Protect Your Organisation. Protect Yourself.

Rob Shapland | Ethical hacker and cyber security expert

Steph: Okay. Good afternoon, everybody. Thank you very much for joining us today. My name is Steph. I run the deposit solutions team here at United Trust Bank, and I'm joined by my colleague Niki, who you will all have got an email from this morning reminding you to join this webinar.

So we'll kick off now. Hopefully, some more people may join us as we go, but it shouldn't affect the presentation in any way. A government report published in April 2024 showed that half of businesses and a third of charities experience some form of cybersecurity breach or attack in the last twelve months. We at UTB understand that this is a really important topic for our clients and our contacts.

Rob, who's joined us today here, is an industry expert and an ethical hacker, and he's going to spend the rest of this hour speaking to you about cybersecurity, how you can protect your organisation and, most importantly, yourselves. Any questions for Rob can be submitted on the webinar chat, and we will answer those at the end. So if you do have any questions that you think of as we go along, please do pop them in the chat, and Niki and I will ask Rob them on your behalf at the end.

If you can't use the chat for any reason, then please do feel free to email Niki. As I said, you should have got an email from her this morning, but her email is ncole@utbank.co.uk, and Niki will be keeping a close eye on her inbox. We really hope there won't be any IT gremlins in the room with us today, but if there are, please do bear with us. Our IT team are here on hand to be able to help us, so we will get anything resolved as quickly as we can. But I will now hand over to Rob for the presentation.

Rob: Thanks very much, Steph. So nice to meet you all. Thanks for coming to this webinar. First of all, first things first, I'll introduce myself. So, my name is Rob Shapland. I work for a company called Falanx Cyber, part of a larger group called Wavenet, and I work as an ethical hacker. So what that means is I get hired by companies to effectively pretend to be a cybercriminal, break through their defences, and then, rather than stealing all the information and selling it to other cybercriminals or encrypting it all and demanding a ransom from you, I then show you how I did it. So the idea being, if you are targeted by those real-life hackers, hopefully, everybody put defences in place for you, at least helped you do that.

Now, there's two main ways to do that. The first is through technical cyberattacks. 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 with pink hair, tattoos. They'll be watching these huge monitors spinning around and passwords slotting into place, listening to banging techno music, all that sort of stuff. I wish it was like that, honestly, if it was, I'd be so happy. My goal in life is to eventually build a basement in my house that looks exactly like that. But it's not really like that in reality. It's people in their studies, bedrooms, etc., or even in office buildings, working as hackers for a larger group trying to break into companies to make money in the vast majority of cases.

But I'm not going to cover too much of the technical side of hackers in this one. Unless you work in IT, it's not going to mean a lot to you. So what I am going to talk about is the other side of hacking, called social engineering. And this is how the vast majority of people are

hacked, is through someone clicking on a link or an attachment within an email, or a LinkedIn message, or an Instagram comment, or any other way they could be sent it. Or maybe I pick up the phone, and I pretend to be from your IT service desk or your outsourced IT company, and I need your password for something. Or my specialist niche within what is already quite a small industry, as you can imagine, is dressing up and breaking into buildings, so literally into your office building. I will dress up as an employee using a fake badge that I've created, or perhaps a cleaner, or an environmental technician, a fire alarm fixing guy, like whatever I think will work to get me inside. Then once I'm inside, find an empty meeting room, plug in and hack in from inside the building, therefore bypassing most of the cybersecurity controls.

When I'm not doing either of those things, I do a lot of training. One of the main things I do alongside what I've just talked about is awareness training for staff, making it a bit more interesting, telling stories, making people care about cybersecurity, rather than just making it a thing. You have to tick a box saying, I've done my training trying to do it, something a bit more effective, shall we say, do a bit of writing for magazines. And then I like to do a bit of media work for BBC, ITV, and a few others to illustrate cybersecurity to the general population that doesn't really care about it. And make them care in some way, make it more relatable.

So, as I said, thanks very much for joining me this morning. We're going to talk through a story mostly. So I'm going to be talking about a breach that I did, a company that I hacked into, and it's going to illustrate a lot of the ways that criminals might break into your organization, but probably more importantly, how you can defend against it as well. And I wanted to start off thinking about how you might actually be breached. When we see on the news that a company has been hacked into, how is it? Has it happened? Why has it happened? What are they doing?

Broadly, there are two main ways to break into a company. You can target a company directly. So if I wanted to break into your organization, I might do a whole bunch of research, I might find some holes in the systems, I might find a person that I think might respond to a phone call and give me a password, and then I execute that tact and it breaks in. Or in many cases, what happens is you fall victim to a kind of mass attack that doesn't care who it's targeting. It goes after thousands of thousands of companies and they're just kind of playing a numbers game. So they might be sending out the same phishing attack to 10,000 companies, hoping that just a few fall for it. Or they might find a particular system that you use is vulnerable to some exploit that the hackers have developed. And they look for anyone that's running that system, they don't care who they are, and then they pinpoint that, and then they target that organization because they're running that particular system.

So most organizations are breached through this kind of spam, that attack, but some are hit through these kind of targeted attacks as well. And when we talk about breaching a company, there's two main stages to it as well. The first is what we call initial access. It's getting through those outer defenses. So all the things you put in place to defend your organization, like firewalls, antivirus, staff training, all those sorts of things, how do we get through those? How do we get inside the system? And then when we do do that, what do we do after that? And that's where we try and find the information that might be worth money. Or we take all the data stored on the network and we scramble or encrypt it, which is called ransomware, and then we demand a ransom payment to unlock it, and we make money that way. So there's this kind of two-stage process to breaking in.

Some of you on the call will be working for charities. So I wanted to include this little slide to say, why are you more vulnerable? And one of the reasons is budget. Nearly every company suffers from this, but charities even more. So. It's how do you have enough money to defend yourselves against the sophistication of cyberattacks nowadays, especially

when you feel like you probably should be spending that money on more and more pressing things that your charity is doing? But actually, if you don't defend yourselves, it can undermine everything else that you're doing. So it's how to spend that money in a kind of useful way, in a way that actually protects you. You tend to have a high volume of staff as well, high turnover, you have a lot of volunteers or temporary staff, etcetera. It may be difficult to make them both care about cybersecurity and also get involved in it and understand security policies and all that sort of thing. It's generally more use of personal devices as well, and it's quite hard to push out the security updates onto those devices and again, make people care about using their own devices in a secure way. And even with the budget you have, it's really quite hard to know how to spend it accurately. Every company suffers from this. If you've got a budget of 10,000 pounds, how do you spend that money in such a way that it defends you in the best possible way?

So, in this presentation, we'll be talking a little bit about the most effective security controls you can put in place after I've talked about how you actually get in as a criminal in the first place.

So let's go on with the story. So, my job as an ethical hacker, what usually happens is I will get contacted by an organization that wants to know how well defended they are. So perhaps they've spent their budget on cybersecurity for the year, they've bought some systems in, they've done staff training, etc. They've got physical security controls on their offices, but they don't know whether it works until you've been attacked. How do you know whether what you've put in place is actually suitable to protect yourselves against criminals? So rather than wait for the criminals to break in, and then you find out afterward that it wasn't good enough, why not get someone in to actually test it and see whether it's working? Then you can find out whether the security systems are actually up to scratch or not.

