that would be from Amazon. Wait a minute, relax. “Waiting on delivery today, \_\_\_. This completes your order.” No, it would be from amazon.com. Yes, but I can’t see the address. Ah ha… [Check it 0:20:40]. I feel like the ‘Helen Jones’ is added after the ‘hello’ and not written as part of it, or it’s slapped on the standard email confirmation, which looks completely legit otherwise. [Stupidly] there, it’s \_\_\_. I don’t understand. “Your order was delivered, paid via cheque.” It’s not asking for anything but it looks fake, because of the colour created, I can’t see the email address. Also, why is [Carla Craig 0:21:19] sending me that? It’s all by [Trenta], it should either be from Amazon or Trenta. Hmm, I thought it must be [from], though… “We shipped your item, and this completes your order…” No, it’s phishing. I don’t know what it’s phishing for, but it’s not legit.

“[Granada 0:21:46], \_\_\_. Oh, this is a different address. “Your password will expire in three days, click…” Passwords don’t expire, passwords definitely don’t expire on any website, upgrade webmail… Unless it’s, like, an \_\_\_[0:22:06]. Too late, phishing.

‘HR recruitment’, ‘hrdep@yahoo.com’. What company are you..? Oh my God, “Please click here to download application from your search click date, and, for your interest, my name is Adam French. The job we offer are full-time and part-time positions. The job we offer is a full-time…” Hmm, of course it’s perfect. It’s the best job you could have, even if it’s full-time or part-time, just read and whatever words look good to you, you’ll click on that. “\_\_\_[0:22:41], please \_\_\_, the application \_\_\_.” Yes, sorry Mr French, you’re definitely phishing. “Double click the application. If you have any other queries, do not hesitate… Looking forward to seeing you soon.” So am I, never. The email address is wrong. The email address, the click bait, the grammar mistakes, and the fact that it looks too good to be true, and no name. It’s what job? For what job?

“eBay invoice notification,” I don’t shop on eBay. I don’t know what they look like. ‘billing@ebay.co.uk’ looks legit. Then, this message… “Your registered name is [crucial 0:23:26] \_\_\_ from eBay.” That is, like, both ways. I mean, if you have your name in the bloody email address… No, it looks too legit from the beginning, with the right email address, and that’s not the email address, and that’s just, like, the title. [It would 0:23:45] also be in brackets afterwards. “This is automated, do not reply. Invoice number, eBay invoice is available to view. \_\_\_[0:23:54], \_\_\_ PayPal. To view your invoice, go to ebay.co.uk, click on ‘My eBay’. It’s very small font, so I can’t tell if that’s before the email address. It looks fine. “\_\_\_[0:24:06].” [Poof], it’s fake. I can’t see anything. Right, yes, it feels legit. There’s nothing wrong with it.

‘paypal@epaypal.co.uk’, on the other hand, does not look legit. “Transaction \_\_\_[0:24:23] the only version at epaypal.co.uk.” It could… I mean, some websites, they do that. The email addresses have changed since I was young. Why do you want to? Because I’m fine, from the previous one, to think that PayPal is legit, because I don’t know PayPal, that’s why. [Is that 0:24:48] the logo, the coloury dash and another coloury dash? “Hello from PayPal, log on to see your monthly activity and recent transactions. Primary email address,” obviously, the one that you’re sending something to, that’s not hard to get, “Log in now. \_\_\_[0:25:03] address, by your first and last name,” again, not really hard to do if there a person there getting two sorts of email addresses.

“Type PayPal into your browser and log in that way.” That’s legit. I feel like this a lot more legit, but I’m not sure about… It looks very nice. “\_\_\_[0:25:30] [download the free app.” It’s the ‘download the free app’… Yes, but it looks completely legit, apart from the PayPal email address, which is likely to \_\_\_, because it looks legit, and why would it be [paypal@epaypal.com](mailto:paypal@epaypal.com)? Wouldn’t it be, like, information, bla, bla, bla, anything else? Well, damn, crap. It’s not asking anything from you, “Log in now.”

It’s telling you that thing, make sure that you connect, but nobody’s going to look at that. I mean, that’s… I’m going to give it a two, because I’m not sure it’s phishing, I’m not sure it’s legit. I’m more sure it’s legit than phishing. I’d click on that immediately. Yes, but the email’s quite good at classifying [if they’re good 0:26:38]. Right, I’m giving it a four. It’s more likely legitimate than not, but I’m not convinced either way.

iOffer again, how are you doing? I missed you. (Laughter) Oh, this one I did purchase. See, I told you that one looked legit. “Click below to pay, click below to pay, click below to pay…” What’s that all about? I can’t tell because of the missing images, that Gmail would cancel images from unknown sources. Well, why on Earth would you Facebook or tweet about it? You’ve purchased it, it’s an invoice, “Made a mistake, click here to cancel.” It’s not asking for anything else, it just looks like a poorly made email. It’s not asking anything out of you. Yes, “An invoice with payment and shipping instructions shortly…”

Umm… If you’ve buying more than one, why would that be the subject? Oh, this one pains the hell out of me. Oh sorry, no, ‘gogglebox.uk’. Why are you goggling? Because you’re watching stuff, I guess. How can an email looking this shit feel legit? Okay, do it again, from the start: The email address looks fine, I guess. I just [generally 0:28:28] think it looks bad, because I don’t know much about it. “You’ve purchased an item,” why would it say ‘congratulations’?

It could just be that they’re translating from a different language and the seller’s not based in the UK, so they say something like that, and that’s completely fine. The seller, invoice sent. I bought from Hong Kong, that’s something they would say. It wouldn’t make much sense, it’s not asking anything. “Click below to pay.” I don’t know, I’m giving it a five. I don’t see anything that it’s asking to phish. It’s saying there will be another one. Okay, then okay, this looks \_\_\_[0:29:14] competently made, but it [works fine].

“Don’t reply, [accounts@google.com](mailto:accounts@google.com).” Hmm, likely. Google… Why would they give you attachments? Ah, because it’s an [old email 0:29:29], and they’re the ones at the top of the email… Ah, bless. This is ancient. “Hi, someone recently tried to use an application to sign into your Google account. We prevented a sign-in in case… If you do not recognise \_\_\_[0:29:45] you should sign into your account and change your password.” This is \_\_\_, having… Yes, that looks legit. It just looks old. Ah, that last line: “If this isn’t your Google account, click here to disconnect.” Oh, no, that’s fine, that’s fine.

Yes, I’ve gotten many of these, and I can see at the bottom that you can just get a quick search, the attachments are fine, it looks legit. Wait a minute… Ah, why has it sent to Helen Jones at Lancaster? Why is it [saying 0:30:22] it’s a Lancaster account? Would it be? Where do I get sent my emails, to the main address here? It’s okay, you could just set it up, which is a bad idea to do, but you can. It’s from Italy. You could just look at the location. Oh, yes, it’s all legitimate, yes. You usually don’t have to take any actions, [but fine 0:30:46].

[‘nosextra.com’], “Create a password to this person and…” That’s fine. “[You] \_\_\_ an email address to change the password, and the \_\_\_, change the password…” What? “Please proceed to this link. This action was requested from an IP address within the network. Find out more about this [address] here,” it’s in the network. It’s in your network, it’s in your private network. It’s a 192 address, that’s standard 192, as you say. The link is [bulky as blergh 0:31:28], but it’s likely, because some people are… “You or someone else entered this email address, shared a password of a [Nos Extra] account.”

You’d have an account, account name and a password, but you would have an email address that’s attached to that, and it might not be your Gmail, but it might be your Gmail, but you wouldn’t say that you entered this email address. It would automatically be sent to that email address. There are some websites where you have to enter a new email address, but it’s the whole “action was requested from the IP address” that’s pushing it. I think it’s phishing, “All about the email address.” No, it would be something else. It would be \_\_\_[0:32:20] that would give you that, but that’s only because I know. No, it’s phishing.

“servicepaypal@... Approximating [DS, 100 and making music].” Yes, tell me more, what you want from me. “You sent a payment…” Ah, it’s making you fearful, you’ve wasted money. Mmmhmm, mmmhmm, so you’ve sent the payment. ‘From’ is the name, ‘servicepaypal’, that could be any name that you could add, but it’s actually from the guy. It’s repeated in the email text, so it looks legit. Why has it got eBay and PayPal? Oh, because it’s from PayPal, [supposedly 0:33:10]. “Seller keeps \_\_\_ address. [Victor] \_\_\_ [the black watch].” Oh, it sounds like a legitimate thing you might buy. I’m assuming that I’m expecting this emails. [Why would] the transaction [maybe] have a link as well?

Are you..? No, PayPal would not tell you who you’re sending this to, definitely not their email address. Maybe the company, but that’s what PayPal is there to… It’s phishing. It looks nice, and legit, and likely, if you have bought that, but it’s too much into the phishing thing. It wouldn’t tell you the address, it wouldn’t use that address. It’s [not 0:33:54] included in the main body to make it look likely. Yes, I don’t believe it. Oh, the shipping address, ‘unconfirmed’. It’s got the correct shipping address. Oh, it’s crap. Is there a comma between those two email addresses? No, no, it’s phishing, but it’s a very nice sort of phishing.

[battle.com 0:34:22]… battle.net, blergh. Finally, my expertise coming into play. It’s battle.net, not battle.com. “Greetings, you’re trying to sell your personal [Tableau] account.” Ah, that’s so sweet, making, like, a \_\_\_, [they’re 0:34:40] going mad. “[As you’re aware], this conflicts with the terms of agreement.” It does, you’re not allowed to. “If this proves to be true, \_\_\_. It will be on-going for further investigation.” It will be on-going? Yes, your account. “By Blizzard Entertainment employees.” One, it wouldn’t be from Blizzard Entertainment, the ‘from’. It wouldn’t be from that, it would be from [the 0:35:06] security setting.

It wouldn’t be an investigation from the employees, it would be an investigation from just [‘under investigation’], it wouldn’t say ‘employees’. “If you wish to not get your account suspended, you should immediately…” I know how serious these emails get. That’s not \_\_\_. “Please open this connection, [usbattle.com 0:35:23] login. The ‘battle.net’, they kept the ‘battle.net’. Why is there \_\_\_ so much in the \_\_\_ Tableau free account? No, and why is the redirect..? “This has been redirected to you, battle.net. If you account \_\_\_[0:35:40], please open this connection. We’ll send this package of dynamic battle.net \_\_\_ to you in the form of email.”

What? Right, one, they wouldn’t find out that you were trying to sell it, because you’d never do it in any way that they could find out, and even if you’re chatting, they can’t monitor the chat, so they wouldn’t know that you’re trying to sell it. “If you don’t submit your information, we have the right to freeze your account. We must work together to \_\_\_[0:36:13]” the email address is way too long. The email looks wrong, maybe they were battle.com a while ago, but they weren’t… Definitely not when Diablo III came out, yes. Definitely phishing.

Gary Cooper, House of \_\_\_[0:36:31]… Be in the name? \_\_\_ [CI], what the fuck’s CI? That’s not a country. The fact that it says, “Sincerely, Gary Cooper, [gary@outlook.italia](mailto:gary@outlook.italia).” Also, that’s amazing to get that email address. That’s, like, impressive. It’s not the email address it’s being sent from. “Hello, you were born there. I’m a medical institution and I’m writing to you. I’m suffering from…” Ah, how the fuck do you know me? Ah, ah no. “I have no heir apparent.” (Laughter) Who am I to you? This one is a lovely email, but actually, it’s taking a long time to talk to you and get you to do stuff. I’ve only heard stories about… “Gucci, Cartier, Rolex…” Yes, yes. I mean, that’s, like, the email is nothing, ‘from’ is nothing, the address is nothing, “Yahoo and Gmail user, click here.” It’s… What the fuck? They’ve put no effort into this. Somebody \_\_\_[0:37:40], no effort into it. Good day. I’m so sorry, you’re going to transcribe all this.

‘team@blackpoolpleasurebeach’, [‘aspectmr.co.uk’ 0:37:52]. Blackpool Pleasure Beach, yes, it is called that. “Dear Blackpool Pleasure Beach visitor, regarding Blackpool Pleasure Beach visitor survey, thank you for visiting…” Then why don’t you put that in the subject? “We hope you enjoyed your day here, we want to find out more about your views, information, it will enable us to [improve 0:38:11] our facilities. We would be very grateful if you could spend a few minutes completing the questions. ‘aspectmr…’ It’s not \_\_\_ survey login. Now, Blackpool would send you the email, and then it would end up at a survey website. That might be a survey lookalike, but it’s sent from the survey lookalike, not from Blackpool Beach. Ah, the little number at the bottom for no good reason, just to look professional. Phishing.

Dear God, did I put any as legit? Yes, I think I did. Oh, DVLA, [‘dft.co.uk’ 0:38:49]. What’s DFT? What’s DVLA? Department of Vehicular Legislation Authority? Oh my God, is it that? I actually don’t know. DFT, Department of Federal Transport? It’s on a Gov UK website. “I’m required to verify the driver’s licence details.” What can you get off a driver’ licence? Home address. Why would it get sent off a Gov UK website? Why did it get sent off .co.uk? It’s very nice, very unlikely that they would do this by email and not by post, but then that’s phishing as well. ‘Inconveniences’, oh, ‘inconveniences’, that’s not how you spell ‘inconvenience’. ‘Convenience’… He is phishing. I don’t know what for, but it’s phishing. It’s just very neatly wrapped up.

[Malcolm Lancaster 0:39:59] \_\_\_. Maybe I’m taking too long, maybe I should be doing it faster? I’d be giving it two if I was doing it faster. No, it’s phishing. ‘lancaster.ac.uk’, “Student, I hope you’ve enjoyed…” I don’t know you, Malcolm, are sending me this. \_\_\_[0:40:13] SurveyMonkey.com, that’s likely. \_\_\_ [open]. Yes, that’s likely. That’s very nice.

**P340**

P340: So, it’s from Security, Verified by Visa. The subject is that the card has been suspended, and it’s addressed specifically to an email address.

It’s addressed to ‘Dear valued customer’ rather than to a specific name, which probably isn’t a good sign. The reason for the error isn’t certain, which, you would hope they would know the error.

They want to update information, so they do want particular information from you. So, I think that is definitely phishing, mainly because there’s no name addressed to, and they don’t know the reason for the error.

So, this is from Barclay’s online: [support@thenet.com](mailto:support@thenet.com). The subject is ‘Important Account Information’. Again, it doesn’t say the name of the account holder. It just says ‘Barclays account holder’. ‘We’ve detected unusual activity’.

[Pause 0:01:36 – 0:01:46]

They’ve put a name who it’s from, which would imply that you could, maybe, check whether he is actually the manager of Barclays.

[Pause 0:01:56 – 0:02:14]

I think it’s quite similar to the previous one, so I’d say it is probably phishing as well.

From Nat West. The email address looks quite legitimate. It’s not got a name it’s addressed to, but it says ‘Your latest statement for ding 801’, which would imply that they know the account information, which would suggest it’s probably more likely to be legitimate.

‘If you need more help in sending a statement, visit our statement area’. And that’s a legitimate website: Natwest.com. So I doubt that would take you to a dodgy website.

It has contact information, and so its calls may be recorded, which is likely to indicate that you can contact them. So I’d say that’s definitely a legitimate one.

So this is from eBbay. The ‘from’ email address looks fairly legitimate, apart from it says ‘admin@ebayz’, which, I’m not quite why there’s a Z there.

Again, it’s not emailed to a name, it’s just to a member. It’s been suspended due to concerns.

[Pause 0:04:06 – 0:04:20]

It’s asking you to take a few minutes to update personal records. And it’s from the safe harbour department, eBay Inc. So it’s not from a specific person, which makes me think it’s less legitimate. It’s from a department as a whole.

There’s no contact details of who to contact, if you’re concerned about anything, although there is a ‘Need Help’ tab. So, I think this one could be phishing, but I’m not too sure about that one.

So, this one is from Sean Granata \_\_\_[0 :05:13]. It says, ‘Your password, it’ll expire in three days. Click here to validate your email. Bank System Administrator’.

I’m not sure about this one, because it could be a university email, and the password does expire on those kind of things. However, the email doesn’t look very secure.

So, I’m not sure about this one. Again, there’s no addressed name, or name signing it off, so I’d say it could be a phishing one, but I’m not too sure.

So, this is from Facebook Mail. It’s addressed to a name, to Helen, which would imply they know who you are, which is probably, they’ve got that information, which is maybe, a sign that it’s not phishing.

The link that it directs to is an official Facebook page, by the looks of it, although it says, ‘If the link doesn’t work, try copying and pasting it’, which, I’m not sure why it wouldn’t work.

And it says, ‘If you didn’t enter this as your email, please disregard the message’, which, if they were trying to phish, they might not put something like that. So, I think that is definitely legitimate.

So, this is from iOffer, about the History Man DVD TV. It says, ‘Congratulations. You purchased an item’. It describes the item.

It says, ‘You should receive an invoice with payment and shipping instructions. Made a mistake? Click here to cancel.’

I don’t think that would be phishing, because they’re not actually asking for any personal details. However, it says, ‘You purchased an item from Gogglebox’, and the ‘from’ in the title says it’s from iOffer, which is a bit of a mismatch.

It says, ‘If you made a mistake you can click here to cancel the transaction’. So that could be where the phishing is going on, but I’m not sure. So I’ll say that is legitimate, but I couldn’t be sure about that.

So, this is from Philippe [Boucheron [0:08:16]. ‘I’m sorry for reaching you rather late, due to the situation. My family had a trip to Manila, Philippines. Everything was going fine until last night, when we got attacked by unknown gunmen. All our money, phone and credit cards were stolen. They didn’t hurt anyone \_\_\_[0:08:32] passports.

We reported the incident. The response was casual. We can come back in two weeks [for] investigations to be made. The truth is, we can’t wait until then as we’ve got a return flight.

Right now we’re strapped for cash, due to the unexpected robbery. I’m wondering if you can help with a quick loan to get us back? We need £1,850. I promise to return you, in full, as soon as I return home, hopefully, tomorrow \_\_\_[0:08:56] let me know [what] you can do’.

So this, in the context of, if these people are friends, would seem like a legitimate email. If this email was received by someone you didn’t know, then they’re obviously trying to get money from you. But if the trust is between these people, then it seems legitimate.

So, this is from Nat West. It says it’s from Nat West, but the email is: uup@\_\_\_.com 0:09:36], which doesn’t seem to match up to Nat West.

It says, ‘Your account will expire. To continue, log in to online banking. In case this process is not performed, your account will be disabled.’ And it’s from Nat West Team, which is, again, not signing off using a name, which seems less trustworthy.

It gives you a 24-hour time restriction, which seems very short to do something, as people might not have looked at their emails. So I don’t think that’s entirely legitimate.

I assume, when you click on the log in to online backing thing, perhaps they’ll somehow take your banking details from there. But I think this is a phishing one, mainly because of the email address.

So, this is from Carla Craig, and this is telling someone that their order has been shipped. It has a specific address that it’s been shipped to, and a name, and it all just looks very genuine. So I’d say that’s probably, definitely a legitimate one.

So, this is from the HR Recruitment Department. The email address looks slightly unprofessional, as it’s got, like, some numbers in, and is at Yahoo.

It says, ‘Dear Applicant’, and then says that they’ve carefully reviewed the CV, and glad to inform them that they’ve made the short list. I imagine, if they’ve reviewed the CV carefully, it would be addressed to a particular applicant.

