United Trust Bank

Webinar Transcript

Protect Your Organisation. Protect Yourself.

Steph:

Good morning everybody. We'll just give it a couple more minutes for some more people to join and then we'll kick off. Okay. Good morning everybody. I'll just give the camera a minute to catch up. And thank you very much for joining us today and for our cyber security webinar. I am joined in the room by my colleagues, Nikki and Francis from the deposit solutions team, and Rob as well who I'll pass over to in a moment. So we at UTB do understand that cybersecurity is a very, very important topic and a government report published in April, 2024 showed that half of businesses and a third of charities experienced some form of cybersecurity breach or attack in the last 12 months. Rob is an industry expert and ethical hacker, and he's going to spend around 45 to 50 minutes speaking to you about cybersecurity and how you can protect your organisation and yourselves. Questions for Rob can be submitted on the webinar chat and in the q and a. So please go ahead and do that as we go along.

So if you have any questions or you think of anything, then please do go ahead and do that. If for any reason you're not able to ask using the q and a function on teams, then please do email Nikki Nikki's email is ncole@utbank.co.uk and we'll pick those up. So at the end we will go through and we will ask Rob all of the questions that you have submitted via Microsoft Teams. Hopefully there won't be any IT issues and you can hear us see us, okay. But again, if you do, please do let us know via Microsoft Teams. We'll do our best to try and help you. And I'll now pass over to Rob. Thank you.

Rob:

You Rob. Thanks Steph, really nice to meet you all. I will jump by the camera to pan over to see me shortly.

Steph:

There you go.

Rob:

Here we go. Great. Hi everyone. Nice to meet you. Before I start the main presentation, I'll introduce myself. So my name is Rob Chaplin and I work as an ethical hacker. So what that means is I get hired by companies to basically pretend to be a cyber criminal hack through your defences, but then once I'm inside, I'm not going to steal your data and set it to other cyber criminals or encrypt it and demand a huge ransom payment. I'm going to then show you how I did it and help you protect against it. So when you are targeted by those real criminals, hopefully you've already got those defences in place. Now there's a couple of different ways to do that. The first is through technical cyber attacks. So if you've ever seen a TV show or movie with hackers in it, it's always shown the same way.

There'll be a bunch of kids in a basement listening to some banging techno music like pink hair tattoos with these huge monitors with cubes spotting into place and passwords getting cracked and files getting knocked over all sorts of stuff. Honestly, I wish it was like that. If I had enough money, I'd build a basement in my house that looks exactly like that centre, but generally speaking, it'll be people in offices in their house, in their study, et cetera, hacking in trying to break through a company's defences to get inside. But I'm not going to focus too heavily on the technical side of hacking during this presentation because it's not that common compared to the other type. And also that's kind of your IT team to look after certain. Instead, I'm going to focus instead mostly on the human side of hacking, which is known as social engineering.

This is where you trick someone in the organisation to doing something on your behalf. So an email phishing attack for example, where I'm trying to trick you into opening up a link with attachment that is a social engineering attack, perhaps a phone call where I call you tend to be from your IT service desk, I need your password for something or my specialist niche within what is already quite a small industry is physical intrusion building. So dressing up as perhaps an employee with fake badge and everything, or maybe a cleaner from a cleaning company, maybe the guy that's come in to fill up your coffee pods or your printer paper or whatever else I think will allow me inside the building. Then once I'm inside, I'll either grab a laptop and steal it and access it from there, or I'll plug into an empty port in a meeting room or something along those lines and start hacking in from inside the building.

So when I'm not doing either of those things, I do a lot of trainings. That's why I'm here talking to you guys to give you a little bit of a taster of what cybersecurity training should look like, what I think it should look like, and then I do a bit of media work for BBC ITB, sky News and a few others as well. And I did writing for various different magazines. So we've got four main topics we're going to cover off with you today. In the first section, I'm going to talk to you more about social engineering, that human side of hacking. I'm going to tell you a story. I always like to tell stories when I'm doing trading on cybersecurity to help you understand how the criminals plan and attack and what you can do to depend against it. Well then look at phishing attacks as this is the most likely way that you've be breached is through someone opening up a link or attachment within an email, within a LinkedIn messages message within Instagram and sorts of things.

Well then move into passwords. So how you can have a secure password and also how you can remember all those different passwords. I think we'll all agree we'll have far too many passwords that we need to be using, and I'll come up with the best way of how you can actually use a password that's memorable, but also very, very strong against hacking attacks. And then we'll think about who might hack us and what the impact would be if they were successful. Hopefully any audio issues are sorted out. We've just moved the microphone a little bit closer, so I'm going to jump in straight away with my favourite topic in the world to talk about, which is social engineering, which is how most companies are breached. So if you were to suffer a data breach or a hack, it's most likely a social engineering technique would've been used, perhaps phishing.

So we'll have a whole section on phishing, but phishing is a type of social engineering because I'm trying to convince you that I'm from a company that I'm not in order to get you to open up a link or an attachment. But for this section I'm going to tell you a story and it's a story of a company that I broke into a little while back and how it's all planned and executed. So what happens from my perspective is a company will approach me and they'll say, we've got some cybersecurity defences in place. We bought our firewalls and our antivirus and all that sort of stuff. We've given our staff a bit of e-learning and we run them through an induction process and we've got our badges for getting into the building, but how do we actually make sure those defences are working because we don't know until we're actually hacked.

We have no idea. So I will come to them and say, okay, what do you want me to achieve? What would you like me to steal? What's your crown jewel? What's the most sensitive information on your network? And the company in question, were a legal company and their sensitive data is pretty much everything they have, but they have all sorts of confidential data about companies and individuals, and they said, okay, we're going to set you a few objectives. So the first one, we want you to get into our email system for one of our senior partners, hack into his office, 3, 6, 5, get into his email and send an email from that account. Next, we wanted you to break physically into our head office building, get access to our server slash comms room where all the IT get I stored. Also, grab some client paperwork and then plug a USB stick into one of our computers that's unlocked and unattended to show that you could have introduced viruses and things like that into there.

So a quite difficult set of objectives. So the first thing I like to do is plan how I'm going to achieve these attacks and break it down by the objectives and how I might achieve those. So the first part of any attack against a company, and this is what criminals do as well, it's called open source intelligence gathering or osint. It's just a posh way of saying research on the internet. Really, if you're going to attack any company, you're going to need to do a bit of research about who they are, where they're based, what they do, try and find their weak points. So I'll start on the company's website. I'll look at who they are, what they do. Then what I'll normally do is I'll look for the links to their corporate social media pages as these normally have a wealth of information. So most of you will have a marketing team that run social media pages.

So you might have a LinkedIn, you might have a Facebook, you might have an X or an Instagram. I am looking through those images and messages that you've posted, anything that might give me clues about how I might be able to hack into your company. So perhaps images of your staff wearing ID badges and events. I can then take those images of those ID badges, feed them into an ID badge printer that I have with my face on instead and print out a badge that makes me look like an employee. And that's a really, really simple one. Now, for this company, the first objective was to break into their email system. Now most people in this call will probably be using Office 3, 6 5 for your email. So how does someone get into someone else's email? You need a few different things, right? You need their email address, obviously you need their password, you possibly need to get past multifactor authentication as well.