So that's how it will work. Someone will contact me and say, can you try and breach our defenses? And I'll usually say to them, can I have an objective, please? And I'll say to them, what's your crown jewels? What's the worst thing that you could possibly lose from your computer network in terms of data? And often it will be customer information, clients, donors, that sort of thing, their personal details, because if those go, then of course it's extremely embarrassing. It's really bad for those people as well. So I'll usually go after something along those lines, but I'll talk with the client to find out what the most suitable thing to go after is.

Then the first stage, once we've defined that, is to start the planning of the attack. So imagine that you are the criminal. You put yourself in those shoes and you're targeting a particular organization. You're going to want to do some research about who they are and what they do and where they're based and all that sort of stuff. So you start off on the company's website, you start to look at all those things. The idea is we want to identify any particular weak points within that company. Are they running a piece of software that's 15 years old, they haven't updated, but I can just run a really easy script against it will give me complete access to that device and I can use that. If I look at their building, can I see there's like 20 different entrances and I could walk into any single one of them and that's how I break in. Do I see any evidence that the staff might not be very well trained or anything like that? It's a little bit harder to find, but there's a lot of poking around you can do to try and find out the weaknesses of the organization and the company.

I'm going to tell you a story about a pharmaceutical company, a pretty large pharmaceutical company, mostly UK-based, pretty well defended, or at least they thought they were pretty well defended, but they contracted me to try and find out whether those defenses actually work, as I mentioned. Now, with this company, I started off with the first stage of the research, which is known as OSINT, which is just a posh way of saying

research on the Internet. It stands for open-source intelligence gathering. It literally just means me searching for stuff on the Internet. So at a very basic level, looking at their website, looking at Google Maps, where their offices are located, etc. And the company in question had 15 offices dotted around the UK in various different places. And I could look on Google Maps and Street View and Orange man, you can drop on the map and you can get kind of a virtual tour around the building almost allows you to pinpoint potential entrances and weak points. So 15 offices. So quite a selection of offices if I want to physically break into one of those offices. They had their main website and then they had a lot of other services called SaaS, which stands for software as a service. So the kind of cloud-based systems that most companies use nowadays, like Office 365 and Google, things like that, they had a smattering of different ones. Of those, they had around 25 computers facing the Internet. That is, I could kind of see them and do stuff potentially with them. They had their Office 365 for their email and SharePoint and all that sort of stuff.

One of the main things I do when I'm researching companies is I look at their corporate social media pages. So most companies nowadays will have an official LinkedIn page, an official Instagram, Twitter, maybe even Facebook as well. And it's normally at the bottom of their website. There'll be links through to their social media pages, and I really like to look at those because they have all sorts of interesting information available because they tend to be run by the marketing teams of a company and maybe they don't have security in mind that much. So it allows me to find perhaps photographs inside the building of the company. It might allow me to find pictures of people wearing their work ID badges that I could then make a replica of that badge.

Sometimes I can dig into individual people's LinkedIn profiles and see if they talk about what experience they have. So if they're an IT employee, I can look through their profile and say, oh, they've got three years of experience using Office 365 and they've only been working for three years, and it's all been for this one company. So I know that company uses Office 365, gives me a little bit of information. I'll even look at job adverts through LinkedIn and indeed, and things like that. If they're advertising for an IT job, what experience are they asking for? Because that implies they're using those systems and allows me to customize the attacks based on that. Sometimes I've even seen firms that are advertising for employees will have little virtual tours of their office. You can see how cool a place it is to work with the table football and stuff, but that gives me an exact layout of that building. So if I'm going to break in there at some point, I know exactly where I'm going. I don't have to look lost. I know the exact way to the server room or to the meeting rooms that might be empty etcetera.

There's loads of information you can find out online. LinkedIn also gives me your email address. Now, not directly, you can't see someone's email address on LinkedIn, but you've got their name and you've got where they work. It's not going to take a genius to work out what their work email address is based on that. It's probably going to be first name, last name at the company's website address. And if that's not the email address format, a quick bit of Google, you can easily find out what format they use and then take the names and apply it to that format. So using that against this company, I was able to identify about 100 staff email addresses that I could use to potentially do a phishing attack where I might trick someone into opening up a link or attachment.

So I've got all this information from the OSINT. This is just a sample of the sources you can use. There's all sorts of stuff you can do. You can go onto council's websites and find out, like architectural diagrams and blueprints and planning permissions and all sorts of stuff. There's loads of things online that you can find. But this is a small sample of the stuff that I tend to use, mostly Google Maps and social media is the main ones that I'll use to kind of research a company.

Now, this company had tasked me with breaching their defenses, getting onto their computer network, and gaining access to the designs of a new kind of drug that they developed. So, as I mentioned, they're a pharmaceutical company, they spend lots, lots of money on research and development, and they tasked me with breaking in and finding this design they just developed. They were just about to go public with the information and it was a really quite revolutionary treatment. So they thought what would happen is they'd be targeted by perhaps Russian, Chinese, Iranian cybercrime groups that would be looking to break in and steal this information and then sell it to other companies, potentially could produce it on the cheap. So they asked me to come in and try and break in and steal this information.

And I wanted to do a number of different attacks. So I wanted to do a phishing attack, so an email, get someone to click on something and gain access. I wanted to do a phone call-based attack and I wanted to do a physical intrusion, so a literal break into one of their offices. So I planned three separate styles of attacks to see which ones would work. Maybe they don't work, maybe just one or two of them would work, so they could learn the most they possibly could of the kind of attacks that, excuse me, the criminals are doing. Sorry.

So the idea behind it is that different criminal groups will use different styles of attack. So if I can simulate those different styles, I can help the most in how to defend against it. So the first breach I wanted to do was a spear-phishing attack. Now, what spear phishing means is not just a blanketed phishing email to lots and lots of people. It means targeting one or two people inside the company with a specific attack.

So I found on LinkedIn, as I mentioned, there are 100 different employees. I took those names, and I started to search for them on other social media platforms. So through Instagram, through Facebook, through Twitter, to see if I could find any information on their personal life because there's this kind of mix nowadays between your personal life and your work life. And I'll illustrate what I mean by that. So I found one of their employees on Instagram, and he hadn't used the private account option. So even when I'm not friends with him, I could search for his name and see all of his photographs. And this particular employee had just come back from a holiday.

I think he'd been in Tenerife for the last week or so, and he'd come back and he'd put all his holiday photos up online. So I was looking through those holiday photos, trying to find anything that might be of interest. And in the background of one of the photographs was the name of the hotel he'd been staying in while he was away. So I thought, okay, is there a way I can use that information? And this is the kind of fun bit about designing these attacks, is you think about, how could I make him click on something? How could I make him click on a link or an attachment? And I thought, okay, what if I pretend to be the hotel that he stayed in and maybe say that he's left something behind?