It describes the job vaguely, and the interview. It does give a name, Adam French, and his position. However, it doesn’t explain anything about where the interview is, which is quite important information, and says that you need to download the application form to see this.

It says, ‘Contact me via email’, and you’d probably expect to be able to contact someone, regarding a job, via phone. So I’d say this is definitely a phishing one. The ‘Please download, please click here to download application form’, doesn’t look very genuine.

So, this is from PayPal. The email address looks relatively genuine. And it’s addressed to a full name, first and second name. It does, however, say that this isn’t a phishing email, because it’ll always address you by your first and last name.

It says, ‘If you’re concerned about security, do it this way instead’, and that looks like a genuine email address. So I’d say this is definitely a legitimate one.

There’s also, ‘Need help? Contact us’, and finding stores and things, so they’re trackable.

So, this is from Dropbox, [noreply@dropbox.com](mailto:noreply@dropbox.com). It’s addressed to a specific name, and it says it needs to verify email address before it can check folders. ‘You need to verify your email address by clicking the link below’, and that’s quite a common thing to do.

As long as this person had just signed up for a Dropbox account, then this would seem like a very legitimate email, I think. Although it is signed off from the Dropbox Team, I think it is legitimate.

So, this is from PayPal. The email address doesn’t look very genuine. There’s lots of numbers and it’s quite long. Although it does say in the email that that is the details of the person that the money has been sent to.

They know the shipping address, which would imply it is correct. It asks you log in to your PayPal account. There’s a section saying ‘Questions’. ‘Go to the Help Centre’, and a website, which is [www.paypal.com](http://www.paypal.com), so that seems legitimate. Yes, that one looks quite legitimate.

So, this is from Blizzard Entertainment. The email address: noreply@battle.com looks genuine. It’s quite an informal \_\_\_[0:15:25] of greetings.

It says they’re trying to sell their personal \_\_\_ account. ‘[It] conflicts with terms of agreement. The account will be disabled if this is true’.

‘If you wish not to get your accounts suspended, you should immediately verify your account ownership. Open this connection to do so’, which looks to have a lot of different symbols, and I’m not sure if that’s very genuine.

It gives three days, which seems to be quite a reasonable amount of time. It’s not rushing you into it. ‘If you had already opened a \_\_\_[0:16:17] account, please disregard this automatic notification’. Regards from that account, Admin Team. I think this is a genuine one.

So, this is from Gucci, Cartier, Rolex. The email address doesn’t seem to make much sense, in relation to what that is.

‘Yahoo and Gmail customers click here, \_\_\_[0:16:53], click here’. So there seems to be a lot of links that it wants you to click on and not a lot of explanation of why. So I think this one might be a phishing one. But then they’re not specifically asking for any information, but they might do that when you click on the link.

So, this is from NUS Extra. ‘You or someone else entered this email address to change the password of an account. To continue the password reset process, please proceed to this link, if requested from IP address’.

So, it gives you the specific IP address that this action was requested from, which is a good sign, because that could probably be checked. And the email address looks very genuine. So I think that this is legitimate. However, the link is really long, which makes me slightly cautious.

This is from HMPS Recruitment, it’s by JobAlert. It says, ‘Dear Candidate. I job which matches your criteria has been published. Please click on to the following link, or paste it into your browser, and search for the vacancy below’.

This link doesn’t look very genuine, and you would have thought, in this context, they would just send the actual job, rather than asking you to do that.

And it’s also not addressed to a particular name, and signed off from HR Recruitment. So I think that one’s phishing.

This is from eBay. It says it was addressed to a specific name, including first name and second name. There’s an invoice number.

It sends you to an address which is a legitimate website: ebay.co.uk. And there just seems to be a lot of links to specific eBay things. I’d say that’s definitely legitimate.

So, this is from Plusnet Support. The email address looks legitimate: [support@plus.net](mailto:support@plus.net). It’s addressed to Miss second name, which is a good sign.

There’s an account user name, which the receiver of the email would be able to cross-reference, if they have that user name.

It tells you what to do to get the software running. There’s also a help assistant for Plusnet, which you can use. And there’s also a number which you can call. Obviously, this number might not be a real number, but I think, in this case, it is. And there’s also specific pages that directs you for help, so I think that one’s definitely legitimate.

So, this is from HSBC. That logo, I don’t think, is HSBC’s actual logo, and it doesn’t address a name, which isn’t a good sign.

It just says ‘from the Customer Business Unit’. It doesn’t give you any numbers to call, or any help websites, or anything.

It just says, ‘Please click here to begin to resolve the issues’, but it doesn’t explain how this will be resolved. So, I think this is definitely phishing, mainly because I don’t think that is HSBC’s logo.

So, this is from [frank@easyroommate.com](mailto:frank@easyroommate.com). It’s addressed to a first name. It tells you to beware of scams. The website address looks fairly legitimate. I’m not sure why they wouldn’t just send it, the message online, [though [0:21:51], why you have to click a separate link.

The text is all different colours, which isn’t very professional. I’m not really sure about this one. I think it might be legitimate, I mean, because they’ve addressed it to a name, and the email address looks legitimate, but I’m not sure.

This is from iOffer. The email address looks legitimate: ioffer.com. It says, ‘Dear guest user’, so it’s not addressing the recipient directly. ‘Gogglebox has received your payment regarding the item. Click below to view the status of your purchase. Thank you, iOffer’.

I don’t know why they wouldn’t just tell you the status of the purchase in the email. So that seems slightly strange, but the link looks fairly legitimate. However, I find it strange that they haven’t addressed the person by their first name. I think this could be a phishing one, but I’m not 100% sure.

This is from Adobe Customer Care. The email looks legitimate: @mail.adobesystems.com.

‘To view this in another language, click here’. So, if you wanted to read another language, you would have to redirect. However, if not, then you wouldn’t.

[Pause 0:23:21 – 0:23:31]

It asks you to visit a website to prevent unauthorised access to your account, and to create a new password. The website it lists is a genuine website, I think: [www.adobe.com/passwordreset](http://www.adobe.com/passwordreset).

It says, ‘You can visit a customer alert page, which you’ll find here’, which, again, is another redirection. So there’s three ways that it’s trying to redirect you. But I think it is legitimate because of the genuine websites.

So, this is from Caxton FX Cards. The email address all looks fairly legitimate. It’s addressed to a recipient with first and second name.

It says, ‘Changes to the terms and conditions’, and you can click there. It gives you an email address to reply to, and it also gives you a phone number and an address. So I’d say this is legitimate.

This is from: directgov@slc. So it’s a message for students receiving grants and loans [from 0:25:00] a student loan.

It’s saying there’s fraudulent activity. ‘To allow us to update our database, [fill out] information. To do this, paste this into your browser’. The website doesn’t seem relevant to what the email’s apparently about, so that doesn’t seem very professional.

And it’s just signed off ‘Student Financing’ and not providing any information to contact people, which you would have thought they would do, regarding the concerns that people might have about losing their grants. So I’d say this is definitely a phishing one.

So, this is from: [studentfinance@directgov.co.uk](mailto:studentfinance@directgov.co.uk), which looks like a really genuine address. There’s also a logo at the top of the page, which is, as far as I’m aware, is the right logo.

‘We require students to update their account information, due to a recent update. To update your account, please validate here’. It seems more genuine than the previous one.

‘Fill it out exactly as you filled it out when you were signing up for finance, or the payment will be suspended because of failed verification’.

It says it doesn’t incoming emails, and there isn’t anyone to contact still. It looks slightly more professional, because of the logo and the address, but I’d still say it could be a phishing one, mainly because there’s no contact details.

So, this is from TNS, on behalf of Dell. The email address doesn’t look very genuine. It’s got a lot of symbols and numbers.

It says, ‘Dear valued customer’, rather than a specific name. There is a logo, which is a good sign. There’s a specific case number. So, if people didn’t have a Dell laptop, or didn’t have a case number, they’d instantly know it was phishing. So I think a case number’s a good sign.

It’s asking for you to complete a survey, and they’re just asking for feedback. I think this might be a genuine one, mainly because of the case number, but I’m not sure.

So, this is from Priority Mail Postal Service. The email doesn’t look very legitimate. It’s just some letters and numbers that don’t seem relevant.

There’s an order number, and it tells you specifically when you’d ordered it. So if you knew you’d ordered something at that time, then you’d be knowing it was real or legitimate.

‘To receive the parcel, go to the nearest office and show this receipt’. I think this might be legitimate because, if not, then there’d be a lot of people going to the office and showing false receipts, which are quite easy to track. So I think it’s legitimate.

This is from: noreply@accountsgoogle. There’s a suspicious sign in. So it’s addressed to the first name. And it’s saying that someone tried to sign into the Google account. Prevented the attempt. And it tells you how they tried to log in.

It’s saying, ‘Someone else might be trying to use your account. Reset your password immediately’.

It then gives you a link to ‘Troubleshooting Steps’, listed at, and then there’s a genuine [looking/log in 0:29:02] website address.

I think this is definitely legitimate, because it’s addressed to the right person, and the reset password link is quite small, so it’s not, it doesn’t look too in your face, like, that’s all they want.

So, this is from Gary \_\_\_, and it’s about confidence. So, it’s saying who he is, and he’s in a medical institution, where he’s writing, suffering from a medical condition.

‘I’d like to leave my good fortune to you. I have no heir. Could you contact me with your full name and phone number, to complete the procedure’.

This is definitely phishing, I think. [If we 0:30:05] don’t know the person, and it just seems - and they don’t know the person because they’re introducing themselves. So it just doesn’t seem very genuine, someone wanting to give them all their money.

So, this is from: thanks@virginmobile. It’s not addressed to a particular person.

It says, ‘Head over to our website to send us an email’, which doesn’t seem very legitimate. Why don’t they just attach their email address on there?

They’re saying the balance will be taken on or after a certain date. I think this might be a phishing one.

This is from: service@paypal. It’s saying, ‘Your card’s about to expire’. It’s addressed to a first and second name.

It says that, ‘Your account ending 1234 is about to expire’. Seen as it gives the account number, that’s a good sign.

There’s a link to update your card. It’s not signed off from a particular person. There is the official logo though. And if it’s got the, it’s got the card number, I’d say that was a good sign. So it’s probably legitimate.

This is from ‘The Team at Blackpool Pleasure Beach’.

It says, ‘Thanks for visiting Blackpool Pleasure Beach’. They want you to complete a survey, and sends you to a survey link.

[Pause 0:32:02 – 0:32:12]

And it depends very much what’s on the link. I think this could be genuine, but it’s quite difficult to tell.

This is from DVLA: info@DFT. So there’s the official, I think it’s the official DVLA logo.

‘We require driver licence details’, which seems like an odd thing to request. They have a system of that.

It asks you to fill in the link below, which is: DFT.gov.uk. So .gov.uk seems legitimate, but I’m not sure what DFT is.

‘And drivers who refuse to do this will lose their licence and will have to take a fresh test’. That doesn’t seem very legitimate, as people might not respond to emails, and that could just be how it is.

There’s an address to reply to. However, that could be made up. I’m fairly sure this is phishing, just because the subject matter doesn’t seem legitimate.

This is from: [malcolm@lancaster.uc.uk](mailto:malcolm@lancaster.uc.uk). So, lancaster.uc.uk is a genuine address.

It says, ‘Dear Student’, which they would do in a university context, as that’s just what they do when they send out lots of emails.

They’re asking you to fill in a short survey, to be entered in with a chance of winning. It’s on the on the SurveyMonkey, which is widely used. So that seems okay.

It gives you an end date, which, if they were just desperate for you to do it, they probably wouldn’t do. There’s also an email address to contact, which is another Lancaster address, which is good. So this is definitely legitimate.

**P341**

P341: I think the first one was a PayPal email. Think it’s legitimate because I usually trust PayPal emails. And it’s only asked you to review your recent transactions so it’s not asking you to say anything. So I would probably say definitely legitimate on the first email.

Check out a job, which month your \_\_\_[0:00:48] has been published on our website. Please give \_\_\_ and search for them.

[Period of silence 0:00:55 – 0:01:18]

I don’t know this one because you’re confused now because I the Lancaster University on top, but I’ll put one to six. I will put three, four just for the fact that I usually write down what I put online to have job alerts to come to my email. So I know which website it was. If there is a website that I don’t know, I'm not going to avoid it.

But in this case, if it’s Lancaster University then I’ll perform… Oh dear.

[Period of silence 0:02:20 – 0:02:53]

So Lancaster University logo is everywhere. Sorry. I didn’t know that.

[Period of silence 0:03:00 – 0:03:12]

I personally have problems with Dell because my previous computer was Dell and I really didn’t like the customer service I was getting. After I called them once, I was getting weird like calls and emails. So I don’t know if this will affect it. But I probably would check it out. If I didn’t have any case with them, I’ll probably call them up and ask them, but in this way, I'm just going to put two.

[Period of silence 0:03:59 – 0:04:10]

This is harder than I thought. Thank you for your interest in our new role. We have opened our \_\_\_ to let you know we have \_\_\_.

[Period of silence 0:04:26 – 0:05:05]

No, we’ll say on this one, which is hire employment department, HR dept 33433 yahoo.com.uk about a job application. I'm going to say definitely phishing. By the fact that, if you have applied for a company or for a job, they're not going to send you an email from a yahoo, I think. Sorry, I wouldn’t trust it.

[Period of silence 0:05:46 – 0:05:56]

Greetings.

[Period of silence 0:05:58 – 0:06:39]

Okay, I guess the next email is from an online game, which I heard of it, but never played it. This is Diablo III.

[Period of silence 0:06:57 – 0:07:22]

So I'm not sure. It shows that… It seems to be legitimate. I mean it comes to the person, who received that email is so… If I actually tried to sell my personal Diablo accounts and I received that email after my attempt, then I will say it is legitimate. But I haven’t heard of that battle.com before. So I’ll put a four or five because I'm not sure. So I'm going to put four.

\_\_\_[0:08:09]

[Period of silence 0:08:10 – 0:08:44]

I have a PayPal account for a long time now and never received an email saying that my Visa, my card is about to expire, but probably put definitely phishing because, if it’s something then I just go to the official website PayPal and do it, but I wouldn’t click on there, update card from the email.

So anything that has to do with a card, I'm just going to go to the official website and I’ll check it out and not in from email. I just don’t like the fact that I need to put all those personal information about my card expired and security code, just by clicking from the email.

[Period of silence 0:09:45 – 0:10:06]

I’ll probably… On the next one, which is the iOffer. I received your payment regarding \_\_\_. I don’t know the website. I’ve never heard of it. Sorry.

[Period of silence 0:10:26 – 0:10:50]

I'm not sure because… I think it’s okay. I mean, if I did actually have anything to do with iOffer company and actually did this kind of purchase, I would have clicked it, but if not, I’ll know that it’s phishing, but in this case, when I don’t know, I think the email looks legitimate, so I’ll put… I'm not sure. I'm not 100% sure, so I'm just going to put five.

[Period of silence 0:11:34 – 0:12:00]

No, but the student [bweb save the season] from the Student Loan Company. I really don’t trust working with emails. So I don’t trust an email so easily. So, in this case, I will say definitely phishing. Well, it looks, how do you say? No, I just… Something doesn’t look quite okay.

If it was something like that, I think a phone call would have resolved this, or I just find that, when you have applications to receive grants and loans previously they called me if there was something, an issue or send me in a letter, not through email and ask me to update my information through just clicking. So I would say definitely phishing.

[Period of silence 0:13:15 – 0:13:45]

This is again another email from iOffer about this DVD purchase. You just purchased an item from Google box and it’s talking about a re-invoice with payment and send me instructions shortly. As I said before, if I, assuming that I did this purchase and I received that email that I will find it legitimate. If not, I would say definitely phishing, but in this case, it’s all right. I don’t find something not legitimate. So I’ll put four.

This is \_\_\_[0:14:44] HSBC emails from the business account with us have been blocked for receiving payments and error logging was detached by security system, this account will be disabled if you acknowledge measures. Please proceed to begin to resolve this.

No, when it has to do with banks, I prefer letters or calls. So if there is an error with logging, I wouldn’t do it through online. I don’t know the email, so I will compare the emails that I have received from my HSBC before and see if I recognise this HSBC business.co.uk, but I don’t know if they actually emailed this, their emails is like that. No, I think a letter or a phone call would be more appropriate than ask me through an email. So I'm not sure. I'm just going to put definitely phishing. I wouldn’t reply or do further action.

[Period of silence 0:16:05 – 0:16:17]

This is the NUS Extra.

[Period of silence 0:16:20 – 0:16:33]

I’ll say definitely legitimate on this one because I don’t know. It again comes to the fact that if you have a change, if you have recently tried to change an email address or password and you receive this email, usually click on it. So, if not, I would have ignored it. But just by the look of it, it gives an IP address. You can check it out. That doesn’t mean anything. I don’t know. I would say legitimate. I’m more cautious when it has to do with bank details.

So Visa, dear valued customer, your credit card has been suspended as an error was detected in your credit card information. The reason for that is not certain, but for security reasons, we have suspended your credit card temporarily and we need to update your system for further use of this credit card. No. I’ll say definitely phishing. I just told you, I don’t do emails with… No. Yes. I say definitely phishing.

So the next email is fill in, you fill a \_\_\_[0:18:29]. I can't pronounce this. Sorry. So I'm sorry for reaching you rather too late due to the situational things in our family and \_\_\_[0:18:38].

[Period of silence 0:18:39 – 0:19:08]

Such a lot of money, 1,000, almost 1,000 quid. I promise to refund you in full as soon as I \_\_\_. I say definitely phishing. If I knew the person, I would have called. If I don’t know the person, I wouldn’t reply so it’s definitely phishing.

[Period of silence 0:19:38 – 0:19:57]

I’ll say definitely legitimate. I mean I have been to this website before and they send emails like that. So I’d say five, not six, you know. I know. So I would have probably clicked it.

[Period of silence 0:20:13 – 0:20:31] I’ve never seen this notification. I've seen facebookmail.com. I usually have… No. No, definitely phishing. I just don’t recognise the email. The email looks a little bit odd. It might not be, but I've never seen this email from Facebook. This notification plus facebookmail.com. It’s just the email shows it’s weird.

So I say it’s a two, not one. Definitely phishing because it’s just the email that I find it now with the rest of the emails, it’s okay, I think.

So this is an eBay invoice notification. \_\_\_[0:21:33] payment method.

[Period of silence 0:21:33 – 0:21:51]

It looks legit, this email. I mean the email is sent from, it looks okay and they only ask you to… It’s a receipt and they only ask you to check… It doesn’t ask you to do anything, does it? \_\_\_[0:22:20 – 0:22:28].

It looks legit. It doesn’t ask you. It’s like an invoice email, like a receipt. eBay’s money has been paid out. So I’d say definitely legit, six.

This is another eBay suspension email. We regret to inform you your eBay account has been suspended due to concerns we have with the safety \_\_\_[0:22:53] eBay community. The user agreement section \_\_\_ immediately to avoid \_\_\_.

[Period of silence 0:23:00 – 0:23:55]

Well, I say, it looks like phishing because I mean, again from the email that it’s been sent from, it bothers me that there's a \_\_\_[0:24:13] ebayz.com. The ebayz.com, it just feels, it is a bit odd for me. And I think I've came across those emails asking you, telling you that your eBay account has been suspended, but they never ask you to update your eBay records for some reason. No, they don’t ask you to do that. So I say I'm between one and two. I’d say one, definitely phishing.

[Period of silence 0:24:50 – 0:25:02]

So this email is Plusnet support. This is now ready to \_\_\_.