So first one email address that's easy for lots of companies. They'll list email addresses of key contacts on their website, especially for legal companies. For others, the easiest place to go is to LinkedIn. So LinkedIn doesn't tell me your email address, but I can search for the company name and then bring back a list of employees, and that tells me who you are and where you work. So it's not going to take a genius to work out what your work email address is going to be from those two bits of information. So first one's easy to find. So for this company, I narrowed it down to senior partners on LinkedIn, pulled out their email address and they had it on their website as well to confirm anyway, so I've got the email address. Second part is the password. Now of course, this is the most potentially most difficult part to get hold of.

It's the bit that's supposed to be secret. However, the easiest way to get hold of someone's password is to cease, has someone else stolen that password already for you? And the best place to do that, there's a huge database full of already hacked usernames and passwords on the dark web, but if you know where you're looking, you can find it easily enough. That list is about 13 billion entries long. So imagine an Excel spreadsheet. Column A is email address, column B is password. There are 13 billion rows in this spreadsheet of people's usernames and passwords. And what's happened is these have been stolen from websites. So perhaps a website gets hacked into the criminals access, the underlying database that stores all the usernames and passwords downloads it. But then they do this for thousands different websites over the last 10, 15 years to the point now where we have this 13 billion long list.

So I like to search in this list for the email address that I'm trying to hack into. So I took this email address that I'd taken from LinkedIn and from their website searched through this list for it and it was in there eight separate times. So this person, this senior partner, had registered his work email address on personal websites to use as his login, and then those websites have subsequently been hacked. And in every single case, his password was the same. So it was a variance of the word password. So I thought logically there's a very good chance that his password for work is going to be the same as every other one that he's been using because if he's using it eight times, he's probably using it a hundred times. So I thought, I'll log in with this usernames and password, but I've got to be prepared for the fact there's probably going to be an extra step.

The multifactor authentication sometimes called two step or two factual authentication. That's the extra code that you need to put in. Maybe you get it texted through to your mobile, or you might have an app like Microsoft Authenticator that prompts you to enter a two digit code that appears on the screen. So I thought, is there any way for me to determine whether they're using Microsoft Authenticator or some other authenticator before they actually log in before I alert them back potentially that someone trying to log in. So I went back to LinkedIn and what I'd like to do is to search for IT employees of the company and then click into their profiles. And on LinkedIn, some people will just have a list of all the jobs they've done, but other people will break down those jobs into the individual duties they had and experience they learned within those jobs.

And one of their IT people had done that and he'd listed out all the projects that he'd done for this firm, and one of those projects was implementing Microsoft Authenticator. So I thought, aha, I know that they're using Microsoft Authenticator, so I know I've got to get past this extra step. Now in order to get past two facts authentication, it's quite difficult, but it normally involves tricking someone via a phone call. So I will perhaps phone up and pretend to be from the IT service desk and we're logging in and doing some maintenance and we just need you to authenticate us through authenticator. But I got really into it. I often get really into these social engineering things, and I thought what I'd like to do is not only pretend to be one of the IT people, but I'd like to make a voice clone of them using some of the AI software tools that you get nowadays that can clone voices.

So as an example, you might've seen during the European championships, you had Gareth Southgate having his voice cloned and saying silly things on video. So I thought if I can use that sort of tools to create a replica of an IT person's voice, then even if my target knows his voice, it might still work in order to do that. Back to LinkedIn, search for the names of the IT employees, search for all of those names on YouTube, and one of those IT employees had spoken at a conference where he'd spent an hour doing a presentation. So I had an hour long sample of this guy's voice. You literally need about two to three minutes. So an hour is plenty. So I fed this into the voice clone tool that I use and created a replica of this person's voice. So now the idea is I'm going to try and log in with the username and password.

If it works, it'll trigger Microsoft Authenticator. I would then phone this person their phone number's on the website and pretend to be from the IT service desk being this IT person with the voice quote. So everything's going to come in together. So I logged in, the password worked, so he was using the same password. It then triggered this M authenticator. So I phoned him up quickly, played my voice clone to him saying, hi, it's David from it. We're just doing some maintenance on your account. You may have noticed us log in, it'll prompt on your phone for M Authenticator. Would you mind just opening that up and putting in the number on number 65 into your phone? And he went, oh, hi Dave. Yeah, no problem at all. I'm having some weird things going on my laptop anyway, so it'd be great if you can have a look.

I'll do that for you now. So he typed in a number and now we're in, and now we're inside his office, 3, 6, 5 email. And this guy had been there for about 12 years. So he'd been sending thousands upon thousands of emails over those years, never deleted anything. It was all in there. They had all massive amounts of sensitive information from this company's email. So that would be a data breach just alone. I've done that, sat at my desk at home and it took me a couple of hours to do. So that's the first part of sheet. Now the second part is to break into their head office building, and that's going to require some very different planning because I've got to physically be there. Now the objectives they've set me are to break into their server room where their IT kit is stored and to get onto a laptop and grab some paperwork.

So I thought back to the idea of pretending to be an employee because I found some images of their ID badges on LinkedIn and I thought I could create a replica badge, turn up

as an employee trick my way into the building, maybe just join the morning traffic as people come in and follow people through doors and things because quite a big office, chances are that would work. The problem is getting into the server room because that's normally restricted to just IT people and perhaps the facilities team. So how am I going to get past that extra layer of defensive? I'm just dressing up as a random employee. Everyone knows the IT team, so I can't pretend to be an IT person. So I thought, okay, I'm going to go up with a different scenario. Instead, what I'm going to do is I'm going to dress up as an environmental auditor there at the building on behalf of the local council to run some audits of the building temperature leakage from Windows and things like that as part of the council's commitment towards net zero carbon emissions.

But in order to make this as believable as possible and to make it work, I wanted to come up with some things I could do. So first of all, I wanted to create the outfit. So I've got a green polo shirt there. I spent way too long designing that logo with the tree and everything on there. I've got a lanyard ID badge. I've got a device that actually measures temperature leakage from Windows. I had a clipboard with work reference details on there, and then I thought, I'm going to need an appointment as well, ideally. So I want to be turning up with them knowing I'm coming already rather than just turning up and trying to convince my way in. So I went back to LinkedIn. I researched the local council for the area where this building was, and I thought there probably is someone at the council who's responsible for the council's placed towards net zero, and there was someone's job specifically that.

So I got one of my colleagues to phone up the target company pretending to be this council person saying, hi, it's Thomas here from local council, and we're doing energy audits of every building in a local area. Your road is up next. So we're going to be sending in Benchmark Energy at 1130 on Friday to do an energy audit of your building. Can you give any help he needs? Now, the reception staff said, oh, you'll need to speak to our facilities team before we can let you in. They gave us a move on number, but we tried that for about a week and the guy never answered. So we just left a voicemail message saying about the visits. That's about as good as I can get, so I'm going to have to turn up and hope to convince my way in based on this voicemail being on this guy's phone.

So I turn up 1130 on Friday as we've called in about dress like this, go straight up to reception desk and say, hi, I'm here from Benchmark. We've got an energy audit appointment booked in for you at half past 11. Would you mind if I pop upstairs and get started? And she said, oh, I dunno anything about this. I need to speak to our facilities team. And he happened to be in the background and he walked over and he went, I dunno anything about this either. And I said, oh, I've got a note here on my clipboard saying that there's an appointment booked in 1130. Facilities team should be aware there's a voicemail on this mobile number. And he said, oh, that's my mobile number. So he got his phone out, put it on speaker phone, phoned up his voicemail, and there was that voice from my colleague saying, hi, we are booking you in for an energy audit appointment 1130 on Friday with Benchmark Energy.