Playing on curiosity, a lot of these kinds of phishing attacks play on emotions. If I can make him really curious about what he might have left behind, maybe I can trick him into opening up something that looks like a photograph, but actually is a piece of malware, a virus that will give me access to his computer. In order to do that, I need to design the attack to make it as believable as possible. So I quickly googled the name of the hotel that he stayed in in Tenerife, went to their website, and had a look at the website address, and it was quite a long address. And I thought, what I'll do is I will buy a website name that looks really similar and send him an email from that.

Now that's really easy to do. You can go on. There's loads of websites allow you to buy other website addresses. So I bought a website address for about five pounds, I think it was. And what I wanted to do was send him an email from that address. Now chances are

he wouldn't even know what the email address of the hotel he stayed in was. I mean, would any of you know he got back from a hotel? Would you really know what their email address was? If you got an email that looked like it was that hotel, you probably believe it. But to make it even more believable, I copied all the logos and stuff, the colors they use on their website, the fonts and everything, to make the email really, really believable.

And I sent him an email from that fake hotel saying, hi, we hope you had a lovely stay in our hotel last week. We think you may have left some valuables behind in your room. Please see attached a couple of photographs. Could you let us know if they're yours or not? That's a really convincing hook. You might be panicking about what you've left behind. At the very least, you're probably quite curious about what might have been left behind. So he double-clicked very quickly to open up this photograph.

Now, I'd made this email attachment look like a photograph, but it actually wasn't. And when he opened it up, it just said, cannot open file. But what happened in the background is I put like a virus in there. That gave me complete control of the laptop he was using at the time. Now that's relatively easy to do. I'm sure when you're an ethical hacker, you can design software that will do that. And it's not like in the movies. Whenever a device gets hacked in the movies, it goes all sort of corrupt. And the matrix things appear with the greenhouse flowing, text on a black background and everything like that. And maybe a laughing face appears and stuff.

It doesn't work like that in reality. It all happens in the background. You won't even know. And then I'm just kind of lurking there on your laptop. I can see everything you're doing in real time. If you're connected to your work network, if you happen to be on your work laptop and you opened up that email, I can see all that. I can connect to other devices on the work network. I can turn the webcam on and have a look at it. You can access all your passwords you've got stored in the browser, all sorts of stuff just because you double-clicked on an attachment.

So by tailoring this attack directly to him, using the information I'd taken from his Instagram profile, he made it much more likely that he would actually interact with that. And what happened is he replied to the email and he said, I'm really sorry, I can't see the photograph, it's not working. And I said, oh, don't worry, we've had contact from someone else that stayed in your room afterward to say that it was their items, so no problem whatsoever. So then he forgot about it. But he hasn't realized, of course, that now I'm in his computer and even if he turns his laptop off when he turns it back on again, I've got a little program that will kick in and it'll give me access again. So I'm now inside his laptop and effectively inside the network of his entire company. So that was my first breach and first way into the company. We'll talk about defense against this sort of stuff a little bit later on in the presentation.

So we'll go on to the secondary breach. And this was done by a phone call. Now, you might have seen a lot of stuff on the news about companies being phoned and using AI, voice cloning, and all sorts of stuff. So I decided I wanted to do an attack that was based around a phone call. Now, for this company, they had information on their senior directors available on their website, so you could click through to individual profile pages on their website, and it listed the contact details of their senior director's phone numbers, email addresses, etcetera.

So really, really handy for me to have a number to call him on. Now, usually, when you're trying to log into a company's systems from the Internet, you have to log in using the same systems that they do. So imagine you're on your Office 365 email and you're working from home. You have to log in with your username and password, and you'll often have

something called multifactor authentication. Alongside that, you have to log in with a separate code that gets texted to your mobile. Or maybe you have an app on your phone that has a rotating code that you log in with as the hacker.

In order to get into your email system, I'm going to have to get past both the username and password and that multifactor authentication thing. This is where the phishing phone calls come in really, really handy. So this senior director, as I mentioned, had his details available online. Now I have kind of a search engine that searches the dark web. And you may have heard of this on the news, it's kind of a hidden part of the Internet. You access it with a special browser. There's lots of dodgy stuff on the dark web, but one of the things you'll find on there is a list of usernames and passwords that have already been hacked into. So what's happened is a website that someone's registered to has been hacked, and the passwords have been stolen from that. And that's happened thousands of times over the years. Loads of websites have been hacked in this way, and the list of already hacked passwords is now up to about 13 billion across all the different websites that have been hacked over the years. So lots and lots of people are in this list. Most of you will be. And again, I'll talk to you about how to search this list yourself later on in the presentation.

So I used my little dark web search engine to search for this guy's email address. And he'd been breached, as in his email address and password had been stolen a number of different times. And looking down the list, the password he'd used for all the different websites that had been hacked was the same. And it's a really weak password. It's based around the word password. So I thought, okay, if he's used that password four or five times for different websites, there's a strong chance he's using that everywhere, as a lot of people do reuse the same password across lots of different places. So I thought I'll try logging in as him with that password into his Office 365 email and see if that gets me in. So I typed in his email address that I'd got from the website. I typed in the password that I got from the dark web search, and it worked. It let me in, but it triggered the multifactor authentication, which is why multi-factor is so good because even with the username and password, I still can't log in. But if you're clever and use phone calls, you can still get around that.

So what I decided to do was pretend to be one of their IT employees and see if I could trick him into allowing me through the multifactor authentication. So what I did was a little bit mean in a way. I signed him up to a kind of a mass email spamming service. So within a couple of minutes of me signing him up, he got hundreds of emails coming in. Now, I thought, I'll swoop in as IT tech support and see if I can fix the problem for him. Now I got really into this and I wanted to make it as believable as possible. So I started to research some of their IT employees, and they had about ten different IT employees. I took those names of their IT people that I got again from LinkedIn, and I searched for them on YouTube to see if any of them had ever done any presentations or anything like that. And there was a video of one of their IT guys speaking at an IT conference. There's an hour-long video of him doing a presentation on something. So I had an hour-long sample of his voice. Now, you may have seen in the news stuff about AI voice cloning. If you can take a couple of minutes' sample of someone's voice, you can then create a replica and get it to say other things. You might have seen it recently with Gareth Southgate saying funny things on Twitter that they didn't really say. So there's all sorts of funny uses for it, but also there's some malicious uses of it.

So with the sample of an hour of his voice, I was able to create a very good replica of his voice. So I thought I would use that to phone up this target, this person I'm going to try and trick with the IT person's actual voice just in case he knows it. To be honest, it was probably overkill. I probably didn't need to do that. I probably could use my own voice. It would have been absolutely fine. So bear in mind, he's got this mass spam of emails coming in. I now phoned him up as IT tech support with the correct voice pre-recorded type stuff out. And it says it. So it said, hi, it's Tom here from IT support. We've seen a mass

volume of emails coming into your email address. Have you got your, is your email inbox being spammed? And he said, oh yeah, I was just about to phone you guys up. Having a real problem at the moment. I said, okay, no problem. What we're going to do, we need to log into your computer to resolve the issue for you. So can I. I'm going to log in for you. I've got your password already from it, so I'm going to log in. What you'll see is an authentication prompt on your phone from Microsoft authenticator. When that comes up, could you type in the number? It says.