[Period of silence 0:25:11 – 0:25:20]

I never heard this McAfee, but this is not a \_\_\_ download. Plusnet Protect. I've never heard of this type of software. It’s an antivirus, I guess, but I never heard this Plusnet support. So it depends, actually. I'm not sure so I’ll be between three and four. But I’ll say three.

[Period of silence 0:26:14 – 0:26:36]

I don’t know. I’ll say three.

Dropbox needs to verify your email address before you \_\_\_[0:26:48]. Please verify your email address by clicking the link box. I say five. I think it’s legit. I don’t know what is a Dropbox. I never came across it. So the email looks okay. Like it doesn’t seem something noreplydropbox.com.

\_\_\_[0:27:23] with Dropbox and the bottom in the right is a 2012 Dropbox and so I think it’s okay. I think it’s legit so definitely legit.

No, this Yahoo and Gmail user, click here, click there, give your loved one a luxury watch today. Good luck, click here. That’s definitely phishing. The password looks very, how do you say? It just doesn’t look legit, the email address, as we said. And no. Phishing.

You sent a payment off to Keith. This is another PayPal email and for \_\_\_[0:28:30] and it’s telling you that you sent a payment of 150 quid to Keith White.

[Period of silence 0:28:40 – 0:29:34]

The email by itself looks okay. I could have said legit. It’s just the email from \_\_\_[0:29:43] paypal.com and there is another email, saying that approximating, it just, it confuses me, that. But I don’t know if that means, like it doesn’t ask you to do something. No, I think it’s legit. I mean, it has all your information up there. It says about the \_\_\_[0:30:09] psychology, Lancaster University. It has every information, if you want to check it out if it’s true or not. It doesn’t ask you anything so I’ll say definitely legit.

Your late statement. Oh, I hate emails from banks through emails. Like from NatWest. So this is an email from NatWest. Your latest statement from accounting ending is waiting for you online now. Just log onto NatWest, but again, you can also set your \_\_\_[0:30:53] on your account. It seems legit. The email sent from looks okay. Yes. I’d say definitely legit. I don’t see something wrong with it.

Barclays. Dear Barclays \_\_\_[0:31:25] we have \_\_\_ in your account. This may be a cause of logging into online banking from \_\_\_ or just \_\_\_ authorised. \_\_\_. The email looks legit, but the fact that there is… I don’t see… I mean, the email sent from, which is support \_\_\_[0:31:48].com is just, I’d say definitely phishing. I guess the \_\_\_[0:31:53] been with Barclays.com.

And I wouldn’t… I don’t know, it’s just when something is wrong, we usually block your account so you have to deal with it on calling them or letters or something like that, not through emails. So I say phishing.

\_\_\_[0:32:19 – 0:32:45] I don't know. The email is okay. The email has been sent from \_\_\_[0:32:53] account for all of the information. I don’t like the fact that I have to do it online \_\_\_ the information, but I say four or five. I will say five. I don’t see something odd on that.

This is a new one from Amazon for £360.

[Period of silence 0:33:17 – 33:31]

I think it’s legit. I’d say between five and six because it’s an email from Carla Craig. It’s… No, I changed my… So it has \_\_\_[0:34:58] confirmation on there and there is… I don’t know. I don’t like the fact that there is no associated delivery tracking number on it. And it costs like almost £400. That’s a lot of money to not have a tracking number on it. And I guess you…

And it says here, “Your possible quick Y track information may not be available.” Now, I say between phishing one or two. I mean if I spend so much money and buy a TV, it would have the tracking number on it. I don’t know. Yes. I’ll say between phishing one and two.

This is an email from G. Cooper, Gary Cooper. Date and number, therefor I will kindly leave you my fortune to good use \_\_\_[0:35:16]. Oh, this is phishing, definitely phishing. I don’t know. It’s just you receive those emails once in a while and you know this is phishing. It just asks again to contact him with full name and your phone number email the copy of the procedure. This is phishing.

FedEx. Your parcel has arrived at the post office in December... No, this is phishing too because the different tax information. I mean it’s all the tracking numbers to… I don’t know. It’s just weird. And email from it’s also weird.

This is a Virgin Mobile email. \_\_\_[0:36:37] is now ready to use. I think this is legit. \_\_\_[0:36:48]. I don’t know. I don’t like that there is a… No, I don’t say legit because I don’t like the file that is no name for attachment. Why would you..? It’s usually in a PDF or something, PDF or this is an unzipped. No, I’d say between one and two. I’d say two.

Your \_\_\_[0:37:28] account will expired today on June 3 \_\_\_ using. This is definitely phishing for the fact I don’t recognise the email address isn’t NatWest. It should be something at natwest.com or something like that. So the email is just weird so I say definitely phishing.

This is an email from \_\_\_[0:38:03]. Definitely phishing. I don’t like the email that it’s being sent from. I don’t know. I mean I can't be certain. I say three because I really don’t know. If I don’t like the emails, I do click here, upgrade webmail 13. I say three.

\_\_\_[0:38:46]. This is an email from \_\_\_ information has been \_\_\_ recently discovered that an attacker \_\_\_ there has been an \_\_\_. I don’t know. The fact that it has been sent from a .customercare at \_\_\_[0:39:12] systems.com… I think it’s legit. I think that. I'm not sure. So I'm not putting a six. I'm going to put five.

[Period of silence 0:39:30 – 0:39:49] This is an email from Gmail, telling you about you need to… Someone tried to sign into your Google account. If you do not recognise \_\_\_[0:39:59]. The email that it has been sent from seems okay. So I’d say I'm not so sure, but tend to more legit so I’ll say it’s either four or five. I’d say four.

So just looking, this is an \_\_\_[0:40:38] on [fx] email. The emails are from… I don’t like the fact that it says via \_\_\_[0:40:46].co.uk. I think it’s a five. \_\_\_. It’s seems legit, but I don’t like the fact it is \_\_\_.co.uk. I say it’s a five.

And this is an email from Blackpool Pleasure Beach.

[Period of silence 0:41:26 – 0:41:58].

I think it’s a legit Blackpool email. Yes. There does seem something odd on it or any feature to tell me that it’s trying to phish you out \_\_\_[0:42:15]. That’s why I said, it’s legit.

This is an email from \_\_\_[0:42:23] verify the driver’s licence \_\_\_. Follow the link below.

[Period of silence 0:42:36 – 0:42:46]

I don’t know. I'm not happy with the… I don’t think that you lose your driver’s licence by not completing an email. I say it’s a phishing. I mean, if it’s some place are serious you need to upgrade your contact \_\_\_[0:43:18], they should have sent you a letter, not an email. So I say phishing.

Welcome to Lancashire. I hope you have enjoyed your first few weeks at university. And just to find out why you chose to… Oh, this is an email that have been received so many times. I’d say it’s legit.

**P342**

P342: Okay, so it’s a PayPal account. First of all I’d look to see who it was from. So it’s from @paypal.co.uk, so I’m pretty confident that’s okay.

It’s got all the PayPal numbers and registration and things.

It says, “Please do not reply to this email,” so if it was phishing they’d probably want you to reply to the email.

I’d probably say that was okay.

Again, this email says, the from… The from email is NUS, there is a link so you can find out about the IP address. I don’t know that they usually send links that are that long, it looks a bit suspicious, but I suppose if it was a phishing email they’d probably send something really short and succinct that wouldn’t look scary, so it’s probably legitimate.

The website inside the link matches that of the email that it’s sent from, which is usually quite legit. I’ll go for ‘definitely’, I may as well.

I’m not familiar with [iGrasp 0:03:02]. [HMP Recruitment], from HR, about a job reference. It’s about job alerts, I don’t know if anyone would be phishing about that. I suppose they might want to put a virus on your computer. The email address does match the links. It’s probably legitimate. I don’t know 100% though. I’ll go for a five.

This one is from Plus Net, it’s probably legitimate. It’s got all the phone numbers, it’s got the email reference. It’s about setting up an account on your computer. Yes, that was \_\_\_[0:04:58]. Yes, so legit.

(Laughter) The one [off] Philippe is definitely phishing. Anything off of BT Internet, or like off @Yahoo, it’s just like a personal email, isn’t it? Especially if they’re asking you for money, it will definitely be phishing.

The one off eBay, it’s from eBay.co.uk, all of these mass generated emails, invoice numbers etc., lots of personal information. I’ve had them myself. Yes, legit.

HR Recruitment Department. Umm… There is no information about the company. There is a link to click download, it wouldn’t be in a ‘click to download’, it would be in an attachment. [HRDepartment@Yahoo.co.uk](mailto:HRDepartment@Yahoo.co.uk), no. I mean, maybe it would be, maybe it would be like an official email, but it’s very un-official. I wouldn’t trust it; I’d say phishing.

Email [off] [Shaun Granyata 0:07:20]. It’s from Washington College, it’s .edu, I don’t think it’s easy to get a .edu email, but with their being no other information in there, I’d question it. Validating emails tend to just have very short messages, though, don’t they?

[Let’s see], the @Lancaster.uk email address, so yes, it makes sense that it would be a legitimate thing. I would give it a five, just in case.

(Laughter)

This is the [Diablo 3 0:09:24] account email. I’m not a gamer, I don’t really understand. I imagine if I was a gamer and someone sent me this I’d be a bit freaked out. Why are you trying to sell your Diablo 3 account? Why would you try and sell your Diablo 3 account? There isn’t any kind of official… There doesn’t seem to be any official marketing on here. I’d give it a two for the phishing, but I just don’t know.

[FedExPriorityMailPostalService@FortWayne.com](mailto:FedExPriorityMailPostalService@FortWayne.com). Tracking number. \_\_\_[0:10:29], FedEx [to you]. It doesn’t look anything like FedEx. I don’t know, I’d say it was phishing, because it just doesn’t look anything like FedEx looks, and why would FedEx email off a [DTF.193@FortWayne.com](mailto:DTF.193@FortWayne.com). I don’t even know what that means.

Yes, this PayPal looks alright. It’s from [Service@PayPal.com](mailto:Service@PayPal.com). It’s from MacKenzie Music – if you had bought something off MacKenzie Music you’d know about it, especially something that was £149. “Payment sent to… Please do not reply to this email.” That looks pretty legit, I’d say.

(Laughter) EBay suspension, “We regret to inform you that your eBay account has been suspended.” But it’s at [ebayadministration@ebayz.com](mailto:ebayadministration@ebayz.com). So, no.

“Due to the safety and integrity of the eBay company…” They would never do that. It’s not really how eBay works, is it? I don’t know. I’m confused now. Yes, no, I would say it was phishing.

“Lung cancer in the terminal phase,” phishing, [Gary Cooper]. [What are you like?] Oh, you can add him on Skype, just to like… See his face. (Laughter)

iOffer, I don’t know. It’s from ioffermail.com, no reply, ioffer.com. It’s probably legit, if you did order something off ioffer.com.

This Amazon.com email doesn’t look right at all. It’s from Carla Craig. I don’t know what- Is it asking you to do anything there? “Thank you for ordering with us… You will be informed when we ship your items to complete your order…” Shipment has no associated delivery tracking number. You’ve bought a used, ‘acceptable condition’ TV for £359, that seems crazy. I don’t know. It just doesn’t kind of look right. I mean, if it’s been forwarded from someone called Carla Craig… I don’t know, I don’t think that looks real.

No, that Barclays one is weird. [Support@bnet.com](mailto:Support@bnet.com), from Barclays. I don’t know.

[TNS 0:17:59] on behalf of Dell. I can’t even read this. “Dear valued customer… Dell customer service survey…” Let’s make it bigger. “Dell has asked TNS… A customer satisfaction research company in the IT industry to help conduct research on your experience so that it may be used for [sales] purposes, Dell \_\_\_ response to email, \_\_\_ have to contact our… \_\_\_ Dell survey will help \_\_\_[0:18:51] mail to TNS.”

It’s got the ‘to be removed from the list’ click on the thing there. It’s got lots of information. I don’t know what \_\_\_ is, I’d probably Google what [Rap2] was before completing this, I’d feel suspicious about it. But there is lots of information about Dell, so I don’t know. Again, it would be in the context of, have I just bought a computer? I’ll give it a three.

PayPal@oe.\_\_\_.co.uk. Yes, I’d give that a legit… Hmm.

Okay, I’d say that was legitimate. Maybe I’m being a mug. I don’t know.

(Laughter) [[Natwest@\_\_\_p@\_\_\_.com](mailto:Natwest@___p@___.com) 0:21:38] okay, so the NatWest one is phishing. “Your account will be disabled in 24 hours.” That doesn’t happen; no one would do that.

Okay, this is a proper NatWest one. Information.Natwest.com. Just log in. It shows the email address. I’d say that this was legit.

“The bill for your Virgin Media is ready to view.” From Virginmobile.com, the Virgin Media [team 0:22:34]… “Virgin Media is now ready to view…” They don’t [name the] attachment, why haven’t they named the attachment? Virgin Media [team] \_\_\_.com. Virgin Mobile would name their attachment, right? Phishing. But it’s from @virginmobile.com. But it’s not from VirginMedia.com. Okay, phishing.

\_\_\_ effects, Mastercard. Lots of details on there, it’s from \_\_\_.com. [Advice from Three.co.uk], I don’t know what that means. Terms and conditions.

Ohh, this Three thing has really freaked me out, I might just… Yes. [Why they’ve said 0:25:36] Three, what does that mean? Phishing.

[Studentfinance@directgov.uk](mailto:Studentfinance@directgov.uk) [don’t reply to 0:25:45] this email, formal notification. Yes, directgov.uk is legit, I would say.

Password reset information, [email@mail.adobesystems.com](mailto:email@mail.adobesystems.com). That’s legit.

[Facebook@notificationfacebookmail.com](mailto:Facebook@notificationfacebookmail.com), it’s an email address. Facebook do have an email address [like this 0:26:42]. The links look legit, but they could hide links that aren’t that [text], I don’t know, maybe a four.

Dropbox, [notify@dropbox.com](mailto:notify@dropbox.com), looks pretty standard.

Frank at EasyRoommate, yes, I know this email well. Uk.easyroommate.com, the link looks legit, from [frank@easyroommate.com](mailto:frank@easyroomate.com), yes, legitimate.

HSBC… Funds blocked. Attempted [error in login] was detected by our security systems \_\_\_[0:28:09] message… For receiving payments.” HSBCBusiness.co.uk. That wouldn’t be HSBCBusiness.co.uk. Or would it? I don’t know. It doesn’t sound right, I’d say phishing.

[Accounts@Google.com](mailto:Accounts@Google.com). [Support@Google.com](mailto:Support@Google.com). This looks legitimate, I’ve had these before. It’s got like a name, a little picture, yes, that’s probably legit.

\_\_\_[0:29:29], so slow. (Laughter) “Get ready for your luxury [fix], \_\_\_ luxury spa.” Urgh, no. Phishing.

Directgov.slc.co.uk \_\_\_. “To allow us to update our database fill out the information securely. You can do it by going to [mindface.com].” That doesn’t sound… Great. It’s from the Student Loans Company, but it says ‘Yours sincerely Student Finance England’ and I know the Student Loans Company work for Student Finance England, but they just collect debts. Ooh, I don’t know. I would say phishing.

Security Verified by Visa, “Dear valued customer, your credit card has been suspended and errors detected in your credit card information. The reason for your error is not certain, but for security reasons we have suspended your credit card temporarily. To update your information…”

“The reason for this error is not certain,” they would have given a… I don’t know. Surely you can see if your credit card has been. I don’t know. This one does look legit. The Verified by Visa one does look legitimate. That’s a sneaky one. “Detected by your credit card company… Information.” It’s just, “Dear valued customer…” No, it would put your name; it would put Helen Jones, phishing. Yes. No.

The team at Blackpool Pleasure Beach, \_\_\_[0:32:19]. It says it’s from team@blackpoolpleasurebeach but it says [surveys at \_\_\_.co.uk], which might be legitimate, but it doesn’t really seem very official. But Blackpool Pleasure Beach wouldn’t have that much of an official email anyway, I wouldn’t say. I would give it a phishing…

DVLA, DFT… “We are updating our database and all drivers are required to update and verify their driver’s licence details,” is that a thing? “We sincerely apologise for any inconvenience this may cause you…Driving \_\_\_ Agency, Swansea. DFT.” What’s DFT? DFT.gov.uk. Well, .gov.uk sounds legit, but it would be from @gov.uk, wouldn’t it? Umm, doesn’t look very official, I would say phishing.

[Al Malcolm 0:34:20]@Lancaster.co.uk \_\_\_.ac.uk. “Welcome to Lancaster, a Survey Monkey. Survey Monkey is legit, obviously. [Ross Malcolm] it’s @lancaster.ac.uk. Yes, I’d say it’s legitimate.

**P343**

P343: ‘Security verified by Visa.’

[Background noise, 0:00:03-0:00:16]

It’s, ‘An error was detected in your credit card information.’ No, Visa would not suspend my credit card temporarily. That’s a customer support service, verified by Visa.

It looks legitimate.

[Background noise, 0:00:44-0:00:55]

Paper. I want to see the monthly activity and recent transactions.

This seems to be legitimate as well.

It gives that, advertisement as well. NatWest. This mentions who sent the mail, including the name, and my account number, so it looks legitimate.

HR Manager. This looks alright. One of them has got to be a phishing E-mail, but I seem to be getting all of them as legitimate.

Direct Govern. May require all students to obtain that. No. It’s not even proper English. This does not look legitimate at all. Phishing.

HSBC. No. Does not look like legitimate. Again, this NatWest account does not look legitimate. FedEx.

‘Dear customer.’ It says the order number and the order date. If it’s giving the order number it should be right. Legitimate.

Says, ‘Beware of scams protecting.’ This one is a scam itself.

Gram. No, this looks like that will really lead me to a phishing site.

This has got a lot of assistance provided, so I think it’s legitimate.

No name for attachment. ‘Hello,’ that doesn’t sound like the right greeting. No. Phishing.

‘Dear valued customer,’ good greeting. This looks legitimate.

PayPal. The ‘From’ E-mail ID looks good, ‘service@therealpaypal.com’. E-mail address unconfirmed. It takes us to the PayPal site, so this can’t be a phishing E-mail.

This is from Wash-Col.edu. It’s the way you link. Phishing.

‘Greetings’. Funny way to greet, but this looks good. But the site looks dodgy. Yes, the site looks dodgy. I’ll go with phishing.

It’s got the Barclays logo, but the greeting is not good. They don’t usually ask to verify account requests just like that. Phishing.

‘Caxton Effects’. It’s got that Caxton Effects site for E-mail link. Yes, this looks alright.

It’s received from a good E-mail address.

At Mineface? No. This is phishing.

It’s got the Dropbox logo. It looks good to me.

No, this is definitely phishing. Click here. Giving a familiar J-box. You don’t get bonuses just like that.

It’s giving them sign-in attempt details. Location as well. Mmm, this is good. Legitimate.

It’s received from Offen-mail. It says, ‘Gogglebox has received your parent.’ Yes. This is not legit.

Adobe, that’s got that round logo. Not legit.

It says the card number, mentions the name. From servicecentre@paypal. I’ll go with legitimate.

From eBay Administration. To update your E-mail accounts, click on cgi1ebay.com, so that’s an eBay. Legitimate.

From Facebook, Notification of [CV here 0:08:17]. No. You don’t need that as an E-mail addy. Not legit.

Again, [Call Backsock]. And again, I-offer. This is definitely phishing. Click here to cancel the transaction. Nice try.