And he looked at me and I'm there at 1130 on Friday. I'm wearing the benchmark gear. And he went, okay, what do you need to do? I said, well, I'll need to get up to the top floor,

start there, take some energy readings from the windows, et cetera. Maybe you need to get into other places and then I'll give you report at the end. And he went, okay, that's fine, but I'm going to need to accompany you around the building. I was like, okay. So it is good. I've got in, but I don't want him accompanying me because I can't very well steal paperwork and access a laptop and things like that if he's going to be with me. So I thought, okay, how can I get rid of this person? What's the best way to do that? So we got up to the third floor and I went to the first window and I started scanning and I wrote down, I had an iPad that I wrote down the results on.

So I wrote it down on there. I then moved the little gun about an inch and took another reading and wrote it down and then another inch and wrote it down. And he went, how many windows have you got to do this for? And I said, every window in the building. He went, that's going to take all day. Yeah, it's going to take all day. At least I might be here quite late. Oh, he looked, his outlook on his phone, he went, well, I've got no meetings today, so you're lucky I can stay with you all day. I was like, oh my God, he's going to stay with me for the entirety of this thing. So an hour and a half later, I've done the third floor. I'm completely bored at this point. I'm literally going to every window, every inch of every window taking these readings.

We finished the third floor, but I'd noted on this floor, that's where the server room was. So I said, do you have any major heat sources in this building? And that's the whole point of this energy audit idea was that we'd get me into the server room and he went, oh yeah, there's a server room over there. You need to get in. I said, oh, yes, please. So we unlocked that, have a separate code on it, let me in. And as he let me in, he got asked a question by someone, so he turned his back. So I had about two minutes on my OMS server, which was I have to get some photographs and prove that I'd been in there, et cetera. The second objective was to grab some paperwork that proved to be quite easy. They had it everywhere. It was on cabinets, on people's desks, on printers, et cetera.

And the more time that went on, the more bored he got and the more distracted he got by other things. So it was very easy for me to grab a bit of paperwork while his back was turned. But the last objective is to get access to someone's laptop in an unlocks and unattended state. And that's really difficult because every time someone gets up from their desk, they're locking their laptop or they're taking it with them, or they're in a row of desks with 10 other people and the energy audit guy can't just sit down amongst those desks and start typing away at someone's laptop. So I thought, okay, how am I going to achieve this? We end up doing the second floor, another hour and a half, first floor, another hour and a half. We get down to the ground floor and he tells me they've installed triple glazing on this floor and asked me my opinion of the heat sensitivity of these windows.

I'm like, yeah, it's great. Obviously I have no idea what I'm doing, but on the ground floor, there are some meeting rooms that are outside of the main kind of public area of the building. So I thought, okay, perhaps I could ask to use one of these meeting rooms to sit down for a little while and then he'll leave me on his own because it's my own. It's in a public area, and then maybe I can say, if I need to get back up to take some breaths again, can I come back up? And he said that he said, yeah, it's fine for you to sit down here, but if

you do need to get back up to take some other readings, come to reception and ask me and I'll come down and get you and bring you up. So I waited in this meeting room for about half an hour on my own.

I couldn't do anything in there of any interest. Then I went back to reception and said, I've missed a couple of readings. The facilities person said, just to grab a visitor badge from you, is that okay? And she said, oh yeah, no problem whatsoever. So she gave me a visitor badge and now I've got free reign. But before I left, I said, which floor is the facility's person on in case I need it? She said, oh, he is on the third floor, right? I completely avoid going to the third floor because I'm not supposed to be on my own. So I went back up to the second floor, started walking around again, I'm looking for any opportunity, someone leaving a laptop unattended. It was getting a bit later in the day, so I thought maybe people are getting a bit more lax or whatever, there's less people around, but it doesn't happen.

Go to the first floor, no one is doing it. I thought, how am I going to achieve this objective? Now, earlier on in the day, there had been a woman who had been asking me all sorts of questions about what I was doing. She just really genuinely interested. I dunno why it looked like the most boring job in the world to me, but she was asking me what I was doing, whether I liked the job, all sorts of stuff. So I thought, okay, maybe if I sit next to her and ask her if I can use a desk just to write up some results, maybe she'll get chatting and maybe she'll offer to make me a cup of coffee or something. So I do exactly that. And after about 10 minutes of chatting with her, she says, I'm going to make a cup of coffee.

Would you like one? I said, oh, yes, please. And she got up from her desk and she left her laptop unlocked. So I quickly plugged in A USB stick, and essentially what this USB does is it pretends to be a USB keyboard and by pretending to be a USB keyboard, it can send keyboard commands to the computer. So I have a predefined kind of script in it that sends a bunch of keyboard commands, launches various programmes and things like that, and essentially gives me remote access to that laptop even after I've left the building. So I ran that. That gave me access to the laptop. She came back, gave me a cup of coffee, we had a chat, and I left the building. Now I know it's a bit mean though. I took advantage of a good nature, but part of doing this social engineering stuff is I always agree at the start that no one will get in trouble for what we're doing.

And also I came back and did training for them. So a big part of my job is doing training like this, but for companies on site interim, get everyone together. And she was in the very first training session that I did at the headquarters of this company in the building I've broken into, and I walked in and she was there in the front row and she looked at me and she went, oh no. She suddenly realised who I was because it was only a couple of weeks earlier. So I grabbed her quickly and made a chat and she totally called about it, and she's actually now one of their biggest security advocates for defending the building and the network and stuff. So I always make sure no one gets in trouble. But the point of telling you that story was to show you that a company that was actually quite well defended overall, and it had those extra layers of defence, the multifactor indication on the email, et cetera, they had decent defences, their building, but it just kind of went wrong because they were too

trusting and because the training that they'd had via e-learning modules and stuff like that didn't touch on this kind of stuff and most won't.

So that's kind of a flavour of the physical intrusion, complying with a bit of the voice cloning stuff. Now, I wanted to move into the main way that you'll be hacked as an organisation. If one of you were to go to me, Rob, we've suffered a data breach, help us out. I'd go, okay, what happened? Oh, someone clicked on a link, someone clicked on an attachment. That's normally what's going to happen, and that's how criminals normally break in. The reason that's so popular is because you can do it anywhere in the world. I could be sat at my desk at home, I can fish any company in the entire world because everyone has remote access to their email. So they can work from home or wherever, usually through obvious 3, 6, 5. So the idea behind the phishing attack is to trick one of you into opening up a link or an attachment, and I think there can be a misunderstanding of who that has to be.

It doesn't have to be someone senior in your company. It doesn't have to be someone in the IT team, any single employee of your company, even if they're even working there a day is a threat. Anyone that opens up that link with attachment. So if it's an attachment, what happens is within 10, 20 seconds, I'll have complete control of that laptop. But it's not like you see in the movies where the green matrix text appears behind you, the big laughing face appears and the mouse starts whizzing around the screen. It doesn't work like that. When I say take control, it'll be in the background. You won't know what's happening. You won't know I'm there, but I can passively watch everything you're doing, every website you're visiting, every password you're typing, I can turn the webcam on and have a look at you if I want to.