So he said, oh yeah, no problem. So he gets this prompt on his screen to type in the number 23. He's got me on the phone, he types in number 23. That completely bypasses the multifactorial indication. And now I'm inside of. So although multifactor authentication is brilliant if you listen to someone else and you type in the number when you didn't prompt for that authentication yourself, it can be defeated in that way. So now I'm inside his email system, and I can access all his emails. And he'd been at the company for about 15 years. So imagine the volume of emails you've got when someone's been there for that long and all the sensitive information. And also I could start sending emails as him, so I could reply to existing email threads asking people to do stuff for me, asking them to send personal information, all sorts of things that you can do with that. So that phone call allowed me to defeat their defenses as well. So now I've breached the company twice already, effectively through the phishing attack and through the vishing as well. So that's two breaches done.

But I wanted to do a third breach and this was going to be a physical attack on their offices. So me getting inside, pretending to be someone I'm not, and as I mentioned when I was talking about the research phase, there were 15 offices that this company had around the UK. Now, I did a bit of research on Google Maps and Street View to have a look at which offices might be a good target, which might be a bad target. Now, they had a main physical head office, which was where the really sensitive information was stored. So do you remember the start I talked about? The objective was to gain access to a drug design. Now, this was physically stored on a computer in their head office, so they expected me to try and break into their head office. But I looked on Google Maps and Street View and their head office looked really, really secure. You could see from the street view images. There was only one main entrance, which seemed to have like a security hut at the front, and then around the side were all big fences with razor wire on top. There were no side entrances or back entrances, and I'm not allowed to cut holes in fences and stuff like that because I'm not allowed to cause any physical damage. So I thought that's going to be a really tough nut to crack because if that's what the defenses look like, you can imagine the processes and procedures and things like that that they have are going to be very good as well.

But I know from previous experience of breaking into companies, it doesn't generally matter which office you break into, any office you get into is all interconnected on the computing side. So I could probably break into one of their small offices and not even bother going anywhere near the head office, get inside that way and use that as my way to break into the company. So I thought, let's have a look back on Google Maps. Have a look at the office that's the weakest. And one of their offices was located on a high street in a small town surrounded by shops, just like a small admin office. I thought, that's going to be a great target because there's lots of foot traffic going back and forth, so I can go have a look at it myself and observe what the security might look like without causing any suspicion. It can't have big fences, it can't have security patrols and things like that, so it's going to be much worse defended than the main head office. So I thought that's going to be my target.

So I then went there about a week beforehand and just did a walk past. Have a look. What's the security look like? Appeared in the window, and all I could see was a single reception desk with someone behind it, no security barriers, and then a lift up to the top

floor where it looked like their office space was. And from seeing the number of people coming and going, it looked like there were about 15 to 20 people working there, and they were wearing ID badges. And I got photographs of the ID badge, and I've got a machine in my office that can print out badges and lanyards, any styling design that I need, so I can create replica ID badges and things. But I thought, I don't want to go in as an employee because there are only 15 people working there. Doesn't matter how good my replica badge is, if I walk in and sit down, people are going to go like, who's this guy? So that's not going to work. So I need to come up with another way of breaking in.

Now, bear in mind, when I get inside this office, I'm probably going to have to connect to their computer network to access the files I need to steal. So that limits what I can pretend to be. For example, if I pretend to be a cleaner, it looks really suspicious. The cleaner brings a laptop with them, sits down at a desk, and starts typing away. So you are kind of limited on the pretext, the way you're going to dress and act by what you've got to do when you're inside. So what I decided to do was to dress up as an engineer from BT, British Telecoms, because BT is everywhere, right? You see them on every street corner fiddling with wires and stuff like that. So I thought, maybe I can go in and pretend that their head office has got some sort of network problem, some sort of connectivity issue through to this regional office, and I'm here to resolve the problem. As you'll see, a lot of my scenarios resolve around there being a problem, and I'm there to help out, I'm there to fix it.

Now, in order to make that as believable as possible, I wanted to create an outfit that looked like BT. So relatively easy to do a Google search and find out what BT engineers wear or just walk around a town for an hour until you see one. So I designed a high-vis jacket based on the design that BT used. I then got myself like a bag full of tools and cables and all sorts of stuff that I could use to look like an engineer. I got myself a clipboard. When you're doing social engineering attacks, that is physical intrusion like this, having a clipboard is one of the main tools that you use because it just makes you look more officious and more like you're supposed to be. There. Had some paperwork on there with the BT logo and some work reference numbers and all sorts of stuff. I then had an ID badge that I'd stolen from a BT engineer's Instagram profile. So basically I went back to LinkedIn again. As I mentioned, social media, really useful. Searched for engineers, found various names and things like that that were registered as engineers that worked at BT. Again, search for them on Instagram. After quite a bit of research, I found an engineer, a photograph of him wearing his full uniform, holding his badge directly up to the camera. And it said something like, end of my first week at BT, tired, but really enjoyed it. But anyway, that gave me the exact design of the engineer's badge.

So now I could create a replica using my badge printing machine. Now of course, that's not going to get me into BT's offices, but that's not the point. The point is to make me look the part. And when you're doing these social engineering attacks where you're trying to break into a building, how you act and how you dress, it really helps with whether you're successful. If you look suspicious and you've got a dodgy-looking badge and you don't look the part, people pick up on that. But if you look the part, you act the part, then people want to believe you are who you say you are. My full outfit and my idea, as I mentioned, is to turn up at this office and try and convince my way in. So I've not booked an appointment, I'm just going to turn up and try and convince my way past the reception staff.

So I come into the office on a Thursday, Friday morning, I think it was, as I mentioned, as you come in off the street, there's a kind of reception desk on the right there. There's a lift up to the top floor and the left is a kind of waiting area with a glass table, water machine, kind of the stereotypical small office building. And I went straight up to the reception desk dressed as the BT person and said, hi, I'm here from BT. We've been booked in to run some diagnostics on your network. The head office called us to say there's been some sort

of connectivity issue between you and them. Shouldn't take me any more than about half an hour. Just need to plug into the network somewhere. Do you mind if I run upstairs and get started?

And she looked down at her guestbook. Now, my hope was she would just go, oh, yeah, off you go. That happens sometimes. But she looked down at her guestbook and said, I'm really sorry, I haven't got anything written down for you today. I haven't had any appointments booked. I need to verify with someone at head office. Were you given the name of someone?

Now, I had prepared for this because it was the most likely thing that would happen. And I've written down a name on my clipboard of a guy called Adam who worked in their IT department, a real employee. But I'd chosen Adam on purpose because Adam had put on his Facebook page. It was on holiday that very morning. So he checked in at Gatwick airport. He was flying to somewhere in the Caribbean, I think, and it was about 5 hours ago. So I thought, okay, Adam's not going to be contactable. So if I am asked for a name, I can give his name, she'll try and phone him, won't be able to get hold of him. And then maybe if I keep laying on the pressure, saying I've got another appointment coming up, maybe she'll just let me in anyway.