Got the right logo, Amazon.com. But it’s not got any…

‘Best regards, Amazon.’ Theme, or anything. Phishing.

Oh, this is definitely phishing, they don’t just send some random person your details. He doesn’t just trust you.

‘Phillipe O’Sean.’ That’s Phillipe. He’s not even used my name. No. Definitely phishing.

I-Grasp. This seems okay. This is good.

Well, that’s a big ‘Him’. That address makes me feel it’s phishing.

News extra. No, phishing. It’s not got the eBay logo. Phishing. EBay E-mails usually have the logo.

Pleasure beach visitor. The address it’s saying from is also okay, I guess. No. Service@therateIexpectable. That doesn’t sound legit. Phishing.

DVLA. Info@therateDFD.co.uk. No. Phishing.

Again, the E-mail address it’s signed from says DFD even though it’s DVLA.

Malcolm. This looks legit. It’s mentioned its E-mail ID. ‘Dear student.’ Good.

**P344**

P334: So, first email, I- ‘Our online banking help.’ Yes, I think this is legitimate. Okay. ‘PlusNet \_\_\_[0:00:19].’ Yes, legitimate. I think it’s legitimate. PayPal. ‘Shipping under \_\_\_[0:00:39].’

[Break in audio 0:00:42-0:00:52]

That’s a weird watch. eBay, yes I’d say- yes, legitimate. Okay, Facebook, ‘Hi Helen, \_\_\_[0:01:10] email address to confirm your \_\_\_.’ I would say this is a bit fishy. Okay. ‘No Name,’ alright, ‘Hello. The bill from Virgin Media,’ okay. ‘Our team will be…’ I think this is definitely phishing, yes.

Gucci, Cartier, Rolex, ooh. ‘Give your loved one a luxury watch today.’ Definitely phishing. ‘Dear \_\_\_[0:01:58], your credit card has been suspended as \_\_\_.’

[Break in audio 0:02:01-0:02:11]

Visa. I would say this could be phishing. Okay. ‘\_\_\_[0:02:24] entertainment \_\_\_,’ what is this? ‘It has come to our attention \_\_\_.’ This sounds phishing. I think this is phishing. Dropbox. Yes, I’d say it’s legitimate.

[Break in audio 0:02:53-0:03:04]

No, no, I don’t like this one. This one is not right. Adobe, ‘Reset information.’ It doesn’t look good to me. Okay. ‘\_\_\_[0:03:30] Student Finances. Due to a recent update in our database, \_\_\_ to ensure you receive your scheduled payment.’ This is a weird one. I’d say- I don’t know. ‘Gary Cooper, hello, \_\_\_[0:03:53] was born January-’ oh Jesus. For shame. Okay. ‘\_\_\_.’ MasterCard? No, no, phishing. Don’t like it.

Okay. ‘Thank you for your interest in our new role. I would like to let you know we have \_\_\_[0:04:22] and I’m glad to find that you have made my shortlist. I \_\_\_ you the location.’ I wouldn’t know about this one. ‘We will \_\_\_ dates \_\_\_.’ Okay, I’d say it could be legitimate. ‘Dear candidate, a job which matches your \_\_\_[0:04:53] has been published on our website, please click the following link.’ Yes, why not, could be legitimate. Oh, what is this? ‘[Not 0:05:15] replying is extra. \_\_\_.’ Phishing, I think.

[Break in audio 0:05:27-0:05:40]

FedEx. Their email address is strange. ‘FedEx Team,’ alright, I don’t know what it is. Okay. ‘Dear guest user at Google Books. \_\_\_[0:06:04] payment regarding \_\_\_.’ No way. No. I think it’s phishing. ‘Hi Helen, someone \_\_\_ send your \_\_\_. We prevented this.’ This sounds correct. ‘Hello, I’m sorry for reaching you rather too late due to the \_\_\_[0:06:37] right now. My family and I have a trip \_\_\_.’ Oh Jesus, phishing.

Barclays. ‘Dear \_\_\_, we have detected unusual activity in your account.’ Okay, I think this is phishing. Phishing. ‘This is to inform you that your business account with us-’ oh, I’m hungry, ‘has been blocked recently and \_\_\_[0:07:16]. Please \_\_\_ if you are not \_\_\_ please-’ phishing, I think. Come on. Okay. Easy Roommate? ‘Click here to see the message. Frank at Easy Roommate.’ I don’t know. Okay, I would say maybe legitimate.

‘\_\_\_[0:07:54]. We just \_\_\_ from Google.’ ‘Invoice sent.’ Shouldn’t it have the price, though? ‘I \_\_\_[0:08:16],’ I don’t know. Alright, ‘eBay invoice notification.’ There it is, this invoice has it, the price on it. ‘This is invoice number two \_\_\_ your eBay invoice for the period… Amount due, you have settled-’ what? Yes, this could be legitimate. Okay. ‘Your card is about to expire.’ Okay, could be legitimate, this one. Oh, yummy. Okay, ‘Thank you for shopping with us, we \_\_\_[0:09:24-0:09:33].’

[Break in audio 0:09:33-0:09:45]

Okay, this doesn’t look right, I don’t know why. I think it’s phishing. This one looks phishing too. Oh please, this is phishing. Dell. What on earth? ‘Dear \_\_\_[0:10:15], thank you for your recent \_\_\_.’ No, phishing, I think. Okay. ‘This is \_\_\_ Student Loan Company. We have detected…’

[Break in audio 0:10:35-0:10:47]

I think this one is phishing too. eBay, ‘Dear valued eBay member, we regret to inform you that eBay has…’ no, phishing, definitely. ‘The team at Blackpool Pleasure Beach.’ Blackpool Pleasure Beach, oh God. No, phishing.

‘We’re currently updating our database and all the drivers are required \_\_\_[0:11:28] to complete your \_\_\_ licence.’ I don’t know this one. Could be. Could be legitimate. ‘\_\_\_[0:11:58] to be entered into a draw, please complete this survey. Please note…’ Yes, I think this one could be legitimate.

**P345**

P345: Mmm, so I’ve read the email now. I’m unsure about this one. I wouldn’t say it’s definitely legitimate, but it seems trustworthy enough, because they mention the case number and the service [type 0:00:31]. They don’t ask the recipient to give them any relevant details, any personal details, so I would give it a four, I think. Yes.

Okay, so the second email, ‘Blizzard Entertainment’, seems less trustworthy. It’s a bit more informal, the style of writing. There are some mistakes in it, and, unlike the other email, it doesn’t state anything about data protection. Hmm, yes. It seems unlikely that you would receive such an email, so I’d say it’s a two.

Yes, the next one, the job alert, seems legitimate. I wouldn’t see why not. I would say that’s a six.

Okay, so the one by Philippe, I would identify definitely as phishing, because it asks you to pay over money. Yes, it seems like an unlikely scenario, what he’s describing.

The next one, the one to create a new password, seems like phishing as well, because if you wanted to reset your password, regardless for which account, they would send you a more formal email than this.

Yes, the Dropbox one seems alright.

The eBay one seems alright. Hmm, I think it’s alright. I’m wondering about whether they would write ‘Regards, eBay’, it seems slightly strange. Also, ‘billing@ebay.co.uk’, but that might be possible, so I’ll go for a five here.

The Google one seems alright. Yes, I’d say that’s legitimate.

That seems strange, to get the one from iOffer. That seems strange, to receive an email, like, a confirmation for an order, and then not to get the payment and shipping instructions with that email. That seems slightly weird, but it could be alright, I guess. I wouldn’t trust it, I would give it a three.

The Plusnet one seems perfectly alright. It only asks you to go to the portal and log in, account, username and password. So, if I knew I had an account like that, I wouldn’t be worried about that.

I don’t know about the Easyroommate one. It seems slightly strange, but I can’t really tell why. It always makes me slightly suspicious when they ask you to copy and paste the URL into your browser. I’d say a three again.

Alright, so the [PayPal 0:11:17] one seems fine. I didn’t know that they had their headquarters in Luxembourg. I’m not entirely sure, I’d say a five. I’m pretty positive that it’s alright, but…

The Amazon one seems strange, because it’s not from Amazon. The way they put things, there are a lot of typos and grammatical mistakes. I’d say it’s a two.

The Student Finance one seems like fraud. Yes, I’d say that’s definitely phishing. They wouldn’t ask you to re-enter your complete information like that.

The one from Facebook seems alright. It gives you the… Oh, I don’t know. I guess I think that because they mention the possibility to just disregard the message… The email address it’s from seems slightly weird. I’d say it’s a four.

Okay, the next one is definitely phishing, I’d say, because there’s just no information whatsoever.

So, the one that’s supposedly from the recruitment department I’d say is definitely phishing, just because of the design, and also the way it’s phrased seems really unprofessional, how they’ve advertised the link visually, too. I’d say that’s definitely phishing.

The FedEx one seems like phishing as well. The email’s weird, it doesn’t say which Post Office. Again, grammatical mistakes, seems really unlikely. I’d say it’s phishing.

The next one seems alright, because they offer a phone number as well for questions. It seems alright, I’d say a five.

Here, the next one, same as the one from Philippe, I’d say is phishing, definitely.

I’m not sure about the Barclays one, I’d say a four. It all seems sensible enough, but I’m sorry, I can’t really put my finger on it, but something about it seems off. It’s really ‘maybe’.

Yes, the next one seems like phishing. Yes, definitely, the email address is weird, spelled wrong, not addressed to anyone, written in a weird way. I’d say it’s definitely phishing.

The next one I think is phishing as well, because again, the email address it’s sent from is weird, the way it’s phrased. “To…” I think they wouldn’t take this cause of action if there had really been concerns about, like, an eBay account and the way it was used. Also, ‘safe [hardware 0:20:47] department’ all seems very dubious, so I’d say it’s phishing.

The next one, I’d be suspicious of as well, the Adobe one. I’m not completely sure if it’s… I’m not entirely sure that’s it’s phishing, but I’m pretty sure. I’d give it a two, it seems very strange that they would ask you to reset your password in this way, and also tell you that they’ve reset your password, but then not tell you what they’ve reset it to, I guess. I’m not sure, I’d give it a two.

The next one is phishing, I’d say that, because of the weird email address. Hmm, on the other hand, it tells you about phishing emails and asks you to just put ‘paypal.co.uk’ into your browser. Huh. I can’t be sure of this one, I’ll give it a three I think.

The NatWest one seems legitimate.

The PayPal one seems alright. I’d say five, because I’m not entirely positive, but yes.

The next one, I’m not entirely sure. It seems a bit informal, but not as bad as some of the other ones. I’d give it a four.

Yes, the next one is definitely phishing, I’d say. They wouldn’t send you this kind of email if your account would really expire. No, it doesn’t make any sense.

Okay, the next one’s definitely phishing as well.

Yes, the next one I think is phishing as well, because the information they give is so unspecific, the language they use is not very clear. It doesn’t say what kind of problem there has been. I’d say a two.

Yes, the HSBC one I think is phishing as well. It seems really unprofessional. “The account will be disabled if you ignore this message.” Also, there’s, like, no greeting in it.” It seems weird. ‘Customer business unit’, I think they wouldn’t sign it this way if it was really from the bank. I’d say a two.

The next one seems strange as well. On the other hand, yes, I don’t know. I doubt that they would have an email address called [‘thanks@virginmobile.com’ 0:31:02]. A two, I’d say.

Yes, the Pleasure Beach, Blackpool one could be alright, I think. A three, I’m not entirely sure. It could be either.

The next one I’d say is phishing. I think they wouldn’t ask you to complete your information again, or the licence details. No, that could be identity fraud. No, and you couldn’t lose your driver’s licence because you didn’t complete an online thing like that. I’d say it’s definitely phishing.

The next one seems alright, it has a Lancaster email address. I’d say a five, I’m pretty sure that that’s legitimate.

**P346**

P346: Dropbox, noreplydropbox. The email address is okay because it's noreplydropox.com. 'To verify your email address'. 'Hi Helen, Dropbox needs to verify your email address before you can share folders'. I think this is a legitimate email because it has a good email address, noreplydropbox.com, and it has an official logo and there is a sign, 2012, Dropbox. I'd answer definitely legitimate.

Oh, I think it's phishing because these stars/asterisks- okay, Student Finance, Student Finance. Well, there is something strange in the email address. For example, it's written 'Student Financee', double E at the end, @direct.gov.uk. 'This is a formal notification for an important account update'. It's very strange why they write 'We' with a capital W. '\_\_\_[0:01:21] to update your account information'. Yes, and 'click here' is in a separate sentence, so grammar mistakes. Student Finance England. I think this is a phishing email, but I'm not 100% sure. Yes, why not?

[Silence 0:01:54 -0:02:06].

It has a logo and image. Okay, I think it's close to phishing, but I'm not sure that it's definitely a phishing email. I'll put two here.

Okay, there is a lot of text here. Oh no, that's a phishing email, when they ask for money. 'All we need is 1,000, blah, blah, blah pounds. My family and I-' oh. No, no, no, definitely a phishing email.

[Carla Gregg 0:02:44], Amazon. Who's Carla Gregg? I think it seems to be very professional this email. It seems to be official and legitimate because it has a good design. It's not plain text. It's an HTML version of email. I think it's definitely legitimate and it's from Amazon.com.

No. (Laughter) No, no, no. Phishing, phishing. No images and a very strange address and a big link. No. 'Create a new password'. Maybe not. Maybe that's just extra. 'To continue with \_\_\_[0:03:48] process, please proceed to the link'. Maybe no. Maybe this is legitimate. Notwithstanding the link and the absence of the image, it has a link to an IP address and 'a section was requested from IP address', da-da-da-da. I think this is the email which came from a particular website, and they should know information about IPs, IP addresses of users. Yes, this is definitely legitimate, but the design if awful.

eBay. Oh, that's a very strange address eBays.com, and the logo, I don't know whether it's the eBay logo or not. \_\_\_[0:04:46]. No. It seems to be phishing, although it has a good design and the structure of the email is really nice. The link 'to update your eBay records, click on the following link', the link has not the correct address, in my opinion. It's cegi1.ebay.com, ycgcegi1. The address of the person who's sending the mail, admin@ebays.com. The text of the email is very strange. I don't think that eBay writes letters and sends letters like this. It doesn't seem to be legitimate. I think it's phishing, but I'm not 100% sure, so I'll put two here.

HSBC. It seems to be legitimate, although it contains negative information about the block of an account. It has good mail inference, emailinfo@hsbcbusiness.co.uk, and it's written in an official style. It seems to be a letter from the bank really, so I think it's definitely legitimate.

Oh, it's so small. Oh okay, eBay, so here we have the correct email, ebay.co.uk. Yes, this seems to be a letter from eBay. This an automatically generated email. Yes. Yes, this is definitely legitimate.

Okay, so the thing which I'm concerned about is the absence of images, but it happens sometimes. Noreplyioffer. The mail address is good. 'Congratulations, you just purchased an item from Google Books. Invoice'. Yes, it an automated email. I think it's correct, but maybe there were some restrictions of the user and he didn't switch on the images. That's why they are not showing here. It's definitely legitimate.

Okay, so the address is okay, support@plus.net. I'm not hesitating about this. Yes, okay. \_\_\_[0:07:54]. Yes, I think it's a very legitimate email because, well, the text is good. It doesn't push you to do an action. It's up to you to decide whether you want to or do not want to. It has some return addresses, people to whom you can write. Well, not people, but an email reference and also a website and also help assistant details and numbers. Yes, it's legitimate.

Okay, the same address, iOffer.com. \_\_\_[0:08:38]. Yes, I think this is a legitimate email, just an automatic response that they did something or received something, and a link which leads to the site, iOffer.com. iOffer.com is mentioned in the address, so it's fine.

FedEx. This is not the logo of FedEx. The log of FedEx is different, and the email address is very strange, dtf.193, postoffice@- 'the post rider was unable to deliver the parcel'. The text is so strange, and it has 'order reference'. There are no excuses. I don't think that this is how FedEx treats its customers. If customers experience a problem or a post rider is unable to deliver, they apologise, but here there are no excuses. 'With regards to receive a parcel, please-' okay, I don't think that it's a phishing email for sure, but it seems to be phishing. Otherwise FedEx needs to think about how to respond to its customers. Okay, I'll put two here.

Noreplyblizzardentertainment. Oh, I know them, battle.com. '[Recently it has 0:10:27] come to our attention \_\_\_'. Diablo III account. I don't know. I'm hesitating. Well, it contains a link and the text is good. It looks like a very official email, and the email address is okay, noreplybattle.com. Why battle? Why not Blizzard if it's Blizzard Entertainment? There are lots of 'must'. You must do that. You must do that. \_\_\_[0:11:10]. Yes. Well, I'm not confident about this email, but it seems to be legitimate. I'll put definitely legitimate.

Okay, \_\_\_.'Your password with expire in three days. Click here'. Well, the address is washcoll.edu and the [edu states] for education. The address of the person is Edlancaster.ac.uk, so it seems like the person is registered in an educational forum or educational website and this is the message which was sent to him. 'Your password will expire in three days. Click here'. It's very strange how a password can expire. Is it possible? There are no dots. No, it should not be legitimate because the link is 'upgrade webmail'. Why to upgrade? Usually if you upgrade something you need to pay money for that. I think it's phishing. It's a phishing email.

Okay, the email address is good, [directgov@clcslc 0:12:48]. 'This is a message for all students for student grants. \_\_\_'. I don’t know. The address is okay, directgov.lce. It doesn't make me feel not confident about the sender, but the information is that 'we have detected fraudulent activities going on in the student loan accounts'. Again, there is a coma and a T with a capital letter. I'm not sure that the company which is in charge of student loans makes grammar mistakes. 'You can do this by clicking the link below or copying and pasting into your browser'. Mineface.com. What is Mineface? It doesn't seem to be legitimate, but I'm not sure that it's phishing either, so I'll give three here. I think this is the first time I've put three, the answer three. Okay.

Facebook mail. Okay, the links are good. The links lead to Facebook and not to other sites. Yes, and also there is an option to disregard the message. It seems to be official. Yes, it's legitimate.

Okay, I love the design. The design is good. Online banking. I'm not sure that companies who send phishing emails take care about design so much. 'Your latest statement is available now', da-da-da-da. No, no, no, it's definitely legitimate. It looks very neat.

Okay, Caxton, the next question. 'Changes to the terms and conditions of your \_\_\_[0:15:24]'. It seems to be official because there is a post address and there is a phone number. Also, this is the logo of a company and the email address, @caxton@x.com, so it's definitely legitimate. There is something written in small font. Yes, it's six.

No, it doesn't seem to be legitimate. It looks like phishing. \_\_\_[0:16:00]. When they ask to send money I think it's not a real case, and in Italy. 'In your good faith'. No, no, no, definitely phishing. Forget about money, Mr. Gary Cooper. (Laughter) Gary Cooper. (Laughter) That's funny.

You mobile bill, dated- zip. No. Why zip? Virgin Mobile. No name for the attachment. Well, Virgin Mobile looks impressive. 'Hello, the bill for your Virgin Media mobile is now-' what does it mean, 'the bill for your Virgin Media mobile is now ready to view'?

[Silence 0:17:00 - 0:17:11].

No. No, no, no. [He won't] be picking up a mail [for himself]. 'If you'd like to email us back, send us an email'. I don't think this is the way how Virgin sends emails to its customers, and zip files. Files are rarely attached to emails like this. It's definitely phishing.