If you are on your works network, let's say you're working from home, you open up this attachment on your work laptop, I can connect through that work laptop and infect all of those other devices on the network as well and use it as a staging point to attack the entire network just from one laptop. So that's an attachment. If it's a link, what most likely will happen is you click on the link and it's going to ask you for a username and password. So the email might be from your IT team saying that your accounts had a problem, you need to log in or they're switching over to a new website address for office 3, 6, 5 or whatever else. You click on the link, it prompts you to use their password, now they steal it, now they log in as you and they gain access and your personal life, that might be your online banking, it might be your Facebook page, it might be PayPal, that sort of thing.

So the main two things, it also might be an email asking you to do something, click on a apart from particular link. It might be asking you to send over a financial transaction. So buy some Bitcoin, send over some Amazon vouchers. It might be asking you to send over personal details, but it's mostly about links and attachments. So everyone at work receives 40 many emails every single day. I'm sure we can all agree on that, and some of them contain links and attachments. So you need a quick way of devising what is a phishing attack and what is real. So I've brought it down to a few different indicators that I want you to look for when you are assessing whether an email is a phishing attack or not, and I do this every single time. You get really quick at it, it takes a couple of seconds.

So the first one and the most important one is the message will nearly always come from a different address than what would be expected. So for example, if you had an email come into your personal inbox from Apple and it's an invoice for something that you've purchased on the app store and it looks like Apple, it's got the template, it looks like an invoice from Apple, but it's a transaction you don't recognise and it's quite a large sum of money. Now the bottom, it says, if you did not authorise this purchase, please click this link. So you are angry, you're not thinking straight, you don't look at the email address properly that says apple-invoicing.com instead of apple.com. And you think, oh, okay, well I'm angry. I'm going to click on this link. I want to dispute this transaction. Now it asks you to log in with your Apple username and password.

So you log in, looks like Apple's website, but actually you've given it to a criminal because it's on a completely different website address. It's nothing to do with Apple. So anytime you have an email address that has any subtle difference in it, so it has a different spelling, it has an extra bit added to it like a hy separated bit, it has a different ending. So if it was apple.net or apple.co or something like that, that's a criminal sending you a phishing app pretending to be Apple. So that's the main one to look out for. So I've worked as an ethical wacker for years and years and years. I've helped lots of companies recover from cyber attacks. And when you look at what happened, how did that cyber attack start? It's nearly always a phishing attack and it's nearly always someone opened up an email from someone they thought was a colleague or a company that they recognise a client.

But when you look at the email address, it's different in some way. So this accounts for nearly all of the hacks, which is why this is the most important indicator. The second one is how the email makes you feel. So in that previous example about the Apple invoice, I talked about how that might make you feel angry. So anytime you feel particularly excited, curious, angry, fearful about an attachment or a link or an email or whatever you've been sent, if it's from your CFO and it's saying You must do this thing for me really quickly, that pressure of someone in authority makes you paniced. It makes you do stuff you wouldn't otherwise do. So anytime you receive something and you feel very pressured or very compelled to open that link or that attachment, that's where you take a breath and take a pause and go, okay, could this be a phish attack?

Now, we look at the email address, very similar for number three, urgency or threatening language combined with someone in authority is a very good indicator. Spelling mistakes in grammar errors. So obviously if you get an email from PayPal for example, it has two Ls at the end. It's a fairly obvious one, and go back a few years. Phishing attacks were easy to spot because they were full of spelling mistakes in grammar errors. Nowadays, the criminals are starting to use tools like Chat, GPT and other AI things to write the phishing attacks for them so they don't have spelling mistakes or they simply take a real template like a real invoice from Apple and they just swap out the links with their own ones and then send that off. Now, indicated number one, I talked about how it'll nearly always come from the wrong address, but there are some instances where you may get an email from someone.

So it might be in your personal life, a friend or a company. It might be at work, a colleague, a supplier, a client, and it's from their real email address. But what they're asking you to do

is really weird. So they might be saying to open up some strange looking attachment or go to some strange link or change bank account details, especially if it's come from a client. They might say, we are using a new bank account or a supplier using a new bank account. Please use this one. What may have happened is that supplier, that client's email account may have been hacked into in the way I described hack into that senior partners email account. Once they're inside, they don't just look at information, they normally start sending email from there because that email address is trusted. They can even reply to existing email threads.

So if you get a reply from one of your suppliers saying, hi, thanks for your email, just let you know quickly, we're switching over to a new bank account next week. This is the new number, and that comes from a trusted email address replying to an existing email thread you've had with that client. You just have a trigger in your head going, okay, bank account changes are weird, any strange attachment, any strange link, could it be their email has been hacked into and then report it or give that company a call and a number is theirs. And the last one is if you get any email that requires you to send personal information, or especially do financial transactions that are something like a wire transfer or buying cryptocurrency or buying vouchers is a very common one that criminals use. They'll ask you to go and buy 600 pound Amazon vouchers because the CFO is about to go into a meeting with some key clients that he wants to give him these vouchers.

The reason they use vouchers is they're untraceable. You can sell them online for about 60% their value, and it's completely untraceable from, it's a great way of laundering money. So any kind of that sort of request, make sure you are reporting it to your IT team or your personal life, you're deleting it. So I've touched on email so far. I wanted to run you through some of the other things that criminals are doing to break into organisations. This one is done through LinkedIn. Now generally people are less on their guard with phishing attacks once you move away from email. There's a big association in people's heads between email and phishing attacks. But criminals are clever and they know that, so they'll move to other potential ways of hacking it. So this one relies on LinkedIn messages and it relies on within any company, there's always someone that will be open to a new opportunity, a new job, or maybe actively looking.

So these criminals have registered recruitment profiles on LinkedIn. They look identical to real British recruiters. So it's very difficult to determine whether who you are speaking to is a real person or whether it's a hacker. Now, many of these are based in North Korea and they target organisations to make money essentially. So once they've got into your computer using this technique, they'll then do a ransomware attack, which I'll talk about shortly. Don't fall into the trap of thinking, oh, it sounds like a spy novel. I'm not going to be targeted by a North Korean hacker. They're one of the most active groups in the world actively targeting western organisations. They have literally about 15, 1600 hackers like me, purely targeting western organisations. So you could well be a target for them. They're just looking for anyone that might be open to a job. And what they'll do is they'll send you a message through LinkedIn saying, hi, we saw your profile.

We think you might be a great fit for a job we've got coming up at Google or Meta or Spotify, some prestigious organisation. We'll send you the details next week so there's no link and there's no attachment in that first message often. Then a week later, sorry, we haven't got back to you yet. We're just finalising the job spec a couple of days later as mentioned, we think you may have been brilliant fit for this role. Here's some details. Now have some bullet points. It sounds so perfect for you because they've looked at your LinkedIn profile and they've designed a job that is perfect for you. So they'll also have more money than you're on now, maybe 50% more money than you're on at that time, and then they'll send you the job spec through, it'll be a PDF file. That PDF is an attachment.

When you open that PDF attachment, they take control of your computer just like they would if it's an email attachment. It's just done much more subtly over time through LinkedIn. Instead, it drops people's guard and it works brilliantly. They're able to hack into loads and loads of systems using this. I use the same techniques when I'm doing phishing attacks against companies. I don't just do email, I will do LinkedIn phishing, I'll do comments on their Instagram posts, whatever. You have to be on your guard everywhere that you could receive a link or an attachment and then open it up.