So she tries to get a hold of Adam, can't get through to him, comes back to me and says, look, I'm really sorry I haven't got hold of Adam. And I said, well, I'm going to need to get up because I've got another appointment in an hour or so. He said, there's nothing I can do. I can't let you in until I've spoken to Adam. The problem is I'm really busy. I've got some urgent meetings to go to and some calls to make and things like that. I'll tell you what, you try and get hold of him, I'll give you his number. So she gave me a post-it note with Adam's phone number on it. Then she gave me a post-it note with her phone number on, and she said, if you manage to get a hold of Adam, put him through to me and I'll check. It's all right for you to come in.

So I thought, oh, okay, I reckon I can work with this. So I took these two phone numbers and left the office, waited about five minutes, phoned my office, and said, could one of you guys phone this number, the receptionist's number, pretend to be Adam from IT at this company and say it's okay to let the BT engineer in. So one of my colleagues does exactly that, speaks to the receptionist, completely convinces her. I walk back into the foyer, and she says, oh, I've just spoken to Adam. It's fine to get you in. So she brings over the guestbook, gets me to sign in, and gives me one of those visitor badges. And I love getting a visitor badge when I'm breaking into buildings. I love it because it then means that people can look at me and go, okay, he's been through reception. If I sneak in the back door, I'm always a bit on edge, but having a badge makes me feel very calm and collected.

So I'm just about to go upstairs in the lift, and she says, oh, no, hold on there for a minute, I'll call down our IT person to help you out. And at that point, my confidence completely crumbles because I did not expect them to have an IT person in such a small office. There is no network problem. I've completely made that up. And even on the off chance he lets me in, how on earth am I going to hack their network if I've got an IT person sat next to me the whole time? So I think, okay, you know what? Should I walk away now and pretend I've got another appointment or whatever? But I thought, no, no, no, let's just see what happens. A real BT engineer would actually be quite happy that an IT person was there to help him out. So let's play it out and see what happens. I can always make up an excuse and leave halfway through.

So the IT person comes down, and he comes over to me and says, I'm going to be honest, I don't really know why you're here. We've not got any network problems. I've not heard

anything from head office, but the receptionist over here says, oh, no, it's okay, I've just spoken to Adam at head office. He said there is a network problem. They're not really sure where the problem is, whether it's this end or their end, but they've got the engineer booked in, so we need to give them any help. And the IT guy just shrugs and says, okay, fine, if you want to come with me, then we'll get it sorted. So we go up in the lift, we go up to the top floor, the lift doors open, he turns around to me and says, the weird thing is we don't even use BT here, but coming anyway.

So despite the fact they don't even use BT at this office, he still let me in, which is why I pick them as a normal company to pretend to be because there's always something that must be owned by BT in the walls or whatever. So we get inside, and the office is really small, as I mentioned, there's about 15-20 people working there, but it's quite crammed in. I'm sat right next to the IT guy, and he says, is there anything you need to get working? I said, I need a network cable to plug in to get me one of those. What I really need is for him to go away. So I said, would you mind making me a cup of coffee? And he said, oh, yeah, no problem. I said, do you think you could get me a cappuccino, please? He sort of frowned at me a bit. That's a weird thing to ask. And then went, yeah, I'll give it a go. So he disappeared off. I thought, maybe that buys me a little bit of time. But he came back about a minute later. It turned out the machine just had a button. He pressed cappuccino on. So he's back next to me in no time.

Now, luckily, I've downloaded the BT logo onto the background of my computer, and I've got some graphs that measure network fluctuations and things, so it looks like I'm doing something legitimate while he's sitting there watching me. But after about 15 minutes, he said, I'm really sorry, I've got a meeting for the next hour or so. Will you be okay on your own? You can give me a shout if you need me. It's like a big sigh of relief from me. Yeah, absolutely fine, no problem. So he disappears off. Now I'm left on my own. There's other people around me, but they're not paying me any attention because I've come in with the IT guy. Now I have an hour on my own on their computer network.

Now, as I mentioned, I'm not going to get too technical on you during this presentation, but most of what it is when you're inside a company's office is guessing people's passwords, and you can do it really, really quickly when you're inside an office. Now, one of their employees, a different senior director this time, had a very weak password, again, based around the word password. I think it was something like password 24. So I reckon he probably started about eight years earlier with password one. And then the IT team had made him change his password every couple of months. He made it 234567 all the way up. So I was very quickly able to guess that password. He had access to everything. And as I thought, I could access the head office network from this small office, connect through, and then steal the designs for the drugs that I'd been tasked with getting, getting hold of the treatment. So from my perspective, I've got, in three different ways, breached the company.

When I'm doing the physical intrusion, I record it on hidden cameras, and I use that as part of training. So when I'm doing awareness training for companies, I'll use phishing attacks I've done, I'll use video of the buildings that I've broken into and make that into really interesting training. And if they don't want to do that, I'll just use stories like this to illustrate the points. So it makes it much more engaging for them, and they're able to learn a lot more from it. So from this, from my perspective, I've got in, got out, very, very happy that I've been able to breach this company multiple times.

So with that story finished, I wanted to illustrate some of the main ways that you can be broken into and how to defend against it. Now, some of this is very applicable to your personal life as well because your own email address could be breached and then your own personal computer or phone a hacker could gain access to. And I'm going to talk about

passwords in a minute. Of course, all of us have got far too many passwords. So when we see a company on the news that has been hacked, has been breached, it's nearly always done through a phishing attack. So similar to the story I told you of pretending to be from the hotel that he stayed in. Or maybe it's even less targeted than that. Maybe I just send out an email to everyone pretending I'm from the IT department and they need to enter their password or whatever.

There's a few different things you can do to defend against phishing attacks. So the main thing, when you have an email come into your inbox and it's got an attachment in it, it's got a link in it, or it's asking you to do some sort of financial transaction or send over any of your personal details. What I want you to get in the habit of doing is checking the bit after the sign. So I'm not worried about the bit before. So the bit after the sign. So say you had an email from Apple and it's saying you've bought something from the App Store and you don't recognize the transaction. The idea is the criminal is trying to make you feel a bit worried or a bit angry. Angry enough that you click on the link that says, if you didn't authorize this purchase, please click this link, you click on that link, it goes through to what looks like Apple's website and you log in. But because you're angry, you didn't think to check the email address. And actually, when you look at it, it's from Apple-Dash billing.com, which is actually nothing to do with Apple whatsoever. That email would have to come from Apple.com dot. And if in any doubt whatsoever, you just google the company and you log in through their website rather than the link you've received in the message itself. But I really want you to get in the habit of checking this bit after the sign. Does it match up with the company or the person that supposedly sent that message?