'Dear applicant'. Yahoo. Yahoo is good. I trust them, but the first part, [hrdept 0:17:52] 33433, what does it mean, 33433? '\_\_\_. Job offer full-time and part-time positions \_\_\_'.

[Silence 0:18:11 - 0:18:38].

It doesn't seem to be legitimate and professional, although it uses Yahoo as a brand. It's not written in an official style and he names himself, the person. 'My name is Adam French'. He names himself in the middle of the letter. That's a strange way. These arrows which point at the link, it seems like they try to attract attention. If it's a letter from Yahoo they don't need to put these arrows because if it's an applicant for a job he will open any emails for sure. It's phishing. Sorry, Adam French.

PayPal. Wow, I love the design. It looks professional. Yes. Definitely it's legitimate, no doubt, the structure, the outline.

No. The first impression is that it's definitely phishing. 'Hi Helen, please don't reply \_\_\_'.

[Silence 0:19:53 - 0:20:07].

Maybe they're just a small company which helps to find accommodation. That's why they send an email like that. 'I've just received a message from \_\_\_ member'. This is the website easyroommate.com. 'Hi Helen, click here to see-' it seems to be okay. It really seems to be okay, but what makes me doubtful about this email is that it has a very long link. Yes, but the reason for providing this link is that maybe the person will not click here, which is underlined, which has a hyperlink, and that's why the whole link needs to be provided. Yes, it's definitely legitimate.

PayPal. The design is great, but the web address is very strange. 'To Keith [Pollitt 0:21:15]. \_\_\_'. It seems to be real. It has such a good structure and detail. Also, it leads to the PayPal website, so if you have any questions you can contact their help centre. The thing which is really strange is the address of the person who sent it, or not the person, the company who sent this email. 'Approximating these 100- shipment recently confirmed'. Ah, maybe this is the address of the person to whom the payment was sent, the person, Keith Pollitt. That's why it's mentioned there, 'receipt for PayPal payment'. The item has a code number. Ah, yes, it's definitely legitimate.

Does Google send letters like this and attachments? Ah, I see why attachments are here. One attachment is for the Google logo and another for a profile photo. Also, it has an IP address and location, Italy. Yes. Thank you, Google. It was definitely legitimate.

Okay, Visa. 'Security verified by Visa. Dear valued customer, your credit card has been-' I love the logo at the beginning of the letter. 'Need you to update your information for further use on your credit card'. I cannot read the text which is written in yellow. 'If this is not received within- your credit card has been suspended as an error was detected in your credit card information \_\_\_[0:23:46] your credit card temporarily. \_\_\_'.

I don't know. On the one hand it seems to be professional and legitimate because it has the Visa logo. It has a good structure, no grammar mistakes, and the email address looks suitable, noreplyverifiedbyvisa.com. At the same time it tells that they will suspend the card, or they already suspended it. You cannot use it unless you click the link. I'm not sure that it's definitely legitimate, so I will give it four. The first time I answer four.

Okay. Dell. It looks nice, but the text is very small. I can't read it. '\_\_\_[0:24:58] Dell support regarding case number'- oh yes, it has a definitely case number. I think it's official, legitimate. 'TNS on behalf of Dell'. Who is TNS?

[Silence 0:25:20 - 0:25:33].

Customer satisfaction research company, so it's not only an email from Dell, but it's from TNS. 'To complete the survey, please click on the website below or copy and paste- \_\_\_ customer experience'. Well, it makes me doubt. I'm not sure that this is an official email, legitimate email. It has so many details, which makes it look legitimate, but meanwhile it offers to run a survey, participate in a survey. It happens. I know that in companies sometimes it happens and they offer the clients to participate in surveys. I think it's legitimate, but I'm not 100% sure, so I'll give five.

Barclays.

[Silence 0:26:26 - 0:26:44].

No. It doesn't seem to be legitimate. It seems to be phishing. Again, problem with accounts. 'Click here to verify your account records'. They usually send a particular link. The purpose of hiding the text of the link, making it a hyperlink, is that you cannot see the address and a website address because you see only the text. It's phishing, but I'm not sure 100% that it's phishing.

No, I don't think that this is legitimate, no, because, firstly, it has a very strange email address, [up@danktar 0:27:34]. I don't know about the logo. I don't know NatWest, what that company is about. Again, it's a hyperlink not a link, so you cannot see the text. You cannot see the address, the web address. I think it's definitely phishing. Yes. This letter is definitely phishing.

Okay, PayPal again. The email address is good and the references, the contact numbers. 'Visa Delta Electron ending in-' yes, and it's a reasonable email. It gives the number of a card, one, two, three, four. If you read this text you definitely understand whether this email is for you or not for you, so you can make a decision. You can clearly understand if it's phishing or not. '\_\_\_ if you have received any \_\_\_ the card'. It seems to be reasonable. If you have a PayPal account you need to enter your card details so they can track if your card is still valid or not. Yes, it's legitimate.

Oh, (Laughter) phishing. I have no comments about it. (Laughter) The web address is very strange and the text is nonsense, and the 'Yahoo email user, click here'. No, no.

I-GRasp. It's recruitment again, recruitment \_\_\_[0:29:50]. Well, the link which is provided here, that's what I was talking about before. It shows the particular website. No, it doesn't show a particular website. There is something strange. There is no dot after www. It's written as text, but something is hiding. 'Please click the following link to paste it into your browser \_\_\_[0:30:28]'. How do they know about psychological assistant? The link is strange, the absence of a dot after www. A link should not be working.

Maybe they simply typed a text and then created the hyperlink, which doesn't seem to be official or legitimate. That's the approach which phishing companies I think should use. HMPS Recruitment, i-GRasp. I'm not sure. Okay, I'll give three here.

Adobe. It looks official. It really looks a nice design. Adobe Systems email. Yes. Phishing companies I think will not take care of design like that, and also there is a phrase that if you have many newsletters you can unsubscribe or schedule automatically. Yes, it's legitimate.

Okay, so Blackpool Pleasure Beach. 'Hello, pleasure beach visitor'. This is a reply to a particular email. I think it's official. It's real. It's not phishing. 'Everyone taking part will be entered for \_\_\_[0:32:25]'. How do they know that a person visited Blackpool Pleasure Beach? Yes, I think this is a legitimate email because in real life the person could go to this Blackpool Pleasure Beach, write his or her email somewhere and then they simply collect feedback from their customers. Also, it has something like a reference number at the very end of the letter. I'll give it six.

\_\_\_[0:33:10] DVLA. Letters which contain logos make me confident that they are not phishing. '\_\_\_'. Yes, and also the link goes directly to address.gov.uk, which makes me confident about this email, so it's definitely legitimate.

Okay, a letter, yes, (Laughter) from Lancaster University @lancaster.ac.uk. It cannot be phishing. (Laughter) Yes. It's legitimate.

**P347**

P347: 'It has come to our attention that you're trying to \_\_\_[0:00:10].' Mmm. 'As you may know, we are \_\_\_.' [Yes, this proves to me]…

[Break in conversation 0:00:21 - 0:00:39]

Mmm.

[Break in conversation 0:00:40 - 0:00:53]

Mmm.

[Break in conversation 0:00:54 - 0:01:14]

This one's a…

[Break in conversation 0:01:15 - 0:01:32]

Mmm. The link looks very weird.

[Break in conversation 0:01:39 - 0:01:54]

[Again, so much]…

[Break in conversation 0:01:56 - 0:02:07]

'Thank you for your recent contact with \_\_\_. [Until] \_\_\_ to go \_\_\_. Please enter your email address into… \_\_\_ should \_\_\_.'

[Break in conversation 0:02:27 - 0:02:40]

Hmm. Well, at the end, it's not with Dell.com, so it must be phishing.   
  
PayPal. Let's see.

[Break in conversation 0:03:04 - 0:03:21]

\_\_\_.

[Break in conversation 0:03:22 - 0:03:38]

'\_\_\_ your first and last name. [If you're concerned and want]...' Yes.   
  
'I'm sorry for reaching you \_\_\_[0:03:58] [to this address] \_\_\_.' Yes, okay. 'We got attacked by some unknown gunmen, \_\_\_ our money \_\_\_,' dah, dah, dah. 'We have reported [the addresses 0:04:20] \_\_\_.' Yes.   
  
[Your address 0:04:41] \_\_\_.

[Break in conversation 0:04:43 - 0:05:00]

Yes, this one is okay.   
  
Yes.

[Break in conversation 0:05:10 - 0:05:22]

This is definitely phishing. The extension of the email is not one of NatWest.   
  
PayPal. 'Your card is about to expire.' Mmm.

[Break in conversation 0:05:48 - 0:06:04]

Yes.

[Break in conversation 0:06:05 - 0:06:17]

This one is phishing. Since when do PayPal send these kinds of..?  
  
eBay. Mmm.

[Break in conversation 0:06:34 - 0:07:04]

Yes, [these, they are] to update the records of \_\_\_ credit card \_\_\_.

[Break in conversation 0:07:11 - 0:07:28]

Barclay.

[Break in conversation 0:07:29 - 0:08:04]

Yes, this one looks like phishing.

[Break in conversation 0:08:07 - 0:08:25]

[Okay then], 'Thank you for \_\_\_.'

[Break in conversation 0:08:29 - 0:08:50]

Mmm. Mmm.

[Break in conversation 0:08:52 - 0:09:03]

Mmm. Yes, [they haven't included a note].

[Break in conversation 0:09:16 - 0:09:38]

[Good].   
  
FedEx. 'Your parcel \_\_\_.'

[Break in conversation 0:10:53 - 0:10:31]

[I don't know]. This one is phishing. There is an order. They've put the name and the last name. Mmm.

[Break in conversation 0:10:46 - 0:11:00]

Yes. Usually, you receive an email from the bank with your first name and your last name [and that], from Visa.

[Break in conversation 0:11:16 - 0:11:26]  
  
\_\_\_.

[Break in conversation 0:11:27 - 0:11:57]

I don't know. I've never received an email from Facebook, so I cannot really judge. Mmm. I don't know. Yes.  
  
Amazon. This one, I should know.

[Break in conversation 0:12:24 - 0:12:51]

Okay, 'Hello, Helen Jones. Thank you for shopping with us. [We thought]…

[Break in conversation 0:12:57 - 0:13:10].

[Wait], 'Items that total 359.99. Shipping and handling, 15.00. Total before tax…' No.   
  
Okay. 'The bill for your Virgin…'

[Break in conversation 0:13:32 - 0:13:49]

This one is okay. Let's see. This is a \_\_\_. There is an update…'

[Break in conversation 0:14:02 - 0:14:33]

Dropbox.

[Break in conversation 0:14:34 - 0:15:07]

Okay.

[Break in conversation 0:15:08 - 0:15:19]

'To continue with the [parcel], please [process your]…'

[Break in conversation 0:15:23 - 0:16:17]

'You just purchased an item from \_\_\_.' Hmm.

[Break in conversation 0:16:31 - 0:16:47]

No, when you buy something, they don't ask, 'If you made a mistake, click here to cancel.' [Definitely]…

[Break in conversation 0:16:54 - 0:17:16]

Mmm.

[Break in conversation 0:17:17 - 0:18:09]

Mmm. HSBC don't send these kinds of emails. Phishing.

[Break in conversation 0:18:16 - 0:18:27]

This one's okay.

[Break in conversation 0:18:29 - 0:18:41]

\_\_\_. 'Job application.'

[Break in conversation 0:18:44 - 0:19:17]

If you have made my shortlist, why am I not addressing you by your name? And the application form, usually, is on the website of the HR. Phishing.   
  
Adobe.

[Break in conversation 0:19:43 - 0:20:02]

Mmm hmm. Yes, it looks okay.   
  
'Dear Guest User…'

[Break in conversation 0:20:17 - 0:20:29]

Phishing.   
  
Mmm. \_\_\_.

[Break in conversation 0:20:40 - 0:20:58]

Yes.   
  
'Your password will expire in three days. Click to validate your email.' Hmm. A password does not expire. Hmm, hmm. They usually ask you to change it, or to… Okay, the address it comes from, onlinebanking@information.net, \_\_\_, it should be fine. But…

[Break in conversation 0:21:58 - 0:22:09]

Yes. Mmm. The Pleasure Beach Blackpool Team.

[Break in conversation 0:22:25 - 0:22:42]

Mmm. Yes. It comes from a real address.   
  
Okay. Mmm.

[Break in conversation 0:23:00 - 0:23:29]

Mmm hmm.

[Break in conversation 0:23:30 - 0:23:50]

[Should be okay].

[Break in conversation 0:23:51 - 0:24:03]

'Dear Student…' Mmm.

**P348**

P348: So in this email it's from Easyroommate, which is a legitimate website. I'm assuming that Helen would have an account with Easyroommate. It doesn't look like it's asking for any details and you do have to log into your account with Easyroommate to see the messages, so that seems quite okay.

This next email's from eBay. Just giving you a statement. So it's not asking for any information, it's just telling you that it's available. So that seems okay.

This next one's by Visa. That looks quite dodgy because it's actually asking you to lift the suspension of your card straight away.

The next email from Blizzard Entertainment looks like phishing because it's asking you to check account details.

The next email from Gary Cooper looks suspicious. It's using a sob story about cancer and offering money and asking for details of personal stuff.

So the next email is from [iOffer 0:02:40]. It's not a website I know and it's suspicious because it doesn't actually address it to a specific person, so that could be bad.

The next is a PayPal receipt. It looks pretty standard. It's not asking for any new details, it's just providing you with information, so that seems okay.

The next email from Google regarding an account might be slightly suspicious. Probably wouldn't trust that one either.

The next one is from a job website. It seems okay. I don't recognise the name of the company, but again, I might be cautious about it, unless you've set up alerts with that particular company.

The Barclays email looks relatively good quality, but I probably wouldn't click on the link. I'd maybe call my bank.

The next one's from Amazon, just giving you information about a delivery, so that's okay.

The next one's a Yahoo and Gmail user 'click here' link. That's just an ad.

The next one is from Dell. That's just thanking feedback with a customer service survey, so that seems okay.

The next one from NatWest, providing you with information that your account is available for an update and you can view your statement. The URL links to a NatWest website, so that seems okay.

The next one's from Facebook. It's going, again, to the Facebook account and website, so that seems okay.

The next one from HSBC doesn't have the proper logo and you can probably just call your bank rather than use that.

The next one from the Student Loans Company. There'd normally be stuff in writing rather than email, so I wouldn't trust that.

The next one from NatWest seems relatively okay, but I wouldn't trust it.

The next one from [Washcoll 0:08:36], looks like phishing.

The next one from Virgin Media is just an update on a bill, but you don't need to action anything, it's just informing you, so you don't need to do anything.

This other one from eBay I wouldn't trust. It's asking you to do something with your details.

The next Adobe one seems okay.

Dropbox seems okay.

The student finance one has a directgov email and is more informational rather than wanting information.

That NUS Extra one seems a bit suspicious.

The job application form seems a bit dodgy, badly written.

The PayPal email is just informational so it seems okay.

Caxton FX seems a bit suspicious, normally because it's about credit cards.

If you recognise the account user name, the McAfee email might be okay.

Next one is definitely phishing.

The next email from Google Box looks just like an automated information email, so that seems okay.

FedEx looks like the wrong colours for the email, but if you were expecting something, maybe. But if you've received this out of context, you wouldn't follow it up.

Blackpool Pleasure Beach, just a customer survey, that's fine.

The next one's from the DVLA. It looks like an okay email, but it seems suspicious that the DVLA would want people to update their information. Although it is based in Swansea, I'd be a little suspicious.

So the next one is a Lancaster Uni survey. That seems okay.

**P349**

P349: So, the first E-mail must be legitimate.

Well, it’s coming from PayPal, and you have all the details underneath the address and stuff. But you can always check, I mean, in your PayPal account itself, but not clicking on the link, because you never know.

So I think yes, I think it’s legitimate. Yes. It has the logo and stuff on it, so, yes.

Okay, that one looks phishing. It doesn’t have any details on it. It just has a few words, it just says, ‘Click here.’ It doesn’t give any information, so I think that’s phishing.

[Break in conversation, 0:01:36-0:01:56]

So, I think that one is phishing as well. The history man one. It doesn’t look, good E-mail, for me. And it looks weird. I think that this is an automated E-mail, then they reply with that kind of letters.

You can’t really see the picture, but that doesn’t mean something. I mean, if you order something, yes, I don’t know. I actually have no clue about it.

Yes, I’m in the middle about it. I’m not sure.

Well, that one’s from Amazon, it’s talking about the shipping confirmation. You know, if you bought something or not, and I don’t think they’re going to send me something that costs that much. Yes, that’s fine.

Okay, so I think that one is phishing, because it doesn’t have any logo or, like…

‘Students, be web-safe.” This is in the subject. “We have detected…”

Yes, it might be phishing, because it’s interesting that it doesn’t have any pictures. Well, the link they have has nothing to do with the Student Loads Company, so I think it’s phishing.

So that one from Dell, it should be fine. It’s not that clear, I can’t really see it on the computer. But it should be fine, I think it’s right about the cases, and yes, the E-mail address looks fine.

So, I think that Jobhunter is fine, it’s ‘HR’, which is something you can’t really go wrong with, so…

I think that one is fine as well. Yes, I think it’s okay. I’m not really sure if it’s legitimate, but I think it’s quite okay.

‘Plusnet support’.

[Break in conversation, 0:06:13-0:06:29]

Not really sure. I’m not sure because, well, on the other hand you have the account user name, so if you don’t have an account, then you know that this is spam. But if there’s an account user name with your name in, yes, so I think that’s fine as well.

I think this one is okay, as it’s a payment. Yes, it’s a payment, so it’s from PayPal through eBay, if I’m correct. So yes, it has a transaction ID as well, so I think it’s fine.

Okay, so that one, it should be a spam. Oh yes. I think that someone will just send that kind of E-mail. It has a phone as well, and Skype.

But I’m not sure if that E-mail, well, it has here the E-mail and the E-mail that the E-mail came from is different, so I don’t know. I wouldn’t feel that this is safe.

NatWest. What? That’s a spam. That’s definitely the phishing, because it says it’s from NatWest and the E-mail next to ‘NatWest’ is not from NatWest. So I wouldn’t feel okay.

But that looks like it’s from eBay. I think it’s okay. Yes, usually that’s fine. That’s an invoice notification. Yes, I think it’s fine.

The E-mail is from eBay, so I think it’s fine.

Okay, so that’s a spam. I think that’s a spam. It says, ‘Please do not reply to this E-mail, follow the link below.’ That makes you go somewhere. But on the other hand the link starts with, ‘UKzeromay.com’. I’m not sure. And it says, ‘Beware of scams.’

I don’t know. I’m not sure about it, so it looks difficult for me.

Next. Okay, so that one might be okay. I’ll need to read it.

[Break in conversation, 0:10:45-0:10:56]

Yes, that’s not fine. They’re asking for money. Yes. No. And a lot of money, so no.

eBay suspension, okay. Well, I’m not sure what’s going on on that E-mail. Yes, I’m not sure, because it’s not ‘eBay’, the mail, it’s ‘eBayz’, with a ‘z’ at the end, and the cover is until 2005 and the E-mail was sent in 2012, so I think that’s phishing.

[Break in conversation, 0:12:01-0:12:17]

So I think that’s another spam, but why does it have an attachment? Why it should have attachments…

Yes, okay, I think that’s fine. The E-mail looks okay. Yes, I think it’s okay.

Yes, I don’t think that one is legitimate. Yes, I don’t know, it looks weird. I wouldn’t click on the link.

So, NatWest.