So a lot of people ask me, okay, Rob, what's the goal? Why are the criminals doing this? How do they turn the access they have to someone's laptop into money or into stealing that information? So let's play out a scenario with you. I send you an email phishing attack, okay? So it comes into your inbox. It doesn't do any damage when it's just sat in your inbox. It doesn't do any damage when you open up the email. But if you were to open up that attachment, I now have control of your laptop, but I'm not going to stop there. I'm going to start looking at the network connections you have. So if you are working from home, you're connected through A VPN or you're on SharePoint or whatever you do, I can access all of that and I can instal essentially a virus on that computer that spreads, and it spreads almost exactly like a human virus.

So anything it can connect to, it will spread, and then it will spread from there to other things, and it spreads out like a web, but it doesn't do anything yet. It'll wait five, six days, just like an incubation period for a cold, for example, and then it will activate, and at the point where it activates, it will take everything stored on every single device it's got to, and it will start encrypting or scrambling all of the data on those laptops, on those SharePoint sites, on other cloud services, on servers, everything it will get as far as it can get. It will even actively seek out backups of that data that you might have, depending on how you configure those backups, encrypt those as well. Then a big message will pop up on everyone's screen saying, all your files have been encrypted by military grade encryption and we offer the best unlocking service in the business.

Please click the link below to chat to our customer service agents to start your unlocking process. So they treat it like a business transaction, so you have a problem, your entire network is encrypted. Forget the fact that they did the encryption. You need a solution, and that solution is a decryption key, which is a long string of numbers and letters, but when you type in will restore everything back to normal. Without that, all of that data is inaccessible. So imagine your entire company grinding to a complete halt. No one could do any work. The average amount of time it takes for a company to get back up and running, even to a small extent, is three weeks. But for some companies that will go on for months,

even years of trying to get that data to back. So many companies end up engaging with these cyber criminals and you open up the link to the chat service and they're extremely helpful.

They'll speak different languages. They'll offer to unlock a couple of files to prove they can do it. You then have to arrange this unlocking fee, which is essentially the ransom fee, but that will cost you a lot of money depending on the size of your business. They'll customise the ransom fee to you. So they'll look at your turnover, your profit, all that sort of stuff, and they'll go, okay, we think the appropriate ransom fee for you is 2 million pounds. If you've got cyber insurance, it's very likely they'll find that out as well. And they'll say, okay, you've got 2 million pound of cover. Okay, let's charge 4 million pounds. There's 2 million extra in there you can negotiate with them. But the success rate on negotiation is about 50 50, about half the time. They reduce it, half the time they increase it because they get angry at you negotiating with them.

The stats in the UK are about two thirds to three quarters of organisations pay that ransom fee. And the reason is because the company's essentially crippled, there is nothing they can do. They can't do any work. Imagine every single employee of your business being unable to do anything at all, and this all comes from one person opening up that phishing attack they shouldn't have done because they G email address. But not only do they encrypt everything while it's spreading and things like that, what they'll normally do is they'll download some of the most confidential and sensitive information you have on your network. So they'll look for your payroll data for your staff, they'll look for your client information. If you've got anything particularly sensitive like passport scans, ID scans, that sort of stuff, they'll grab that information. Proprietary products services that you've developed, they steal the designs for those, they move it to their own network.

Then if you refuse to pay the ransom fee because perhaps your backups are working and you can get everything back without paying the ransom fee, they'll go, okay, well, you can not pay the ransom fee, but we've got all this sensitive information. We're going to release it publicly. We're going to start doing fraud attacks against your customers that you are going to be potentially liable for. So you have to pay the ransom fee to stop them from doing that. And another question I often get asked is, how can you trust these people that if you pay the ransom fee, they'll actually restore my files and they won't release that information. And the reason is reputation, which I know sounds ridiculous when we're talking about criminals, but their reputation is of the highest importance to them because if you paid and then they don't follow through on the service IE restoring your files, not releasing them, the next time they hack someone, it's going to be known that this organisation can't be trusted.

No one's going to pay. So they have to actually release the files in order to be able to do another attack down the line. So there's kind of this honour among thieves thing. So they very often, nearly all cases will actually release your files and they will not release, I mean, unlock your files and they won't release the other files they've stolen publicly. They probably won't delete 'em off the network. They're probably going to keep them to be honest, but they won't actually release them into the public domain. So ransomware is the

single greatest threat any of you will face as an organisation. It's the most likely thing that will happen to you, and it often comes from that initial email phishing attack where one of your employees doesn't open that link and attachment, which is why training them on what to look for is the single most important step you can take in defence of your organisation.

So tips to avoid phishing attacks in general. First one, checking the email address every single time you have a link attachment request for personal information or financial transaction. Is it the right email address? If it's from Apple, is it@apple.com? If it's anything else, we treat it like a phishing attack. If the message comes from someone you know, recognise the email address and you go, okay, that is actually that person's email address, but it's asked me to do something really weird, trust that gut instinct. If you have it, team talk to them. If not, pick up the phone. Phone up the company that sent that message and go, okay, is this you that sent this email? You'll be surprised how often it's not. If there's something very, very weird about that message. Check number three, if it's sent through another means, whether it be through WhatsApp, through text, through LinkedIn, Instagram comments, Facebook messenger, literally any way you could be transmitted a link or attachment, do you trust the person that sent that message?

So you have to be very careful on LinkedIn because you're dealing with people you've never met before. You have to be very careful on Facebook Messenger. If you are doing, perhaps you're selling an item through Facebook marketplace, someone sent you a link to a payment thing or something along those lines. We don't do anything like that. We don't click links through that kind of thing. Lastly, all of this is enhanced. If you feel very strongly like you want to interact with this attachment or this link. If you brain's going, oh yeah, I really want to open this. That's your pause, that's your trigger to take a pause, take a breath, and go, okay, could this be some form of attack? Now I'll have a look at the email address now I'll make a call to verify whether it's a real one. Okay? And that brings me onto the third part of the presentation today, which is on passwords, and I think everyone in the court would agree, we all have far too many passwords, right?

Between work and our personal life, we probably have well over a hundred. Some of you will be in the hundreds, including all the shopping websites you have to go to and things like that. So how do we come up with a system that allows us to remember passwords, but also have very secure passwords and not use the same password everywhere? So I'm just going to give you a quick briefing on how passwords are actually hacked. So if I wanted to break into your Instagram account, for example, how would I actually get in? How would I steal your password? The first technique is phishing. We've just talked about that. I pretend to be from Instagram, but I'm using a slightly different address. It might be security-instagram.com, and I trick you into thinking that your account's been frozen or someone's hacked into your account, and we need you to click on the link and prove it's you, for example, and you log in with username password to the security instagram.com, and now I have your password, and now I log in.

So that's one of the simplest ways, the second simple ways, what I described earlier, do you remember when I talked about that senior partner and how I used a big database of usernames and passwords? That's the second way to break in. So can I find the username and password of the person I'm looking to hack into using that database as an example, lots of you would've heard of MyFitnessPal, I'm sure it's like a calorie tracking app and website.

A few years back, they were hacked into. So the underlying database that stored all the passwords for that, that company was broken into, and the criminals downloaded all of those hundreds of thousands of use names and passwords. They had absolutely no interest in logging into your MyFitnessPal account and seeing how many calories you eat in that day or that you cheated by eating miles bar or whatever.