Now, if the phishing or the message has come through some other means, if it's come through a text message or through WhatsApp or LinkedIn even, do you trust the person that sent you that message? By its nature, LinkedIn is quite impersonal. If someone's sending you a message through LinkedIn with a link in it, I wouldn't click that. I don't know the person. Similarly, if you get a text from a random mobile number and maybe they say, hi, mom, it's me, I've lost my phone, this is my new number. Hang on a minute. I need to be very suspicious of this because, yeah, it could be my son or daughter who lost their phone, but it's also a known scam that criminals use. So maybe I don't want to interact with this message at all. Maybe I ask them for some personal details, I give them a call and check that it's actually them because that's a scam that's going around at the moment. So you have to be very untrusting with everything, but especially stuff that's come through text messages. WhatsApp LinkedIn, etcetera.

Now, just occasionally, you will get a message from someone you know. So it's come from their real email address. It could be a friend, colleague, supplier, client, customer, donor, whatever. And you look at the message and you think, well, that's come from their real email address. But it looks really weird. It's. By suddenly the spelling and grammar is all strange. They're asking me to click on this weird link or open some strange attachment that I don't recognize. What could have happened in that case is their email address has been hacked into. This is a very common thing that criminals are doing. They're targeting companies that maybe haven't got very good defenses, hacking their email systems, and then sending email to other companies those companies deal with in order to hack into their systems.

So if you do get an email from someone you know, but it looks really, really weird, trust that gut instinct to report it into your IT person or your outsourced provider. And all of this is very much enhanced if you feel like you really want to open it. So like I said, if you get an email from Apple makes you angry. I don't recognize that transaction. I need to sort this out. Or you get an email from your bank saying, there's been some fraudulent transactions, your account's been frozen. You must click the link below in order to unfreeze your account. It's trying to create panic. Or maybe you get an email from the chief financial officer of your

company saying, we do this urgent supplier transaction and it looks like it's come from them, they're in authority, so it puts a bit of pressure on you. Anything like that, where you feel pressured, you feel scared, but on the flip side, you feel excited. Something good has come into your inbox, you've got a special offer for something, or a free Amazon voucher, anything like that, where you're asked to do something and you feel very much compelled to open that link or that attachment. That's when you really want to go back and check that email address or check where that's come from to make sure it's really, really real.

So that's phishing. There's obviously lots more things I could think I could talk to you about with phishing, but the main things you want to look out for are next threats we talked about is phishing phone calls coming into you. Now, if you do get a phone call from your IT team and they ask you to verify your identity or log into something, or enter your Microsoft authenticator number, or give over your six-digit number that's been sent to your mobile. Do not do that. There is literally no reason why you should ever share your two-factor or multi-factor authentication code with anyone, including your own IT team. So that's yours only for you. If you didn't request that number to come to your inbox, then you don't do it. You don't do anything with it.

But one other thing I want to talk about with phone calls is what criminals are doing at the moment to scam you into sending over your money. So what they do is they pretend to be from your bank, so they phone you up. What they do is they spoof or fake the phone number of the bank itself so I could make your phone ring with your bank's name or number on the screen. So let's say you bank with Santander. It will appear to be Santander on your phone screen. So you answer the phone thinking it's there and thinking it's your bank. And then they'll say, hi, it's Santander. Customer service is here. Just a courtesy call. We've seen a couple of strange transactions on your account. Have you been shopping on? And they'll list out a couple of transactions that you haven't done, like really high-value transactions. The idea is to make you feel a bit panicked and you go, oh, no, I don't recognize those transactions. So they then say, well, don't worry about it. We'll put you through to our fraud team, who tell you what to do next. They then pop you on hold, but they put you on hold with Santander's actual hold music they've recorded. So you're on hold for a couple of minutes, and there's the normal hold music playing. Now, our friendly voice answers. This time it's Louise in the fraud team. Louise will say, well, during the time you're on hold, another transaction went through. Have you been on this website? And again, the idea is to make it sound like stuff's happening right now to make you feel more and more panicked.

Then Louise will say, don't worry about this. We're quite used to dealing with this. Unfortunately, we've got a process in place. What we're going to do is we're temporarily going to move your money into a safe account so the criminals can't steal any more of it. Then once we've resolved the issue, we'll move it back into your account. But for security purposes, we can't do that ourselves. So we're going to send you through a couple of codes to your mobile phone to make sure it's us. And that will appear to be from Santander as well because it will appear as their name. It'll even go into your existing text message history as Santander. It would join the other messages if you had from the real bank because they're spoofing or faking the phone number and the phone doesn't know any differently. So it's all very convincing. And they'll say, we need you to go into your online banking now, transfer your money into this account. And of course, that's the scam because now you're just transferring it into someone else's bank account. Or they might direct you to a website. They'll say you need to download some security software to prevent them from getting into online banking. If you go to Santander Dash security, dash Software.com, comma, download the file on there, that will secure your computer. And again, that's a scam because that's downloading a virus that gives them access to your computer.

So we don't want to fall for this, obviously. So the golden rule with all these types of scams is they always are the ones that phoned you. So what we do in order to avoid all of these scams is we never give any information away when someone's phoned us, whether it's our bank, our mobile phone provider, or our broadband provider. We always make sure that we are the one that initiates the call. So let's imagine that your bank phones you now. It's got something there on the screen. You answer. They say there's been a fraudulent transaction. What you do is you say, thanks very much, I'll call you back. No matter what they say, you put the phone down, you then look up Santander's actual customer services number on their website, on the back of your bank card, and you phone them up and you say, I've just had a call. Could I verify whether there's anything going on in my account or whether that was a spam call, please? And they'll be able to sort that out for you. You are in control at that point and that's always the case. So if any company phones you, even just ask you for security questions, don't answer them. That's your personal details. You do not know who is calling. You cannot trust what it says on your phone screen. I'm not being dramatic. It is very, very easy to fake a phone call to look like whatever you want to, so please believe me in that regard and please follow this advice. Also, please don't think that you are too clever to fall for these scams. I know a lot of people go, I'd never fall for that. It's really obvious I'll never transfer money into another account.

They're very good at what they do. This is their job. They are master social engineers on the phone. They're incredibly good. They've got whole scripts to convince you, etcetera. The fact they're passing you around between departments, putting you on hold with the whole music, etcetera, it's all part of that building up the confidence. They are who they say they are. They sound exactly like the bank. It's not, you know, Russian voices or Iranian voices, North Korean voices. These are British voices. It's organized crime. Or the voices run through a filter that makes them sound like they're British voices. And they also have a habit of just catching you at the wrong time. So maybe a week ago, you were looking through your online banking, and you saw a weird transaction, you didn't recognize it. It's probably legitimate, you just maybe didn't recognize the name of the company, you didn't remember the transaction. So in the back of your mind, you've got a note saying, I need to phone my bank at some point and see what that was. And you don't get around to it. But now, a week later, the bank's phoning you, saying there's been some fraudulent transactions, and of course, your brain makes connections, and it goes, ah, that must be to do with that one I had a week ago. I meant to phone you about that, and now you're sunk because they just jump on that and go, yeah, that was one of those dodgy transactions as well. And it all clicks together in your head and then you're a very easy victim.