[Break in conversation, 0:13:27-0:13:40]

Yes, I think that’s fine. Yes, all has the right E-mail, and I think it looks okay. Yes, I think it’s fine.

Barclays. Yes, I wouldn’t try to access that. Yes, I wouldn’t try to click on it. Well, usually they don’t put a name and the E-mail doesn’t end up with the name, ‘Barclays’, so I wouldn’t do that.

Yes, that one is phishing as well. The way that they put the link is not professional at all, so I don’t think that someone who is in a credit department would have the application link like that. And wouldn’t say, ‘I look forward to seeing you soon’, so yes.

I think that’s okay, because the E-mail ends up at, ‘Verified by Visa.com’, so it should be fine. But…

[Break in conversation, 0:15:32-0:15:53]

Okay, maybe not, because, yes, it’s hard. I don’t know. I’m in the middle. I think I would just call the bank. So, Visa Entertainment.

[Break in conversation, 0:16:18-0:16:28]

Yes, I wouldn’t do that, anything that needs to check something. It doesn’t sound good. So I wouldn’t do it. Maybe it’s fine but, I don’t know, I think it’s phishing.

[Break in conversation, 0:16:51-0:17:04]

I think that’s okay, with NUS. Well, the link says, ‘CardsNUSExtra.co.uk’, it has so much stuff on it. Maybe it’s not okay. But the E-mail looks okay. The E-mail address. And they have a \_\_\_[0:17:31] header as well.

I think I wouldn’t link on it. I wouldn’t click on it. I’m not sure.

That’s hard, I don’t know. ‘You enter, you were assigned to this E-mail address’. Well, it doesn’t show the E-mail address. So I’m not sure, I think it’s quite phishing, but maybe not.

So, next one.

[Break in conversation, 0:18:15-0:18:40]

Okay, that’s not a fraud. It’s not a phishing E-mail. He says that if you can log in from your PayPal account to check if you’re not sure about it, so why say that?

Adobe. I think it’s fine, Adobe. Yes.

[Break in conversation, 0:19:15-0:19:52]

Yes, I think it’s fine.

[Break in conversation, 0:19:56-0:20:07]

Hmm, FedEx. Okay, I wouldn’t feel okay about it, I think. Yes, I wouldn’t. I wouldn’t. It doesn’t have any other details on it. Yes, no.

[Break in conversation, 0:20:39-0:20:54]

I don’t know. That one, I think it’s the same with the previous one, but the layout is different, but I’m thinking about it, because yes, it doesn’t have the copyright and stuff. Yes, I don’t.

[Break in conversation, 0:21:17-0:21:40]

Yes, I wouldn’t do that. I never like, they don’t have copyright, they don’t have anything. I wouldn’t do it. I prefer to go to the bank, yes.

Directgov.

[Break in conversation, 0:21:59-0:22:30]

I don’t know. I will say that it can be both. Especially the layout, and that they don’t have anything like, ‘Rights reserved,’ and this kind of stuff. That makes me, like, go back.

Dropbox. I think it’s fine.

[Break in conversation, 0:22:56-0:23:18]

Yes, that’s not okay. The Facebook team stuff. I don’t know. Hmm, ‘If you are not confident with your browser, if you don’t want it, urgent content, please this message to look.’ I don’t know. I wouldn’t do it. I’m…

[Break in conversation, 0:23:56-0:24:11]

Nope. I don’t feel okay with this, with files.

‘Dear pleasure beach visitor, Blackpool survey’. Mmm-hmm. Well, the link has the word, ‘Survey’ on it. So it might be fine. But maybe not, so I’m not really sure between…

Yes, I think that one is fine, the E-mail is quite the same with the link, it has a postcode as well. I don’t know if you receive something like that through the E-mail. Yes.

Yes, no, I don’t think it’s fine.

[Break in conversation, 0:25:44-0:25:55]

I think that’s fine, the Lancaster E-mail, usually it’s okay.

[Break in conversation, 0:26:03-0:26:17]

Yes, that’s definitely fine.

**P350**

P350: ‘servicepaypal.co’... Okay, “Update your card details, October 8th, Helen Jones, Gmail… We notice that your Visa in 1234 is about to expire. Please update your card security codes.” Alright, “Update your expiry date,” okay. I definitely think this is legitimate, because it’s not asking for the credit card number itself, it’s just asking for the security code and the expiration date. I’ve seen one of these emails before, and I looked up which email it came from, and it looks like definitely a legitimate email from PayPal, so definitely, yes.

Okay, “FedEx, priority mail postal service. [dtf193@fortwayne.com](mailto:dtf193@fortwayne.com).” Okay, “Your parcel has arrived at the Post Office on December [6th 0:01:32].” December… Okay, “To receive your parcel, please go to the nearest our office and show this.” Okay, well, there are grammar problems, definitely. The logo doesn’t look like the FedEx logo. The address where it’s from, ‘fortwayne’ doesn’t look like it’s from FedEx, and the order date, “Parcel has arrived… December 7th, [has arrived 0:02:12].” Huh, okay. I’m going to say it’s a two out of six, because it’s sent on the 18th, and it arrived at the Post Office on the 7th. The email, where it’s from, doesn’t seem affiliated with FedEx.

Alright, ‘natwestonlinebanking@information.natwest.com’, so that seems pretty legitimate. “Your latest statement is available online, 8th October. Just log on to natwest.com/online and see more information on your account. If you need more help understanding your statement…” Okay, “With your online banking, remember you can also… Da, da, da, da, da. We’re here to help when you need it.” I don’t think this is phishing, because it doesn’t ask for any personal information, just, “Log on to natwest.com/online.” The email address it’s from is not sketchy.

Okay, Dell… Oh, I can’t see this very well. \_\_\_[0:03:56], zoom in. Right, zoom in. [‘dellsurveyhelp@mailto.rap.tns-online’]. “TNS on behalf of Dell, Incorporated.” Okay, I don’t know what ‘TNS’ means. “Thank you for your recent contact with Dell Support regarding this case number. At Dell, we are committed to delivering the best customer experience to our customers. Valuable feedback regarding your experience with Dell Support will help us improve our internal processes and provide a better service to you. Complete this survey, click on the web address.” That doesn’t \_\_\_[0:04:47] copy the…

Okay, this email address is so long. I don’t think… I mean, I know what [rap to 0:04:57] TNS is. I would assume it should be by Dell or something, the survey. Okay, “Dell has asked TNS, a customer satisfaction research company in the IT industry to help conduct a survey.” Okay, I would say it’s going to be two out of six, because that’s a really… I wouldn’t want to click on that link, it’s too long. I mean, even though the survey will take about five minutes, I just don’t think I would want to do that.

Alright, “Gucci, Cartier, Rolex.” Yes, “Yahoo and Gmail user, click here. Give your loved one a luxury watch today.” The email it’s from is [jbosque 0:06:11], so I would probably say ‘hell no’. I don’t have enough money to buy any of that, and also, I would just go on their own website itself, just not… “Yahoo and Gmail users,” I don’t think that really is relevant if you want to buy something like a watch there.

“iOffer. [noreply@ioffer.com](mailto:noreply@ioffer.com), seller received payment.” I’ve never heard of ‘iOffer’ before. Okay, “Dear guest user, [Googlebox UK 0:06:51] has received your payment regarding the item, [thehistoryman1981]. Click below to view the status. Don’t reply, please don’t reply.” Hmm, ‘historyman’... ‘Messages/show’. Yes, I don’t think this would be phishing, because it is from iOffer. The email address where it come has iOffer in it, and the link does start with iOffer, so I’m going to say five out of six on this one.

Okay, another PayPal. Okay, “paypal.co.uk… Hello from PayPal, log in to see your monthly activity and recent transactions.” Huh, at first, I feel like PayPal wouldn’t put a button in the email, saying, like, “Log in now,” but I’m not totally sure about that. ‘paypal@e.paypal’… I feel like the email where it’s from would probably be… Wouldn’t repeat ‘PayPal’ twice. Hmm, “Monthly activity of recent transactions.” Oh, it says, “How do I know this is not a phishing email? Emails from PayPal will always address you by your first and last name.” Okay, I would say four out of six.

“Plusnet Support, [support@plus.net](mailto:support@plus.net). Your software is available to download. Dear Miss Jones, account username… Thanks for choosing Plusnet. This is ready to download, what to do? Go to portal.plus.net, McAfee downloads.” Okay, “Need help? Da, da, da. Account username \_\_\_[0:09:59].” I think that website it would tell you to go to looks legitimate. ‘Account username and password’, I think that’s fine. I wouldn’t store personal information within my account username and password, and it’s McAfee, something that I’ve heard before. Yes, ‘plus.net’. Yes, okay, six, definitely legitimate.

“Dropbox, [noreply@dropbox.com](mailto:noreply@dropbox.com). Please verify. Hi Helen, Dropbox needs to verify your email address before you can share folders.” Okay, legitimate. Yes, where it’s from, I mean, yes, a six.

Alright, “Blizzard Entertainment. [noreply@battle.com](mailto:noreply@battle.com), Diablo III account.” Hmm, “Greetings, it has come to our attention that you are trying to sell your personal Diablo III account. You may not be aware this conflicts with the EULA terms of agreement. If this proves to be true, your account can and will be disabled. It will be on-going for further investigation by Blizzard Entertainment’s employees. If you wish not to get your account suspended, you should immediately verify your account ownership.” Seems a bit bizarre alright.

“Please open this connection: us.battle.com.” It matches the email where it came from. \_\_\_[0:12:01]. “If your account passes the check successfully, we will send this package of dynamic battle.net mobile authenticator to you in the form of email.” I’m just going to say ‘definitely phishing’. I don’t think they do emails that check accounts. “In three days after you receive the email, if you don’t submit your information, we have the right to freeze your account.” I think this email just tries to scare people, so I think I’m just going to give it a one.

See, Barclays. “Dear Barclays account holder, from [support@vnet.com](mailto:support@vnet.com).” So, this a big red flag, and I would assume it would address you by your first name, because usually banks do that. “We have detected unusual activity on your account. We have decided to limit your account until you complete these steps.” Well, first of all, I would probably try to check my card and see if it works. I would say ‘definitely phishing’, because the email where it came from does not have the company name in it, so one.

Okay, “[service@paypal.com, approximating dz100@[manicmusic 0:13:38]](mailto:service@paypal.com,%20approximating%20dz100@[manicmusic%200:13:38])” or whatever. “I sent a payment of almost £150…” I would say it’s phishing, because… Let’s see… I don’t trust the email where it came from.

“Department of Psychology, \_\_\_[0:14:21] details.” Yes, where it’s from, that line doesn’t match. Give it a two.

Okay, “Your credit card has been suspended. Please update. Dear valued customer…” Again, not my name. “Your credit card has been suspended, as an error was detected in your credit card information. The reason for the error is not certain.” Well, you should probably know that, since, you know, you’re a credit card company, but let’s see though. Hold on. “Click here to lift the suspension,” no. “Security, don’t replied, verifiedbyvisa.com.” I mean, I should be able to reply and ask what’s going on. “It’s not certain, but for security reasons, we have suspended your credit card temporarily.” Okay, usually, I don’t think it would be temporary. I don’t know. I would probably get issued a new one, and there’s… Ah, I’m going to give it a three.

Okay, ‘thanks@virginmobile.com’, that’s, kind of, a funny email address. No name for attachment, 50kb, okay, sketchy. “The bill for your Virgin Media Mobile is ready to view. The balance is £16.94, will be taken by direct debit. Our team won’t be picking up emails from this address. Send us an email, link.” Three out of six.

‘slcdirectgov@slc.co.uk’, “Be safe this season, this is a message for all students receiving grants and loans from the Student Loan Company. We have detected fraudulent activities going on with Student Loan accounts. To allow us update our database, fill out your information securely.” ‘[mineface.com/components/com, content and views’ 0:17:21]. Definitely phishing, one.

“HSBC, World’s Local Bank: This is to inform you that the business account with us has been blocked for…” Oh, by the way, the last one, one of the sentences wasn’t written right, so yes, I don’t like emails with poor grammar, I suppose. Alright, back to this one: “This is to inform you that the business account with us has been blocked for receiving payments. An attempted error login was detected by our security system. This account will be disabled if you ignore this message.” Well, shouldn’t you disable it..? Or, how would they know if I ignore this message? “Please click here to begin. If you are not an authorised signatory, please forward to…” ‘Authorised signatory’. This is just asking for it. Yes, I think it… I’m going to give it a one, because yes, to me, I think this is just flat-out asking for personal information from whoever it is.

Okay, ‘noreply@accounts.google.com’, “Suspicious sign-in prevented. Okay, “Someone recently tried to use an application to sign into your Google account. We prevented the sign-in attempt in case there was a hijacker trying to access your account. Monday, 9th…” Ah, so 9th September, that’s the same day this email was sent, just about an hour after. ‘Location: Italy’. “If you don’t recognise the sign in attempt, someone else might be trying to access your account. You should sign into your account and reset your password immediately.” ‘Reset password’… This is you and you… Okay, definitely legitimate, yes.

‘Carla Craig’, “Item waiting on delivery today. Thank you for shopping with us, we thought you must be informed that we shipped your item and that this completes your order. If we need to return an good from the shipment or manager [the orders 0:20:21], please visit yours.” Okay, TV… What is it asking for me to do? Nothing? “If you need to return a good item from the \_\_\_[0:20:42], ensure your item is…” I don’t see anything wrong with this email. Well, actually now, “Item subtotal: £3.59. Shipping and handling: £15. Total before tax, shipment total…” Yes, the prices don’t add up, so I’m going to give it a one because of that. Yes, poor math.

‘Student Finance’, “This is a final notification of an important account update. Due to recent update in our database, we require all student to update their account information, to ensure you receive your scheduled payment, to avoid a mispayment. To update your account, click here. Please fill the requested information exactly as you filled it when you were signing up for Student Finance, or your payment will be suspended.” Well, I mean, that sentence… I’m sceptical of that sentence. Poor grammar, again, and the email address where it’s from, ‘Student Finance’ with an extra ‘E’. But it’s from Gov.UK though… I don’t like the ‘fill the requested information exactly as you filled it’, I just think, yes, I… It’s, kind of, too demanding. I’m going to give it a two.

‘ebayadministration@ebayz.com’, “Dear valued eBay member, we regret to inform you that your eBay account has been suspended due to concerns we have for the safety and integrity of the eBay community. If you could please take 5-10 minutes of your online experience to update your personal records, you will not run into future problems with the online service. Please update your records by 10th December,” which is today. I don’t think eBay would be like that. They would probably give you a week, real eBay would. “To update your eBay records, click the following link,” which starts with ‘cgi1’, and the, yes, ‘ebayz.com’ where it’s from, I would give this email a one.

Alright, ‘NatWest, ‘[uup@donkeytone.com’ 0:23:45], “Your online account will expire today on 3rd June.” Well, today is 8th October, so no thanks, that is a one.

“Facebook notification plus da, da, da,” ‘facebookmail.com’, never heard of that before. “You recently entered a new contact email address. To confirm your contact email address, follow this…” Okay, well it’s facebook.com… What? “Facebook email address confirmation. Due to new contact [add 0:24:32], \_\_\_ [contact] \_\_\_. If you did not enter this address, \_\_\_ your contact email to…” I don’t like where the sender of that email… I don’t see a logo or anything. I’m going to say give it a two.

“eBay invoice notification from Monday, July 15th.” ‘billing@ebay.co.uk’. “Invoice \_\_\_[0:25:17] eBay invoice, from June 16th to July 15th is now available. \_\_\_[0:25:27] deducted \_\_\_, to view your invoice, go to ebay.co.uk, My eBay, you’ll need to sign in.” Alright, that makes sense. “Click the seller account link under account \_\_\_, select the invoice your wish to view in the drop-down menu. eBay will not ask you for sensitive personal information in an email.” It’s not asking, you just have to go to the ebay.co.uk to sign in, so I will give this a six, definitely legitimate.

“Your password will expire in three days, click here, upgrade-webmail to validate your email.” For what, though? Like, this is from [‘sgranada@washcoal’ 0:26:21]. “Your password will expire in three days.” I don’t know which password you’re talking about, so I’ll give you one.

“Thanks, system administrator. Gary Cooper, subject: confidence. I’m Mr Gary Cooper, born here and there, medical institution in Italy, where I’m writing you. I’m suffering from lung cancer in terminal phase.” Oh. “Doctors have asserted that my days are numbered, I would like to kindly leave you my fortune to good use, especially for a charity, primarily to support to orphan…” Okay. “I have no heir apparent, my situation… I chose you as a trustworthy person, at least I hope…” Okay. “Add my on Skype.” Okay, so, “I count on your good faith to carry out this work and matter. Could you contact me your full name and phone number via email to complete the procedure? Waiting to hear from you.”

Okay, well, it’s not asking for any personal information, but the email address is a little bit weird, ‘GNB’. “Could you contact me your full name and your phone number via email?” Well, I just don’t want to get all these calls coming from random people. “I’m suffering from lung cancer in terminal phase.” I mean, not to be mean, but would you be able to write an email if you’re, like, in terminal phase right now? I’m not sure if you know me, so how would you..? I’m going to give it a two. It’s not one, because it’s not asking for really personal information, though.

Okay, ‘frank@easyroommate’, cool. “You’ve just received an message from Graham. Click here to see the message and profile.” Okay. ‘uk.easyroommate.com’. That is a long email, but there might be a lot of houses or something, and postings. “Click here to see the message and the profile. Hi Helen, you received a message from Graham.” It’s not asking me to do anything. The link is, kind of, too long to be normal, but what it starts with, ‘uk.easyroommate.com’, I’m going to give it a five out of six.

Alright, “A job which matches your alert criteria has been published on our website. Please can you paste into your browser… Job which matches your…” ‘i-grasp.com, www21…’ I’m going to give it a two, “A job which matches your alert criteria has been published on our website.” Hmm.

Okay, ‘i-offer, no reply’, ‘The History Man’. Oh, “Congratulations, you purchased an item on Googlebox.UK,” I can’t even see a picture of it. “You should receive an invoice with the payment and shipping instructions shortly. Made a mistake? Click here to cancel the transaction.” Well, I’m going to give it a one, because of all the missing images.

‘team@blackpoolpleasurebeach’, ‘suverys@aspectmr.co.uk’, “Dear Pleasure Beach visitor, thank you for visiting Pleasure Beach. Hope you enjoyed your day here. Everyone taking part will be entered for a draw. The information you provide us will only be used for search purposes.” Hmm, I would give it a four out of six. It doesn’t ask for any personal information, just to fill out a survey.

“DVLA, report and update required. We are currently upgrading our database and all drivers are required to update and verify their driver’s licence details. To complete your licence verification with us, you are required to fill out the form on the link below. Drivers that refuse to upgrade his or her details within two weeks of receiving this verification will lose his or her driver’s licence and have to take a fresh driving test.” I mean, I don’t think you would have to do that. “We sincerely apologise. Driver’s verification.” Hmm, I’d give it a two. I think you’d have to… Well, in America, where I’m from, you would have to go somewhere to update your licence.

‘rmalcolm@lancaster.ac.uk’, “Welcome to Lancaster, we hope you’ve enjoyed the first few weeks. Give us feedback, enter… Complete SurveyMonkey survey. The survey’s open to current first year undergraduates.” Yes, not sketchy at all. It’s from the Lancaster University email, six out of six.

**P351**

P351: ‘Your online account will expire today, on 3rd June 2013. To continue using your online banking please…”

[Break in conversation 0:00:06 - 0:00:18].