They don't care about that. What they care about is, can I use that same email address and password and log into your PayPal account to your Facebook, to your PayPal, all that sort of stuff. Okay, so can I access all of those financial systems or social media websites, that sort of thing? If I can, brilliant. Then I've just hacked in without ever having to actually touch that bank systems. So they will target weak websites, so websites that may not have the budget to secure themselves properly, especially if they've got lots and lots of users in order to steal those usernames and passwords and put 'em into this database and use them. And as I mentioned, that database has now grown to around 13 billion, and I'll show you how to check whether you're in that list shortly. The third technique, and the last one we'll try is can we guess your password based around predictable things?

Most people are not very good at choosing secure passwords. Most people use a single word with a number, perhaps a symbol, or they might swap out an E for a three an A for an at sign. It'll normally be something associated with name, place, favourite football team, something along those lines. So for example, if they're an Everton fan, they might have the password Everton one, and then they have to change their password at work every 90 days to make it Everton two, Everton 3, 4, 5. I've hacked into people's passwords that have been using password 24 as their password because they've been in the company for eight years. They just incrementing that number one by one. So people are generally not very good at recognising what a secure password is. So how do you get around this? How do we come up with a system that allows us to have good passwords, but also different passwords?

So the first step, let's see if we are in that list of already hacked passwords. There's a couple of ways you can do that. So you can use a website called Have i been pod.com? I am completely aware of the irony of directing you to a random website that sounds dodgy straight off the phishing section. So apologies for that. But it is trustworthy. It's done by a security person like me. You can Google HIBP, go to the first link. That's not an ad. I tend to avoid ad links because they can be swapped out. Dodgy ones goes to the first link in there. That's from the have i been po.com address. You're only typing in your email address. What that does, it'll go green or red, and it checks through that list to see whether you're in there. Basically there's a search through the whole thing.

If you're in that list, it'll go red for your personal email address. For almost all of you, it will go red, which means at some point a website or a number of websites that you've registered to with that email address has been hacked into. It doesn't specifically mean your email address has been hacked into, it just means a website you've registered to with that email address has been hacked. But if you happen to be reusing the same password on that website as you are in your email, then your email could be hacked as well. So you want to check whether you're in that list. If it goes red, scroll down it to a bit more information. What you're looking for is what's the most recent time I've been hacked? Have I changed

my key password since then? If not, I'm going to move to step two, but I strongly encourage you to move to step two anyway.

The other way to check in step one, whether password has been hacked is through the built-in password function on the phone. So Apple now is a nice passwords app you can look into, but you can also go through settings on Android to have a look at your passwords and it will flag up whether any of your passwords have appeared in a data breach, which is exactly the same check that this website's doing, and then you can go and change them. So once we move on to step two, what does that mean? So what you want to do is have long and weird passwords. Okay? Long and weird is your friend. The longer and weirder the better. So what you can do is have long passwords that are constructed like sentences. They're called pass phrases. Pretty much every website allows you to use them, whether you can use 'em with spaces or not.

Spaces, I don't really care too much. You can condense it down into all one word if you want to. The example I normally give in my training is I love green tomatoes is your password. Okay, don't use that because I've been mentioning that for years. That becomes your password that you use. You don't use that for everything, but let's say we use that at work as our work password. The reason that's so good is because it's long and weird. So it's very long. It's about 20 something characters. It's weird because it's a sentence, okay, it's made of single English words. I love green tomatoes, but you can't break passwords down into chunks. So I can't guess someone's password is tomatoes and it goes, oh yeah, you've got a bit of that, right? And then I guess green it goes, yeah, you got some more, right?

It doesn't work like that. You guess the whole thing or nothing. So I would literally have to type in your email address and I love green tomatoes and log in in order for it to work. So that's why these sentences work so well because they're very easy to remember, but they're also incredibly secure. So you would have one of these use at work, you'd have another one you use for your financial systems. So online banking, PayPal investments, Pinterest. I don't mind if you have the same one across all of those because they're so strong. Third one you have on social media plus perhaps your mobile phone, things like Apple and Google. A fourth one is your personal email account, like Gmail, outlook, that sort of stuff. And then you have a fifth one, which is kind of your throwaway password that you use everywhere else.

So this is for all your shopping websites, games, forums, blogs, anything you use where you don't store sensitive information. So you didn't choose to save your credit card details on these websites. It might as well be a good password, but you share it across a hundred different websites. If one of those gets hacked into who cares, they haven't got your password for anything useful. So if they hack into your BBCI player account, they get access to your and log in as you, what are they going to do? Resume watching, whatever show you were watching last week, it doesn't matter because they can't use that password to access your online banking and that's the thing that you care about. So we are focusing our strong passwords on the websites. We actually care. Your second option if you don't like the idea of just coming up with these sentences and remembering those is you can store your passwords if you want to.

So you can either do it in a dedicated password manager app and there are plenty of them on the app store. I'm not going to not allowed or going to recommend your particular one, but look for a name you recognise and they can installed on your phone, your iPad, your desktop, your laptop, and it synchronises all your passwords. You type in one kind of master password or you unlock it with a fingerprint scan in order to access your password. But then when you visit a website, it fills in the password for you. I don't mind if you want to use that. Similarly, if you want to just store your passwords directly into your phone. So for example, on Apple, when you register to a new website, it'll say, would you like to use this suggested password? And it's really long and weird. It's just a bunch of numbers, letters, symbols separated by dashes often absolutely fine for you to do that.

Those passwords are very, very strong. It saves it into your device and then it fills it in automatically. I don't mind you doing that. Yes, if they break into your phone, they're going to have access to all of your passwords. But if someone breaks into your phone, you're in a world of hurt already because all those apps are already pre-GED in. They have access to your email account where they can go to every other website and go forgot password and it sends it and a link back to that email address. They'll have access to your photographs, everything. So someone breaking into your phone is pretty terrible already. Having the password stored in there doesn't make a huge difference at that point. Just on your mobile phone, just don't have a pin number of 1, 1, 1, 1, 1, 1 or nine, nine, nine, nine, nine, nine, don't have your birthday, your kid's birthday, your anniversary, your partner's birthday.

Any easy to guess date because if someone steals your phone, that's the ones they're going to guess first. So make sure that you've got a random pin number on your phone. Then I don't mind you storing stuff directly into your mobile phone. All you can use the dedicated your password manager app, but I like the memory system. You don't have to then have a dedicated app, et cetera. Okay, so that brings me onto the last little section. Before we go over to the questions, who would hack us and what would the impact be? So when we're talking about who's going to hack into organisations and individuals, it's mostly criminal gangs operating out of Russia and surround income countries. They are purely motivated by financial gain. They just want to make money. The best way to do that is to do these ransomware attacks that I've talked about.

There's other stuff they'll do by scamming you pretend to be your bank and getting you transfer your money, et cetera. But the primary method they use is ransomware attacks. They're very, very good at what they do. They're very well financed. They operate like an actual business. When I was talking to you about the ransomware attacks and how you pay them the money, you often pay them in cryptocurrency, et cetera. If you do pay that ransom fee, sometimes at the end of the transaction they will issue you with security advice to help out. They will also even give you a customer satisfaction survey at the end to check you were happy with the service you received from your call centre agent that dealt with your inquiry. It's literally operated like an actual business. So they're very sophisticated. They make billions every single year, which why they can afford to be so good at what they do.