So, like I said, don't think you can be too clever to fall for it. Whatever happens with your bank account, if you receive an inbound call, you don't do anything with that. You phone them back. And if they phone you on a landline, you make sure you call back from a mobile because what will happen is if you end the landline call, it leaves the connection open the other end, and then they still just pretend to be the bank when you phone them back. So make sure you always call back from a mobile when you're doing it.

Okay? So one other threat I wanted to talk to you about is the threat. Your password is stolen. So in your personal life, that could mean they gain access to your online banking or your mobile phone or to your social media platforms, your email, etcetera. In your work life. That can mean they get access to your work email and your work VPN, how you access stuff when you're working from home. So we don't want our password to be stolen. So I put a choice of seven different passwords there on the screen. Just have a look down that list and think, which one would I choose? If I had to choose one of those, which password would I go for? Would I go for 123456 or 7? Now, there are various sorts of good ways to choose passwords. Number one is not a good way to choose a password, but this is how most people tend to construct their passwords.

Most people want their password to be quite memorable, so they choose a name, a place, a football team that might be memorable to them. They put a capital letter at the start, that's where it goes in a name. And then lots of websites make you choose a number. So you just stick that at the end. And then if you're at work and they make you change your password, let's just make it Maggie two next time, Maggie three, or Maggie four Like I told you in that story that person's password was password 24. Just been doing that for years and years and years. Started with password one and worked his way up.

Now, many of you will be thinking that number three is the strongest password in that list because that's kind of what you think a good password looks like. But you might be quite surprised to show you that I can actually get access to that password within about 20 minutes of guessing it. And the reason for that, although there's nothing wrong with a complicated password like that, it's not strong enough. It's not long enough. What we want with passwords is long and weird. Okay. The longer and the weirder the better.

Now, I love green tomatoes is a really good example of a long and weird password. Now, you might just be thinking, but that's just English words. Why can't you just guess those words one by one and gain access to them? But that's not how the technical part of password guessing works. I can't guess tomatoes. And the computer goes tick. In the movies, it always, whenever they're breaking passwords, it slots into place one letter at a time. It doesn't work like that. In reality, I would have to literally have the computer type out, I love green tomatoes, then press enter. Now, it's not going to do that because I love green tomatoes is such a weird password that no one uses it. Therefore, we don't try and guess it because it's too weird. Now don't use I love green tomatoes. That's the password that I put as an example here. I've been using this for a couple of years. Probably. Maybe some criminals know about this. Now they've made it their list of passwords that they'll guess. You need to come up with your own password that you use and securing your own kind of passwords in your personal life and your work life is a three-step process.

Now, the first step of this process is to have a look and see whether our password is already in the hands of the criminals. I mentioned earlier about how websites in the past have been hacked into and the passwords stolen from there. And that list of hacked passwords is about 13 billion long. You can check yourself whether you're in that list or not. And the website you can go to is called have I been pwned. Pwned is another way of saying hack.com. You can just Google Hibp, click on the top non-sponsored link. I never click on sponsored links, by the way. It's another little tip for you. Always scroll down to the first non-sponsored link on Google, click on that, and type in your email address. So I try your personal life one, but you can try your work one as well. That will tell you whether you're in the list.

Now in the example there, it's gone green, which means I wasn't on the list. If it goes red, and for many of you it will go red. That means you are on the list perhaps multiple times. And it might mean they have the password that you've been using. And what that means is the website that you've registered to at some point with that email address has subsequently been hacked and your details have been stolen from there. So they have your email address and probably your password as well. Scroll down, have a look, a bit of the information about it. It might tell you what website it was taken from. More likely it will just tell you the date that it was stolen. Now you can think, okay, when was the last time I changed my password for my bank or for my social media or for my personal email? Maybe not for years. And since that date, my password's been stolen. That means the criminal has the password I use for my bank. So I need to go and change it. So that's the reason to move on to step two.

Though I'd strongly encourage you to move to step two regardless of what happens in step one. Now, step two is where we start using better passwords. What do I mean by better? Is

that long weird I talked about just now, the longer and the stranger the better. And the general advice, both for me and from the UK government, is to use pass phrases, sentences, collections of words, rather than a single word. Which is what I love green tomatoes, is. But please come up with your own one.

Now, once you've sort of come up with a password that you want to use, there's a couple of different things you can do. You can save them somewhere if you want to. So if you want to save them in your phone, so when you register to a new website, your Apple or your Google phone will say, do you want me to save that? It might even suggest a password to you. And that's fine. The passwords they suggest are brilliant. They're really, really long and complicated and very difficult to guess. So if you want to save that in your phone, I don't mind that at all. If you want to come up with your own password and save it in your phone, same thing. Don't mind, as long as the pin number on your phone isn't 1111 or something like that. Isn't your birthday, your date of birth, or your anniversary. Because if I physically steal your phone, I've only got a few guesses to get in. If you're using something really obvious, I can do it. If it's a random pin number, I'm not going to get in before the phone locks itself. So as long as you've got a random pin number, I'm happy if you just save your passwords into your phone. But if you don't like the idea of doing that, you can come up with a memory system. And the system I like to use is to come up with five different passwords. It's not too hard to remember these sentences, so five of them is not too onerous to remember. Make them funny. Make them do with the type of website. Whatever you want works for you.

So the first one you're going to have is for work. So anything you log on to at work is going to have the same sentence. The second one is for your financial things, so your bank, it could be PayPal, pension, investments, cryptocurrencies, whatever you've got related to financial systems. The third one is for your social media accounts and Apple and Google passwords. So that's a third passphrase sentence that you use. The fourth one is your personal email and your fifth one is your throwaway one. It's the one you use for everything else. And what that one is for is for the websites that if they were hacked into, don't really care, it doesn't matter too much. So let's say you go shopping on boots. Do you care if someone logs into your boots account and sees that you've bought some perfume? It doesn't matter. Similar with your BBC iPlayer password. Do you care that someone logs in as you and watches the highlights of the football last night? It doesn't matter. There's nothing in there that's of interest because the stuff that you've got that matters to you always has a different password to those other ones. So if the criminals do breach a website that's not got very good security, they can't then get into your bank because you've always got a different password for those. So we're concentrating our good passwords on the websites that matter to us the most. That would have a material impact on our life if they were hacked into.

And the last step in this process is to use multi-factor or two-factor authentication on those logins as well. All websites that I've listed in those bullet points support two-factor authentication. You go into the settings, and you can turn it on in your personal life. That means that when you log in, you provide a code. You do that once you say trust. This device doesn't ask you again or maybe asks you again three months later. So that's an ideal way of doing it.