That one is a two, because I think that… Oh, no, it’s from some dodgy email, uup@ \_\_\_. That’s definitely phishing. Also your bank wouldn’t email you anything like that. They would phone you or send you a letter.

iOffer. ‘Congratulations. You’ve just purchased an item from Google [Books 0:00:49] UK, \_\_\_. You should receive an invoice with payment and shipping instructions shortly.’

That seems legitimate. The only problem is there are no pictures there, but if you did order that then you would know, and it’s from the same website, and the email seems legitimate. Yes, that one seems fine.

[Break in conversation 0:01:22 - 0:01:34].

[Caxton FX Cards]. Email is legitimate enough. ‘Changes to the terms and conditions of your prepaid MasterCard.’

I would say that one is legitimate, because it’s not asking you to put in any information. There are numbers there. That’s a legitimate email. If you did have one of those cards then you would know, so I would say definitely.

[Student update 0:02:10]. ‘This is a formal notification of an important account update.’ That one, see, the text is a little bit informal, like someone has wrote it in Word and pasted it in. ‘Due to a recent update of our database we require all students to update their account information.’

However, it is from direct.gov.uk. Oh, no, it’s Student Finance E. No, that one can’t be legitimate, because the email address isn’t right, and there’s no other information. It just looks like someone has typed it in. [If it had been an 0:02:55] official thing…

‘Your password will expire in three days. Click here’ (Laughter) – on the dodgiest looking web link – ‘to validate it.’ No, you wouldn’t get that from a system administrator. You would get that from the whole university thing. That one is not legitimate.

Barclay’s Online. ‘Dear Barclay’s account holder, we [have detected 0:03:27] unusual activity from your account.’ Support@vnet.com is the email address, and once again with bank things they rarely email you. I think they only really email you to sell you things.

Service@PayPal. (Laughter) [Approximatingdz100@mancmusic 0:03:55]. That one seems absolutely fine. That’s a PayPal email. If you know that you sent that, to buy a pro-diver chronograph – oh, it’s a watch – then yes, that’s completely legitimate. That’s how PayPal emails look. Yes.

Plusnet support. support@plus.net. ‘Your Plusnet Protect software is available to download. Dear Miss Jones, account username…’ That one seems fine. The only problem is that it’s McAfee, which is awful, and I would delete that but if that’s what you want then that looks like a legitimate email. (Laughter)

Service@paypal. No that one is fake. Oh, no. I can’t tell. Because it was from paypal.co.uk. That looks really fake, but maybe they're just on HTML email or something, so I don’t know. I would click on the update card link, and I would see how dodgy the web link looked. I'm going for a four for that one, because I'm not too sure, just because of the font.

Onlinebanking@information.natwest. ‘Your latest statement is available.’ Yes, that one seems fine. It even says, ‘The account ending in 801’, so if you knew your account number then you should be able to recognise that.

‘Dear valued customer, thank you for your Dell support regarding…’ Oh, yes. That’s fine. Someone has bought something from Dell, and they want them to do a survey. That one seems fine.

EBay suspension. ‘Dear valued eBay member…’ Admin@ebayz.com. That is definitely phishing. Safe Harbour Department. That’s not a real thing. ‘[Per the user agreement we issued 0:06:55].’ No, that’s not. No, that’s definitely phishing. Also, the eBay date thing only goes up to 2005 on the bottom of the email, and it was received in 2012.

Gary Cooper. ‘Hello. I'm Mr Gary Cooper, and was born on…’ (Laughter) From a medical institution in Italy. ‘I am suffering from lung cancer.’ Oh, no. Poor Gary. ‘I choose you as a trustworthy person.’ Yes, definitely phishing. Of course. Although you can add him on Skype, which is a nice touch. (Laughter)

‘Suspicious sign-in prevented. Download attachments from Gmail.’ Usually when you get these they are you signing in abroad, or from somewhere you don’t usually visit, so you would know. Accounts.google.com. No, that one is legitimate.

[Break in conversation 0:08:15 - 0:08:28].

[Philippe Boucheron]. This one, without even reading it, is going to be fake. ‘All we need now is £1,850.’ Yes, definitely phishing.

Create a new password, NUS Extra. That’s the National Union of Students. ‘You entered this email address to change the password.’ Well, if you knew that you had wanted to change your password, then yes, that’s fine. @nus.co.uk. Yes, that’s fine. That’s legitimate. A big long link that’s specific to you as well.

@e.paypal.co.uk. PayPal. ‘Login see your monthly activity and recent transactions.’ Oh, that one is tricky. That one has got a lot of things that say, ‘How do I know it’s not a phishing email?’ Which makes me want to believe that it is a phishing email. (Laughter) @e.paypal.co.uk. I'm going to go with five on that one, because I'm not too sure.

Ebay invoice notification, \_\_\_[0:10:09] ebay.co.uk. ‘Your invoice from the period 16th June 2013 to July 15. Amount due [£2.79].’ (Laughter) Yes, there are no links to click on or anything. It says, ‘Go to ebay.co.uk’, so it’s not trying to scam you. That one is definitely legitimate. Automatically generated too. That’s fine.

‘Regarding item waiting on delivery today.’ That will have been something that you or they put in, like a message on Amazon. Shipping confirmation, Amazon.com. It doesn’t say the email address that it’s from, but it’s an email address from someone you already have, so that’s absolutely fine, and you would know if you had bought a big TV, so it’s obviously not going to be a scam. What else does it say? ‘Please visit ‘Your Orders’ at Amazon.com.’ Yes, that’s fine. Maybe. Yes, definitely legitimate.

ioffer. ‘Dear guest user, you have received a payment regarding the item…’ Well, ioffer sounds like a dodgy website already, but it was in the emails before, so you would know what it was you were buying. Yes, ioffer.com. If that’s a legitimate website, then that’s fine. Six.

Dropbox. ‘Hello, Helen. Dropbox needs to verify your email address before you can share folders. Please verify the email address by clicking the link below.’ \_\_\_[0:12:00]. Yes, that’s fine.

Gucci, Cartier, Rolex. ‘Get ready for your luxury…” That’s definitely phishing.

‘Yahoo and Gmail user, click here. Good day. Give your loved one…’ Yes, definitely phishing.

Adobe Customer Care. Mail.adobesystems.com. ‘Important password reset information.’ Why have they reset your password? Did that happen? Did Adobe get hacked? Adobe customer care. \_\_\_[0:12:41]. Oh, if that one is phishing it’s very well done. ‘As we announced on 3rd October 2013.’

Yes, they must have had some kind of break-in, because that was probably around the same time that a load of other companies got hacked as well, so that’s a six.

‘Hi, Helen. You have just received a message from Graham, an EasyRoommate member.’ I don’t know what EasyRoommate is. The subject is ‘You have mail!’ And it’s from Frank, even though you received a message from Graham. I'm giving that one a two, because maybe some people do sign up to EasyRoommate.

‘Please do not reply to this email. Follow the link below into your account to reply.’ No, definitely phishing. That’s not… ‘Beware of scams.’ No, it doesn’t seem legitimate.

SLC.co.uk. ‘Students, be web safe this season!! We have detected fraudulent activities going on with…’ Yes, that’s definitely phishing. ‘Yours sincerely, Student Finance England’, from SLC. It’s not even from direct.gov. It’s direct.gov@ somewhere. The two exclamation marks give it away as well.

Blizzard entertainment. Are they the World of Warcraft people? ‘Greetings. It has come to our attention you are trying to sell your personal Diablo account \_\_\_[0:14:20]. Please open up this connection. If your email account [passes checks].’ Hmm.

[Noreply@battle.com]. That seems like the kind of thing they would have as their email. ‘It’s come to our attention you are trying to sell your personal…’ Us.battle.com. See, that’s not a scam website. That’s kind of… I'm going to go for a five, because I'm not sure what their emails would be.

HSBC. ‘Incoming funds blocked’, in dodgy Arial font, and a copied and pasted logo at the top. ‘Click here to begin to resolve the issues.’ That one is definitely phishing. Anything from a bank seems to be phishing. ‘Incoming funds.’ Oh, no.

[Break in conversation 0:15:26 - 0:15:36].

[Nonameforattachment.zip]. Your mobile bill sent as a zip file.

[Break in conversation 0:15:43 - 0:15:55].

Oh, I don’t know. No way do they send zipped files with your… No, that one is definitely phishing, because they wouldn’t send a zipped attachment.

Jobalert@igrasp.com. No, that one seems legitimate. ‘Good luck with your job search’ at the bottom. I'm going to go a four on that one, because I don’t know if that’s real.

Priority mail postal service from FedEx. That’s not the FedEx logo. ‘Your parcel has arrived [at our post centre 0:16:56].’ No, that one is really dodgy. FedEx never do that. It’s not even from a FedEx email address, from Fort Wayne. I don’t know. That’s definitely phishing. It says, ‘Your package has been delivered’, and then, ‘Oh, we couldn’t deliver your package’, on the same line.

Facebook contact email address information. ‘You recently a new…’ See, it links to facebook.com. I don’t know that Facebook send out emails with their logo on them though. ‘If you did not enter this address as your contact email please disregard this message.’ See, I don’t think they would have that if they wanted to scam people, so I'm going to go with legitimate on that one.

[Security verifying by Visa 0:18:05]. ‘Dear valued customer.’ No, that’s definitely phishing. ‘Lift your suspension.’

Job application form. ‘Dear applicant, click here to download application form.’ What? @yahoo.co.uk. That’s not real. No, definitely phishing.

‘Dear Pleasure Beach visitor.’ Oh, delightful. (Laughter) ‘Thank you for visiting Pleasure Beach Blackpool. Hope you enjoyed your day here.’ See, that seems absolutely legitimate, yes. [SSKH 0:19:00] at the bottom. Yes, that’s legitimate.

DVLA. ‘We are currently upgrading our database, [trying to] verify [their] driver’s licence details. Complete your licence verification [by filling in the form linked below 0:19:20].’ It’s from dft.co.uk. I'm sure there was another one a few emails back from them. ‘Drivers that refuses to upgrade his or her details’ – all the typos make it just really obvious – ‘will have to take a fresh driving test.’ (Laughter) Definitely phishing.

‘Dear student, welcome to Lancaster. We hope you have enjoyed your first few weeks at university. We’re interested to find out why you chose Lancaster.’ SurveyMonkey, that’s fine. Ross Malcolm. I don’t know who he is, but he’s probably a real person from 2013. Definitely legitimate. Yes, that’s fine.

**P352**

P352: ‘No-reply’ or, what is that? ‘NUSextra.co.uk’. ‘Create a new password at NUS Extra to…’ blah, blah, blah. ‘You or someone else entered this e-mail address to change your password.’

Can’t stop. ‘To continue your password reset process, please progress to this link. This action was requested from IP…’ blah blah, blah. \_\_\_[0:00:34] here, blah, blah, blah.

I would say definitely, ‘Introducing \_\_\_[0:00:44] password…’ It looks like quite, ‘NUSextra.co.uk’. Hmm.

[Break in conversation, 0:00:59-0:01:13]

Very, I’m not sure. Confidence. \_\_\_[0:01:21] blah, blah, blah. I don’t give her. \_\_\_[0:01:28-0:01:41]. I don’t give her, so bye bye.

Okay, so here, ‘Verified by Visa’. ‘Verified by Visa.com’. ‘Your credit card has been suspended, please update.’ ‘Your credit card has been suspended as an \_\_\_[0:01:58]. Click here.’ Bye-bye, I don’t believe in you.

Philippine. ‘Sad news’. ‘I’m sorry to wishing you to relate to you this situation. My family and I was trapped.’ I don’t give a… Bye-bye.

Hello, there. No. It’s HSBC, the world’s local bank. ‘This is to inform you that the business account with us has been blocked for using payments. Any time error…’ ‘If you act now, please click here to begin to reset the user.’ ‘If you are not an authorised signatory, please forward to the…’ blah, blah, blah.

Let me give some thought. ‘This is to inform you that the business account with us has been blocked. It has been blocked from receiving payments. And attempt at your university was detected by the security service on this account. If you ignore this message.’ (Laughter) ‘If you ignore this message, this account will be disabled.’

Come on. It should be disabled, even if I don’t ignore this message.

Dropbox. ‘Hi, Dropbox are referring your e-mail address, where you can share photos. Please verify your e-mail address by clicking on the link below.’

There should be another link besides, below, verifying your e-mail address, but as I remember, do I need to verify my e-mail address for using Dropbox? I don’t think so. I don’t think I need to verify. I just simply sign up for one. So I think that’s a faulty one.

Hmm. I just think, hmm. Did I need one?

[Break in conversation, 0:04:41-0:05:04]

Hmm.

[Break in conversation, 0:05:06-0:05:23]

Okay. Definitely phishing, I think. It takes ages for me to do this spreadsheet.

‘Important password reset information. Vital…’ I never use Adobe. ‘If you received this message, we recently discovered that an attack…illegally…your accounts…if you…if you need to reset, please visit Adobe Go password reset, underline UK, to create a new password. \_\_\_[0:06:04-0:06:10]. We apologise for any inconvenience.’

This one I didn’t even get.

[Break in conversation, 0:06:17-0:06:30]

‘Dear eBay valued user. We regret to inform you that your eBay account has been suspended due to…’ ‘In agreement with section nine’, urgh, okay. ‘We may also take this action when required…’ ‘It could take up to five days…’ ‘Once you updated your eBay it will not be…’ ‘To update your eBay records click the following links.’

Mmm, but is that? ‘Your action may cause…’ Hmm. Oops, that’s weird.

‘Thank you for your recent contact with terms regarding case number…’ ‘At Dell, we are committed to deliver the best customer experience…’ ‘Your valuable feedback…’ The pitch.

‘To compare the software, please click on the address below by…’ ‘If that doesn’t work, please copy and paste the entire address to your browser.’

‘This will only take about five minutes to complete.’ Hmm, the link looks so weird. \_\_\_[0:08:15]. Phishing.

[Break in conversation, 0:08:23-0:08:35]

So, ‘Advanced payment.com.’ ‘If possible…’ What is this? I cannot go back. No. Alright. ‘Service@paypal.com.’ ‘Reset for your PayPal payment.’ ‘Thanks for using PayPal, this is…’ ‘You sent…’ ‘Sell the…’

‘Note to seller…’ ‘Thanks for using PayPal…’ ‘User ID…’ Mmm-hmm.

‘No-replay@batter.com’. ‘Greetings, it has come to our attention that you are trying to sell your personal Diablo 3. As you may not be aware of this conflict with the terms of agreement…’ ‘If this proves to be true your account can and will be disabled…’ ‘Bear ongoing for further investigation…’

‘If you wish to not get your account suspended, you should immediately use the verifier account ownership.’ This is so phishing.

‘Your password will expire in three days.’ Phishing.

‘Non-reply@concirclegroup.com’ ‘Today you signed to…’ ‘Hi Helen, someone’s tried to…’ ‘Account with your…’ ‘Someone may try to…’ ‘You should sign into your account and reset…’

‘If this was you and you’re having trouble accessing your account, complete the…’ ‘In case it’s hijacking.’ ‘This IP address, location.’ ‘You signed into this account and reset…’ ‘If you do not recognise this sign-in attempt someone else may…’

Sorry, I have one of these e-mails. I received one of these e-mails before, as I remember. Hmm. This is so similar. I’m not sure where.

‘Someone recently tried to use an application to sign in to your account.’ ‘If you tried to sign in,’ ‘Determined this is hijacking.’ ‘If you do not, someone else may try to…’

Hmm.

[Break in conversation, 0:11:58-0:12:59]

Not sure.

‘EBay Invoice.’ ‘Your message accrued from eBay…’ ‘Do not replay invoice.’ No. ‘You have set up eBay’, blah blah. ‘People that use e-mail…’ ‘Your account will be checked…’ Hmm.

‘There are months…’ ‘May be reset…’ ‘If you feel your invoice…’

I think it’s true. Right now, I think. They didn’t ask me to reset my password or whatever, and the link seems real.

‘Hello. Thank you for shopping with us.’ Oh, it’s just… ‘To inform you that…’ ‘This send you…’ ‘.com’. Hmm.

‘And that completes your order.’ ‘If you need to return these goods…’

‘Your card is about to expire.’ ‘We noticed that your…’ ‘Ending in 1234 is about to expire.’ ‘Please obey your card.’ ‘SNS for…’ ‘Option.’ ‘Ensure you…’ ‘Your bank first.’ ‘Update card.’

‘If you have received a new card, please link the card. If you have already updated your PayPal account with your new card’s details, please disregard this e-mail.’ This sounds, it doesn’t look fake from the e-mail. ‘Service@Paypal.co.uk’.

Hmm.

[Break in conversation, 0:15:31-0:15:50

Hmm. I think it’s a real one.

‘You have mail. Hi Helen, your…’ ‘CMS.’ ‘Please do not reply.’ ‘If the link does not work.’ ‘Please reset your number.’ ‘Easy Roommates.’ ‘You have been receiving an e-mail from Guy.’ ‘If the link above does not work, just copy and paste or give Easy Roommates a call.’

Mmm. It’s similar to an e-mail I received.

‘Actuary Recoup Department.’ ‘Thank you for your interest in our new role we have.’ ‘I would like to let you know we have carefully reviewed your CV and regret to inform you…’ ‘We will be interviewing candidates in the next few weeks…’ ‘You may hear from us then.’

‘My name is Anna Freisian, I am in HR.’ ‘We give a trial…’ ‘It will be 48 hours…’ ‘The tax application form…’ ‘Can clear to Dan O.’ ‘Please double click the application form to be able to open the file and fill in the application form.’ ‘If you have any queries, don’t hesitate to contact via e-mail.’

Oh, that’s a tricky one, but wait. ‘HR@Yahoo.co.uk’, excuse me. Who’s still using ‘@Yahoo.co.uk’ as a business account?

‘NatWest’. ‘On our banking information.Natwest.com’. ‘Your latest statement is available online.’

‘Hi, your latest statement is…’ ‘You just log in and say “Natwest”.’ At NatWest, mmm-hmm.

We’re just halfway. It’s a long hour.

‘Dear Candidate, a job which measures,’ ‘Alert has been completed on our website.’ ‘Please use a foreign link.’ ‘Vacancy reference below.’

Mmm-hmm. ‘The product of 21, though.’ 21 or something. I don’t like the link. ‘If you measure alerts.’

‘Noreply@I-over.com’ for I-over mail.com. The Haitian man. ‘Congrats! You just purchased an I-term from Googlebox UK.’ ‘Invoice sent.’ ‘You should receive an invoice with payment…’ ‘You can mistake here.’ ‘You can see the transaction.’ Hmm.

‘I-over’. ‘From Googlebox UK.’ Mmm. Not sure. Put a ‘Three.’

Alright, ‘Hey, e-mail postage surfers…’ What is this e-mail address? Come on, man. ‘Your browser has a…’ ‘so we should deliver.’ Phishing, bye-bye.

‘Support@Vnet.com’. ‘Cause at…’ What? ‘SUT3.co.uk?’ ‘SUT3.co.uk?’ ‘Changes to the terms and conditions for your cotton?’ ‘Of XP-paid Mastercard.’ ‘We recommend that you keep the updated terms for your records.’

‘See if it helps.’ ‘If you have any questions about our updated service…’ Mmm-hmm. Hmm. That’s not sure. Not sure.

‘I-offer’ again. ‘We have received your payment.’ ‘Click here to fill the statement of your purchase.’ Thank you.