The other group are nation states. That's a posh way of saying countries like China, North Korea, Russia, Iran, all have offensive cyber capabilities. Cyber capabilities all will target Western organisations as well. Activist groups, depending on what business area you operate in, if they have a reason to target you, they may go after you. Insiders is you or anyone that works for your organisation. There have been cases recently where North Korean hackers have got jobs at big tech companies in order to steal information from them. It's one of the easiest ways I did this as part of a social engineering engagement. A while back I noticed the company I was targeting had an IT job advert on their website. So I thought, okay, I wonder if I can use that as my in. So I applied for the job, made a cv, et cetera, applied for the job, got an interview and I thought idea is I'll get to the interview midway through, I'll ask to use their toilet and then I'll sneak off and plug something into one of their meeting rooms and then go back to the interview.

But we got about halfway through the interview and they said, honestly, this is going really, really well. Would you like the job? And I went, yeah, okay. Do you want to start on Monday? I was like, yeah, I've got a notice moment to start on Monday. And they gave me the job and I started working at this company for a week as part of the social engineering job and I was an IT person. So they gave me a username password, I just syphoned all the information they targeted me to go for during this week and then told them who I was and then left the company. But of course you wouldn't have to tell them who you were if you weren't doing it in the style that I do it. So insiders are a threat and that's about checking the background checks on the people you're employing and then occasionally you just get individual hackers.

These are the ones you see on the news, like people who have learned a little bit on YouTube, it may even be teenagers just like the stereotype they hack into an organisation in order to gain access to the data in there. They're often just showing off. Most organisations are very easy to hack into. I'm going to be honest with you, it is normally very simple. So even an individual hacker that just learn some stuff on YouTube can do it. So what's the impact? Let's imagine one of your staff hasn't had very good training. They don't look at the email address, they open up an attachment, infect their computer and that rips through your network and encrypts everything. First thing is massive business disruption for an average of three weeks you'll be able to do nothing. So all of the contracts you might have with clients, all the things you need to do in your day-to-day work stops completely.

Second impact, you might have to pay the ransom fee because you might not be able to get your data back quickly enough or a tool Third step, you then have to go and get help from various organisations and that'll cost you lots of money, is then the reputational damage. If you lost all of your client's personal details, you have to tell them that what impact does that have on the organisation going forward? Can you keep those people as customers from then on? You might even then on top of all of that, then get fined by the information commissioner's office or the regulators of your particular industry may slap you with an additional fine on top of that. So you get hit from every single site. And that all came down to one person that clicked on something they shouldn't have done, which is why it's so important to educate people.

So what can you do? So in the four topics I've covered off, there's obviously loads more things I haven't retouched on the IT side of things. That's a completely separate thing to this and I can tell you all about that, but not during this one. Social engineering. So intrusion of the building, what you're looking for is to not let people tailgate. So follow people through doors. So teaching staff to check behind them to question people checking visitors are supposed to be there that someone can't just rock up with a ladder and a VE jacket and go, I'm here to fix the light bulbs and get into the building. You have proper process in place for verifying visitors during that story. I told you at the start, if they had phoned up the council and gone, do you use benchmark energy for energy audits? They'd have gone, I with no idea what you're talking about.

We doing do energy audits and it would've worked, wouldn't have worked, would've all formed apart. And phishing attacks, remember it's about checking who it's come from, whether it be through an email, through LinkedIn, whatever. Do you trust the person that sent you that message enough to open it? Especially if you feel very compelled to open that. One thing I didn't mention phone calls and it is very easy to spoof or fake a phone number on your screen. So if your phone rings with your bank's name on the screen, do not do anything on the back of that. Answer the phone ask which regarding put the phone down, call them back on a number. There are lots and lots of scams going around where they pretend to be from your bank and they trick you to transferring money. Just be aware, you cannot trust what your phone screen says.

It is very easy, for example, me to phone you and I can make whatever I want appear on your phone screen. And not a lot of people know that. And lastly, passwords remember long and weird is your friend combined with either stor them somewhere I using that memory basis that I talked about. One of the thing I didn't mention in that slide that I should have done do use multifactor authentication. So although in the story I got past it through that phone call that required an extra step that might be quite difficult for companies that have been trained in how to defend against that. So make sure you are using multifactor indication both at work and at home. And that brings me to the end of the presentation. So thank you very much everyone for listening in this sec. We'll go to questions, but if you think of anything afterwards, please feel free to drop me a message on LinkedIn or on X or if you think this training might be useful for your company, please drop me a message on LinkedIn and we can have a chat about how I could deliver something like this to you live or over teams or whatever.

But Steph, have we had any questions?

Steph:

We have. So thank you very much Rob. I hope you all found it useful. I know I always learn something new every time I listen to Rob speak. So we do have a couple of questions. So the first one is I thought PDFs from read only. Can code to take over your computer be hidden in them?

Rob:

Yes, it can. Yeah. So within PDF files within Microsoft Excel documents, word documents, zip files, there are loads and loads of different files that we can use. So the act of double clicking on that attachment, whether it be a PDF or whatever is the point where that code runs and gives us access. Sometimes there's an extra step, it might be on Excel that you need to click on the enable macros button, but there'll be something within that spreadsheet that encourages you to do that. So yeah, we have to treat every attachment with an equal level of suspicion regardless of what type it's

Steph:

Okay. Thank you. And just a reminder, please do use the chat function if you do think of any questions while we go through the ones that have been asked. So the next one is can you be hacked into if you have sensitive information on a Word document or an Excel spreadsheet, which is simply stored on your desktop and never sent by email in an attachment.

Rob:

So yeah, for a hacker to gain access to that document, they would have to gain access to that laptop itself. So they would need to send you a phishing attack that you full for and open up or they'd have to find some other means of gaining access to that laptop and then gaining access to the documents. So what you are saying is can they get it through you sending it, you're not sending it out. So how do they get it? So yeah, they're not going to get it through you sending an email because you're not attaching to anything. So they would need to directly access your laptop perhaps by tricking you into opening up a completely separate email with a separate attachment that then grants some access to the laptop. They can then take that information from the laptop directly.

Steph:

So I guess in that case the best way to protect that document would be to password protect that document using the password information. Would that help?

Rob:

No, it wouldn't. The only reason that wouldn't help, it's like a little tiny extra step, but the password protection that Excel and word uses is so weak that you can break through very easily as a hacker. It is a small stumbling block, but nothing that would stop hacking, getting access to the document.

Steph:

Oh, that's really interesting. I would've thought if you had it password protected that would therefore make sure it's okay.

Rob:

Yeah, no, you can do a technique called brute force where you guess every possible combination of numbers, lessons, symbols against the document and you can do around about a hundred million guesses per second against the document that gives you access within a few minutes generally.

Steph:

Brilliant, thank you. And then the last question that we have so far, but if you do have any others, again please pop them in the chat. How did you learn all of this and how do you keep ahead of the real hackers?

Rob:

Yeah, great question. So I've been doing this for about 15, 16 years now. So I started off literally as T boy just observing people watching what they were doing that early days of this being a job. And over time I've just learned the techniques that we use. So then started doing research, I started actively hacking companies that were asking us to do it and learning techniques through there. And then I just put up over time and then I started doing the social engineering techniques and learning about that, et cetera. Keeping up to date with it is very, very difficult nowadays because as you can imagine, there are thousands of different systems that you can learn how to hack into and you can't know them all. So I have to specialise in certain areas, which is why I've essentially specialised in doing these kind of social engineering engagements where I do phone calls, physical intrusion email, LinkedIn, that sort of stuff, and then doing the training afterwards. So there are systems that I dunno anything about nowadays from a technical perspective, but I have the skills I can go and learn them if I need them. But yeah, it's a lot of work a day job and then it's researching in the evening. Lucky thing is, it's interesting, hopefully you found this presentation interesting. It's really cool to learn about this stuff, so I don't mind doing it at all.

Steph:

So I have a question that I thought of actually at the beginning when you were talking about the AI voice cloning. So is there anything that people can do to combat that or be able to I guess identify it if that is happening to them?

Rob:

Yeah, so there are a few things you can do. So the technology is still relatively early, so the clone sounds very good, sounds very similar, but there are certain things. So it will be, it sounds slightly posh and the intonation is wrong in various different areas. Also, normally when someone's cloning a voice, it doesn't work in real time. So I can't speak and have it yet, have it immediately respond in different ways with the converted voice very accurately. So normally what happen, I would type out script on the voice clone and I'll play that over the phone. If you then ask something that's off script, I've got to type out something else and have it say there's often a delay in there. So it's normally used for single things that I want to say, but the technology is coming on and on and on and we are starting now to see some real time translation into different voices and things.

That probably wouldn't be a thing you could do for very long. But the main thing with a voice clone is to think about what the person is asking you to do. So if you get a phone call from your CEO and it sounds like your CEO and he's saying I need to do an urgent money transfer into this bank account, that's where you've got to think, okay, would that be normal? Would my CEO EO phone me up even though it sounds like him or her, would they phone me up and say, you need to do this urgent transactions, we're always thinking about

the content of the message rather than who is telling me to do this thing. And then that's how you get around it and then it's just telling your staff not to respond to things like that that are urgent transactions.

Steph:

Going back to the question around the Excel and the word documents and what status just mentioned, what would your suggestion be as a secure way of attaching one of those documents with secure that sensitive information to send? Would it be like a sit file or something?

Rob:

So I don't tend to use email attachments directly, so I will use a secondary service that will send that file using a trusted system. I would agree with the person in advance. We are going to use this service, I'm not going to say any names but this file transfer service, I'll transfer this file through this that's coming. I've told you it's coming now it's arrived now you can open it, it's from me. And I'll often follow that with a phone call and I know that's a bit too much for every single attachment, but sending it through a file transfer service is often the way to do it. Sending it as a zip, it almost certainly won't get to the other end because zip files are one of the most common things used for phishing attacks. So they'll trigger alerting systems and quarantining and the sorts of stuff. So you probably won't get as it far through.

Steph:

I think just one other thing that you touched on at the beginning as well was around social media just to make people aware of what content and activity that they are putting out there from an individual perspective, but also for the company as well and how easy it is for you for the criminals to gain that information. So I think that's just more of an awareness thing.

Rob:

Yeah, absolutely. So during the training I mentioned about how I use LinkedIn to find email addresses, to look for posts from marketing teams, et cetera. This is something I'll use all the time and I can go into a lot more detail about that. But I will actively target not just the corporate social media pages of the company and look for anything of interest. I'll also look for individual within the company if I've got enough time, I'll be looking at every single person's Instagram accounts to see what they've posted, whether it's of interest to me, whether it's a photograph from inside the building that I'm targeting, for example, even does it give me a reason to fish them? So have they stayed in a hotel on holiday and I can pretend to be that hotel and say they've left an item behind and here's an attached photograph. Anything that gives me a reason to send them an email. I use social media all the time when I'm targeting companies. So you've got to be very careful of what you are sharing. And when I did the expanded version of this training, I go into a lot more depth about how to stop yourself revealing that information.

Steph:

Brilliant, thank you. So one of the other questions we've had is will the recording be sent out? So yes, we will send a link to the, I do realise the RNA, but we will send a link to the recording. It is hosted on our website so you will be able to see that it is a genuine URL. But yes, we will aim to send that out to you next week. So again, please do feel free to share that. So we've just got a couple more questions and they are, so the first one is I also understand criminals are now appearing on a teams call impersonating people in the organisation where we need to physically meet the person to agree this transaction. And is this a new phase and I guess is this something that you've heard of recently?

Rob:

Yeah, it is. Yeah. So you probably heard of deepfake videos as well where someone is in real time, this technology just come around in the last few months in real time, someone is able to swap their face for someone. So we've seen cases where A CEO has appeared on a teams call and asked someone to do something with a face swap in real time. So yes, the technology is there to do it via Microsoft teams. It's very difficult to defend against. Again, it's training on what to look for. Again, it's talking about what that person is asking you to do. The criminal always has a goal, they're always looking to make money. So you got to think about whether they're doing something that could allow them to achieve that goal. I know it's very difficult though because obviously you have meetings and stuff in real time, but it is quite a lot of depth to go into how to spot those deep fakes. And if you're interested, please feel free to drop me a message on LinkedIn. I can go a bit more detail with you. But yeah, the technology is improving. I've been doing that test against companies with real time teams calls to see if I can trip with into transferring stuff over. So I know it works very, very well and you've got to look for those things. What are they asking to do? That's always the message.

Steph:

Brilliant, thank you. And one more question is around when you have an inbox to receive invoices, how would you manage this attachment issue?

Rob:

Yeah, so that's one of the hardest challenges for organisations is when they have to receive attachments for example. For example, you gave, but also if you are advertising for a job and people who are sending you CVS and things like that, you've then got to rely on the defences you have in place outside of the training I've talked about. So if you have an inbox that's purely for invoices, you're going to need to open those invoices, right? So you have to have other mechanisms in place and cybersecurity is all about putting layers in place. So on that computer that you are using to open up those invoices, you should have software called EDR. I believe there's a question coming up about that in a sec that scans those documents to see whether they're real or not. It can open up within what's called a sandbox and it will see what it does decide whether it's safe and then a layer to open it if it's safe. It's having those extra layers of protection in place on those computers where you have to open up those files. So yeah, it's just about layering different defensive systems

Steph:

And yes, there is a question around what's your view on endpoint detection and response software? Is it worth having?

Rob:

Yes, a hundred percent, a thousand percent, yes. You must have EDR effectively on every single computer endpoint that you use. The reason is that if an attachment does make it past your first line of defence, which is your email gateway and then your staff deciding whether to open it, the EDR is the next thing that kicks in. Yes, there may be a way getting around the EDRI can design PDF files, et cetera that will evade most known EDR until it catches up, but it still catches nearly everything before that point. So yes, having EDR is great, make sure that you've got it across your entire state so you've got it on not just your endpoints, you've got all your servers, you've got your Linux devices, your Mac os, et cetera. So make sure you've got an EDR solution that works across all of those. That is your next layer of defence after your staff is that. And then perhaps you have another layer off that which is your network detection and then you have another layer off that which is stopping stuff exfiltrated from the network, et cetera. But yeah, absolutely EDR definitely have it.

Steph:

Brilliant, thank you Rob. And the final question is will you share the slides? Yes, we will share the slides with you. So if there's no further questions, I can't see any more coming through on the chat. Obviously as Rob said, his contact details are up there. Please do get in touch with Rob anything if you have any questions or if you'd like to engage Rob in terms of training for your company's charities. So thank you so much for joining us, it's been great to have you all with us and we do hope that you found it useful. If you do have any feedback, again, please do feel free to send that through to us. When we get in touch with you with the slides and things, there'll be a feedback survey sent out as well. So again, please do do that and we will try and do these again going into 2025 because we have had some really good feedback. So if there's nothing else from anybody else, we'll sign off now. But thank you very much for joining and thank you very much, Rob for the presentation.

Steph:

Thanks everyone. Thank you.