But why ID is ‘It comes to $15’? Hmm. So, blah blah, question mark, and user ID goes to…

Hmm. This is different, as it’s 41.

‘PayPal@E.paypal.co.uk’. ‘E.paypal.co.uk’. Hmm. ‘View your recent transactions now.’ ‘Use your…’ ‘Dollar-free step.’

[Break in conversation, 0:22:58-0:23:09]

Hmm. ‘E.paypal.co.uk’.

[Break in conversation, 0:23:17-0:23:29]

Oh, yes. I have no idea what is this e-mail address. ‘Thanks@VirginMobile.com’. ‘Thanks@virgin’ No name for attachment. ‘Virgin Media to fail.’

[Break in conversation, 0:23:50-0:24-06]

No name for attachment. What’s that? Facebook. ‘Facebookmail.com’. ‘I recently entered a new contact e-mail. To confirm your contact e-mail address, click the link below.’

Hmm.

[Break in conversation, 0:24:24-0:24:54]

‘From the Support at Plus.net.’ ‘Your Plusnet purchase offer is available to download.’ ‘Support@plus.net’. ‘Thanks for choosing your plus…’ ‘Following your instructions, what to do…’

Mmm. I’m already asleep here.

‘StudentFinance@direct.government.uk’. ‘Student update’, mmm-hmm. ‘An indication due to a recent update, we require all students to update your account information to transfer you.’ ‘Reserve your schedule to update your account information. Click here.’

‘Plus field requires the information exactly as you filled it in when you were signing up for student finance, or your payment will be suspended because of a failed account verification.’

I’ve never received any student direct e-mails, but it sounds so phishing.

Mmm-hmm. ‘The website…’ ‘Student loan company…’ ‘We have contacted…’ ‘To allow us to update our database…’ ‘For your information securely.’ ‘You can do this by clicking on the link below.’

‘Team@blackpoolpleasurebeach’ ‘Dear Pleasure Beach Visitor’, ‘Pleasure survey’, ‘Thanks for visiting…’

Mmm.

‘We hope you enjoyed your day. The information gathered will be crucial to the park. We are very grateful if you can…’ ‘Any information you provided…’ ‘Our section…’ ‘Yours sincerely, Pleasure Beach, Blackpool team.’

It sounds normal, but the e-mail is quite weird, but anyways. Alright.

‘DVLA’. ‘Info@DFT.co.uk’. ‘We are currently upgrading our database.’ ‘To complete your licence preparation, we require you to fill in the link below.’

[Break in conversation, 0:27:55-0:28:05]

I will have to take the first drive attached. (Laughter) It’s crazy.

But, for ‘DFT.government’, hmm. But it’s so, hmm. It looks so normal, but the e-mail, the link, especially it’s ‘www.dft.governent.uk.’ But the content is quite nonsense, because if I just missed the e-mail then I just lose my licence? That’s just nonsense.

So I say it’s a phishing e-mail.

‘For the health service and technological survey.’ ‘Welcome to Lancaster, we hope you enjoy. We’re interested to find out why you choose, and how you find the admissions process..’ ‘To give feedback, just,’ blah, blah, blah. ‘Please give in surveys only if you’re a first-year.’ ‘If you have any queries, please contact.’

That is the kind of e-mail I always received.

**P353**

P353: I think this could be legitimate, because the email address seems to be fine. Like, it’s @dropbox.com. Yes, it seems to be fine, I think, but it could be… No, so I’m going to select five. Okay, I think this is definitely legitimate, because it doesn’t ask you to do anything. It just says that you should go to the website and then you can view the invoice. Yes, it seems to be really fine, so I’m going to select six. So, I’m not sure, like, at first it seems to be fine, but the last sentence, “We’ve prevented a sign-in, attempted case, this was a hijacker trying to access your account.” This sentence brings doubt to me, but other than that, it seems legit, and the link that is an email also seems to be from Google, so I’m going to select five.

Okay, so the email address that this email’s coming from, \_\_\_[0:02:39] [@mail.2.rap], bla, bla, bla seems really dodgy, so I initially wouldn’t trust that. Also, the link that’s linked in the email is really weird, so I would say this is definitely phishing. Okay, here again, it seems to be from [service@paypal.com](mailto:service@paypal.com), but I think it is actually from approximating these [100@mencamusic.com], so that’s definitely an indication it is phishing. Oh, but maybe that’s the seller. Okay, I’ve never used PayPal on eBay, so I don’t know how emails are supposed to look like. Yes, so I actually think this is really legitimate, yes.

Okay, the email address in the next one is ‘Student Finance’ with two Es, so this seems to be weird. Then, the syntax is really bad in the email. For example, they have a sentence, “To update your account information. Click here to validate your information,” then ‘we’ is also capitalised. Oh, this is definitely phishing. Also, the next sentence, it has a dot between ‘finance’ and ‘or’, so yes, I will select, definitely, phishing.

Yes, I think this is phishing, because, I mean, I don’t know, ‘iOffer’, I don’t know anything about this website, but it says that you should receive with payment and shipping instructions, and then made a mistake, “Click here to cancel the transaction,” so that’s the link they want you to click on. I think you should get this email, maybe you didn’t order it, so you would probably click that you made a mistake, and then they have you… So, I’m going to say ‘definitely phishing’, but I’m not actually sure.

Okay, it seems a little bit weird, because it just says ‘hello’ and then, like, no name or anything. Then the last sentence is also pretty weird, with the, “So, if you’d like to email us back, head over to our website.” It’s also pretty informal, because it uses ‘won’t’ and ‘you’d’, so I think this is phishing.

So, it says it’s from Barclays Online, but then the email address is called ‘support@vnet.com’, which is weird. I mean, from the email content, it seems to be fine, but it’s weird that the email from Barclays would come from ‘support@vnet.com’, so I wouldn’t trust that, I think. Yes, I think they would have another email address, so I would say ‘phishing’.

Oh, this is definitely phishing. First of all, the email address, and then how it’s written, like, “Good day, give your loved one a luxury watch today. Good luck, click here.” There’s not much content, they just want you to click on the link, but that’s actually really obviously, so it’s a phishing…

Okay, so, like, the email address seems to be fine. ‘Verified by Visa’, okay, but then ‘Credit Card’ is capitalised, ‘Valued Customer’ as well, ‘Suspend’ is capitalised. Okay, this is probably phishing. I don’t think that they would send you something like this, so I will select ‘definitely phishing’, but now I’m wondering, that some of these might actually really [do this 0:11:42]. I selected ‘phishing’.

Okay, so there’s a ‘paypal.co.uk’, seems fine. What makes me wonder is that, “If you’ve already updated your PayPal account,” like, the abbreviation… Hmm, this is a tough one. Yes, there’s just one thing that makes me wonder, and that’s the “you’ve” part, so I’ll select four.

Okay, the email address in the next one is really weird, [“[dtf.193@fortwayne.com](mailto:dtf.193@fortwayne.com)” 0:13:22]. Then it says, “At December 7th”, which is wrong. Then, they have no space between the dot and R, [postwriter]. Then, they say, “Go to the nearest [R Office] and show this \_\_\_.” Okay, this is definitely… So, I will select one.

Okay, the email address that it’s from is “[admin@ebayz.com, ebayz](mailto:admin@ebayz.com,%20ebayz),” so it makes me wonder if this is phishing. Yes, the link that is linked in the email is really dodgy, so I would say this is definitely phishing.

With this one, I’m not sure, because it seems to be fine. The links seem to be okay as well, so I think I’m going to select six, yes.

This is a weird email address, [“hrdeck33233”], then there’s the first sentence is really long, and there should be two sentences instead of one. ‘CV’ is not capitalised. Yes, this is phishing, definitely, how they link the… They put all the… I don’t what it’s called, the arrows, so yes, I will select ‘definitely phishing’.

“HR recruitment team…” Hmm, the links in the email are a bit weird, especially because it’s [“www21.ires.com”]. Never seen a website like this, so I will say it’s phishing.

Okay, it’s weird that it says it’s from [“[cars@caxtonfx.com](mailto:cars@caxtonfx.com)”], which would be good, but then it’s via “z3.co.uk”. Then, I think it’s weird that they have another email address, like “caxtonfxcar.com” instead of just “caxtonfx.com”, but I don’t know if that’s okay or not. I’m not sure about this one, I will say three. No, actually maybe I will say two, because something is weird about this email.

This is definitely phishing, because it comes from, like, a [new video shown 0:20:04], \_\_\_. Then, yes, no. I will say that’s phishing.

Hmm, okay, now this is definitely weird, because Facebook doesn’t send these email addresses, so I’d say it’s definitely phishing. Also, the email address seems weird.

Here, it’s really weird that it comes from Carla [Craig 0:21:24] instead of Amazon. The email is written in really bad English, for example, “This shipment have no associated delivery tracking number.” Then, “We thought you must be informed that we shipped your item and that this completes your order.” Yes, I would say it’s phishing.

Hmm, with this one, I’m really not sure. What is weird, that it says, “Calls may be recorded” at the end, and, ‘logon’ is written together, but I’m not sure how you write that, actually. It thought it’s two separate words. The links seem to be fine, but they also don’t have ‘www’ in front of them, so I’m not sure. They always have a link to contact us. I will say it’s probably phishing, I will select two.

Here, the next email address is ‘e.paypal.co.uk’, which is weird. I think it is phishing, because it says twice in the email, “[However 0:24:14], this is not a phishing email.” Yes, ‘e.paypal.co.uk’ is just a weird email address, so no. I will say it’s phishing.

Okay, this is definitely phishing, because a bank would never send something like this. No, it’s phishing.

[‘easyroommate.com’ 0:25:14]. The link in the email is really weird, but they really want you to click that link. Yes, I would say I will select… Yes, I will do ‘phishing’.

Okay, they ask you to pay something. That’s definitely phishing. Yes, I’ve had emails like this as well, so yes, I never trust them like this.

“In the form of email” is a really weird expression. “We have the right to freeze your account,” okay, yes, that’s phishing. It’s really unprofessional.

Yes, this is phishing, because it is supposed to be from Student Finance England, but then the link says, [‘manface.com’ 0:28:12], so this is phishing.

Hmm, I’m not sure. I think it’s phishing, because the email is [‘email@mail.wsims.com’ 0:29:28], and I think they wouldn’t have an email address like that, but it still sounds fine. Yes, I think if you click on the link, they might get your information, and then they want you to go to a new website to change… Same user ID or password, so then they will have your information as well, so I will say ‘phishing’.

This is iOffer again, and I don’t know anything about that. I will say three, because, hmm… Maybe… Yes, I will say three, I don’t know.

‘Mobile banking team’ is… Okay, just realised that the email address is really dodgy, so this is phishing.

Okay, this is definitely phishing. He just wants to get the money, yes.

Wow, this is a long link. Huh, the link makes me really wonder, so I will say one.

Hmm, I would say if, like, it says it’s from the Blackpool Pleasure Beach team, but they link… It’s also from another email, [‘AspectR’ 0:34:26], and the link is also for a website called ‘AspectR’ as well. I don’t trust that.

“Licence of \_\_\_[0:35:01]” is capitalised. I’m not sure if you actually do that. Oh, ‘inconveniences’ is misspelled, so I will say ‘phishing’.

Okay, so I think that should be fine, because I’ve used ServerMonkey before, and, I mean, yes, I think this is legitimate.

**P354**

P354: Well, \_\_\_. First we see that the email has come from account administration \_\_\_ Blizzard Entertainment, and sent from the [noreply@battle.com 0:00:21]. I don’t think it is – it is not legitimate \_\_\_, and it wants me to open a connection. I don’t think it is legitimate, because the connection may have some of my information, and password, stuff like that. I think two would be right.

Barclay’s. Well, the sign of Barclay’s is alright, but it is from [support@vnet.com 0:01:08], so it is definitely not from Barclay’s, so it is not legitimate.

eBay invoice notification. Well, it sounds like it is from eBay, because it is billing@ebay.co.uk. I think it is right, but let me see the amount due and see the invoice. Okay, \_\_\_[0:01:47] and copyright. Okay, I think it may be legitimate, because it may be automatically generated, but if I have not ordered anything from eBay it is definitely illegitimate. I think I will go into the link and see. If it requires a password [then I won’t 0:02:25] see it is legitimate, so two would be right.

Next one. Okay, Dropbox, noreplydropbox. ‘Please verify your email address.’ I think it is not legitimate, if it \_\_\_[0:02:54] I don’t think so. I think the sign will be right. Okay, so, three or two? Okay, two would be right.

Next one. Noreplyaccountsgoogle.com. Suspicious sign-in prevented. ‘Someone recently tried to use an application to sign in your Google account. Reset password.’ If I have signed into my Google account previously I think it is legitimate, but if I haven’t maybe there is something wrong with that account. I think this one may be legitimate. Okay, five.

PayPal. Wow, I got a lot of PayPal emails. Approximating \_\_\_[0:03:54] [100@mancmusic.com]. [Service]. I don’t understand the approximating – this one is so long, the email address. So, \_\_\_[0:04:19] shipping address unconfirmed. First of all, I will look at the shipping address, if it is the true address of mine, and also the account maybe. Yes, I think it is legitimate, because the size and the email address, so maybe five.

PayPal. [paypal@e.paypal.co.uk 0:04:54]. Well, this one obviously is legitimate. No, I don’t think it is legitimate. Okay, two. Because the picture it shows me I don’t think it’s the right website.

‘Congratulations. You have just purchased an item from Google [Books 0:05:24].’ [iOffer]. Oh, from the email address I think it is not legitimate, obviously. Okay, one.

‘Your card is about to expire.’ PayPal again. I think the address will be right. ‘Update card.’ This one is legitimate. Five.

[Caxton 0:06:00]. I've never heard of it. Cards. Pre-paid MasterCard. From the address, from the email address, I don’t think it is legitimate, because it is not the official email account, so, yes, one.

‘Your password will expire in three days \_\_\_[0:06:35].’ No, I don’t think this one is legitimate.

HSBC. \_\_\_[0:06:50] [hsbc-business.co.com]. ‘This is to inform you that [this account with us] has been blocked.’ Well, it is weird, because it’s only got a sign on the top, and also the email address is not convincing, so, one.

Dell. Dellsurveyhelp@mailto. No, no, no. From the email address, it is definitely illegitimate.

FedEx. No, it is not legitimate, from the email address. One.

[Direct.gov 0:07:58]. ‘This is a formal notification of your [important] \_\_\_. Please do not…’ Well, first of all I think this one is not legitimate, because the Student Finance email address seems not to be the official one, not the right one, and ‘Please do not reply to this email.’ I think it is weird you have [the stars 0:08:33]. Yes, so, this one is one.

‘Yahoo and Gmail user, click here. Good day. Give your loved one…’ Actually, no, I don’t think this one is legitimate, because the email address is not right. Also they don’t have the sign for Yahoo and Gmail, so, one.

NatWest. ‘The latest statement is available online.’ I think this one is legitimate, because the email address is right, and also they have got the sign for NatWest, and the links and the content. I think it is legitimate. Six.

The other one, [noreplyioffer 0:09:28]. ‘Dear guest user, [has] received your payment.’ Well, I don’t think this is legitimate, because [of], ‘The status of your purchase.’ It’s weird to have the \_\_\_[0:09:48], because I think once I have clicked on the link there will be some malicious virus to get my password. No, I will choose one for this.

No reply [NUS Extra 0:10:06]. ‘Create a new password.’ [NUS Extra]. This is definitely for a, [NUS Extra] card, but I don’t think it is legitimate, because the email address seems to be the right one, but the link \_\_\_[0:10:32] that is not fully represented. ‘Enter this email address to change the password.’ Okay, I will choose four [or] two. Two it is.

NatWest \_\_\_[0:10:54] account. No, this is definitely not legitimate, because the email address is not right.

Direct.gov. ‘Message for all students receiving grants or loans.’ The letter is quite short. It doesn’t have any images. It’s only got a link and stuff like that. So, I guess this is not the right one. Maybe one. One it is.

HR Recruitment Department. That contains his \_\_\_[0:11:54], but the information is quite [weird]. HR Recruitment, but this is not an official account, by accounting or something like that, it is a private account. I don’t think the HR department will actually give a private account. ‘Attached the application form, along with directions.’ \_\_\_[0:12:30]. You know what? I think this one is a little confusing. I will choose four.

[Email@mail 0:12:49]. Adobe Systems. This is something about Adobe products, information password reset. I think the email address is not right. Yes, okay, three.

[P.voltron@btinternet.com 0:13:13]. This is for what? ‘\_\_\_[0:13:24 - 0:13:31] [travel experience is a good thing], but the truth is all we need is £1,850. I promise to refund you in full as soon as I return home, hopefully tomorrow or next.’

Well, this is a guy who \_\_\_[0:13:57] this email to \_\_\_ as to get some money from me, and this is for not a small amount of money, and his email address is a little weird, because it has @btinternet. It’s not like a private account. Yes, I will choose one.

Plusnet Support. The account username seems to be the right one. ‘[What to do 0:14:41]. Need help? Need more help?’ Okay, from the email address I think it is the right one, several links. [It’s got no sign], but I have the intuition that it is legitimate, so five it is.

Gary Cooper \_\_\_[0:15:07]. Gary Cooper \_\_\_ from Gary Cooper. ‘\_\_\_ [assume the] management of this fund. Could you contact me with your full name and your phone number via email to complete the procedure?’ This one is tough. Well, I don’t think this one is legitimate. The email address is a little bit weird, I think, so two it is. Okay, one it is.

[HMPS 0:15:55] Recruitment. A job. Okay, [because the] \_\_\_ to cancel job alerts [HR Recruitment, i-grasp]. It’s a little weird, but I think [the account is right 0:16:19], so maybe three.

Security, Verified by Visa, [noreplyverifiedbyvisa]. This one is not legitimate, obviously from the email address, so two.

EBay Administration. To update your eBay \_\_\_[0:16:47] [adminebayz.com]. One, there is a Z behind the [email, behind the eBay]. It seems not the official one. It doesn’t seem to be the official account. Okay, I will choose one.

Frank EasyRoommate. ‘We just received a message from Graham, an EasyRoommate member.’ [The link 0:17:26]. ‘Do not reply to this email. Follow the link below your account to reply. [We are committed] to help you find the right flatmate. Beware of scams. Do not send money.’

It wants me to click into the account \_\_\_[0:17:49]. Well, I don’t think it is right, because I don’t know what [the use] of the link to see the message and the profile. It’s a little weird, because [of the email 0:18:12] message. I will choose three.

[Amazon.com]. Regards to the pictures, it’s got the image for [Amazon]. Everything seems to be right, except the email address seems to be incorrect, so one.

Facebook notification \_\_\_[0:18:51]. It’s weird to have something like [plus] in the email address, so I would choose one.

Your mobile bill \_\_\_. Virgin Mobile. No, from the email address it is not legitimate.

Blackpool. ‘Thank you for visiting the Pleasure Beach, Blackpool.’ Blackpool Pleasure Beach. Well, the name of it, I think the account shouldn’t be [service@aspeztmr 0:19:45], stuff like that. Yes, I don’t think it is right, so I will choose one.

DVLA. Info@dft.co.com. This is not the right email for the [company 0:20:17]. One.

[R. Malcolm]. ‘Enjoy your first week \_\_\_.’ From the email address I think it is a member of Lancaster University, and the subject \_\_\_[0:20:43] I think it is alright. ‘Welcome to Lancaster.’ [Amazon] vouchers. ‘Complete a survey \_\_\_.’ I think this is legitimate. It is coming from my university.