Okay, last couple of slides before we move into the questions. What's the end goal of the criminals? What they want to do is get onto your computer network and encrypt stuff. Usually scramble it. What that means is they infect your computer and then they move from there to other computers. They scramble all the information so that everything you've ever worked on, every document you've ever produced, is completely inaccessible. And then they come in and they say, we've got the solution for you. You notice I've done this a few times where there's a problem, the criminals have the solution for you. The solution is

you pay to unlock your files, but you might pay tens, hundreds of thousands for the case of big organizations, millions of pounds to do it. Then they provide you the decryption key, which then unlocks everything, and restores it back to normal. This is what the vast majority of criminal groups are looking to do. We saw, say the children get hit by a ransomware attack. They also often steal information at the same time. And if you don't pay the fee, their unlocking service, they then publish all that information online. So not only do they encrypt everything, they steal it and then they publish it online as well. So all the personal details of everyone involved in that charity or that organization goes online for other criminals to misuse. So we don't want to be hit by this ransomware attack.

And often this can come from just one person in the company, no matter who they are. Open up an attachment. Which is why I wanted to talk about phishing earlier on. So how do we protect against this? How do we make sure we don't get hit by the ransomware? How do we protect against the phishing stuff? I've talked about the phone calls, the physical intrusion, and how do we do it in such a way that we don't have to spend millions upon millions of pounds that we don't have. What's the best bang for our buck? So, the first thing, as an organization, every single login page we have that is pointed to the Internet, so people can access, if they're working from home, without exception. Must have two-factor authentication, otherwise known as multi-factor authentication. Same thing. Must have that enabled for every single employee. No reason not to do that. So that's your VPN, it's your email system, it's your HR login, your finance systems, everything must have two-factor authentication. That prevents the vast majority of attacks. It's often free or very, very cheap to enable. In vast majority cases, it's free.

Alongside that, patching, keeping our systems up to date. Many companies are breached because they use a system that's ten years out of date. Don't do that. Make sure you've got your systems up to date. That'll be down to your IT person to make sure your systems are kept up to date. Training, making sure your staff knows what to look for. So similar to what you've just had for the last hour or so, is listening to someone like me talking about it. Don't rely just on e-learning modules that you send out. Ten-minute module once a year or once a month or whatever. People don't listen. I know from going through my own training that I have to do with my organization. I do my health and safety training. Guess what? I forget it five minutes later. But when you have someone like me telling you stories, you tend to remember that a little bit longer. So don't treat security training as a thing that you have to just tick a box and say, yeah, we've done that. Make it good, make it count. And get people in a room for an hour, give them time to ask questions like you've got at the end of this. So they actually understand it and they actually listen and they're not doing their email at the same time.

If someone receives a phishing attack, make sure they know what to do with that. If they're not sure, make sure they're encouraged to talk to someone from IT to verify it for them. Don't put all the pressure on someone that doesn't work in IT to make a decision about opening up an attachment or not. Yeah, train them like I just talked about, but give them an outlet, someone to speak to within IT that they can easily get hold of, that allows them to report a potential phishing attack and get an answer quickly. Because if that's a legitimate email, they don't need to wait three days to open that email. They want to know within a few minutes how they do it so someone they can talk to quickly.

When we're talking about recovery from an attack, let's say we get hit by a ransomware attack, how do we get back? We need to have backups of our information. So our key data on our network, the stuff that matters to us as a business, have it somewhere else. Have it locked away in a safe somewhere so we can get out a CD or a tape or whatever and restore everything back to normal. Make sure you're doing that once a day or once a week. So even if you have cloud backups and things like that, you have a separate, literal, physical thing that's locked away somewhere else. So if a hacker takes everything and locks it, so

you can't do anything, you've got this extra backup system and have a plan. If it all goes wrong, your plan shouldn't be. I've got no idea what we're going to do. Let's panic. It should be at least, okay, we know this number, we're going to phone this company up and they're going to help us out. We know we're going to get all of these staff together. We've got a WhatsApp group set up already to phone those people. If we have some sort of cyber incident happen, maybe we role-play it. Once a year, we get everyone together and we imagine what's going to happen. We do a tabletop-type scenario and we respond because when a cyberattack happens and at some point you will probably get hit by a cyber attack, which is that bad at the moment, that something's probably going to happen, you know what to do, you've practiced it, you're not going to panic, and you've kind of run through it already.

And thanks very much. That brings me to the end of the presentation. We've got about 15 minutes left. For questions. If you think of anything afterward, I put my details up there on the screen. Please feel free to take those down. I don't mind any questions, doesn't matter how stupid you might think it is, anything you think of, please feel free to drop me a message through email, through Twitter, or through LinkedIn as well. But that brings me to the end. So what I'm going to do now is I'm going to hand over for questions. We'll see if anything's coming through the chat, and then we've got 15 minutes or so to deal with that. So have we had anything come in?

We have indeed. Thank you so much. Just a quick note, as there was a question about a recording and copies of the slides. So, yes, we have recorded the session and we will be sharing that with you along with copies of the slides. So do look out for an email from us over the next few days. We'll try and get that out as soon as we can. So thank you very much for the questions that we've had. Please do keep them coming. So if you think of anything while Rob is answering these questions, please do pop them in the chat. We are monitoring it and we will ask them.

Steph: So the first one we've had is around working from home. So how does it affect the chances of being hacked? And then do services such as VPN, and Citrix reduce those chances of being hacked when individuals are working from home?

Rob: Okay, yeah. So there is, there has been an uptick in hacks since COVID since working from home became a thing. One of the things that caused that was companies had to open up all their systems to the Internet in order for people to have to work from home or work from, whether on holiday or whatever else, and access their email, and other systems. What that meant was there were a lot more targets for criminals. So I can be sitting anywhere in the world and I can see your email login page, etcetera. And if you haven't secured those properly, that means I can hack in. So that refers back to one of the previous slides. I said so in order to defend that it's strong passwords, multifactor authentication, and keeping those systems up to date. The other thing that we found with people working from home is they were a bit more susceptible to phishing attacks because they couldn't just wander over to their IT person and say, can you have a quick look at this for me? They found they were trying to make decisions more on their own about whether something's phishing or not. And that refers back to my other previous point about making sure that people within the organization have someone in IT that they can get hold of quickly to verify whether something is a phishing attack. So as long as you have those things in place and maybe you give people a little bit of security advice about how to protect their own home network, like their router to make sure they've got a good password and things on there, then working from home should be perfectly safe. It's just about putting those extra layers in place. As I said, in terms of Citrix and VPN's and things, they're great. As long as you've set them up securely, you're using an up-to-date version, you've got good passwords, etc. And multi-factor authentication, absolutely no problem using those types of systems to allow staff to work remotely.

Steph: Thank you. So the next question is around Apple, and I know we get questions about Apple quite a lot when we have done these presentations before. So the question was, Apple doesn't recommend using software to protect your data as they claim their software is good enough, should we be using extra software?

Rob: Okay, yeah, great question. This one I get a lot as well. So when we talk about iPhones and iPads, you do not need any extra security software at all because it literally doesn't work. If you download antivirus for an iPad, it doesn't do anything. So there is absolutely no point in buying or investing in any extra protection for your iPad or your iPhone. When we talk about Macs, it's a little bit of a different story. So they do tend to have built-in security software that's actually very good. And that applies to Microsoft Windows as well. The defender antivirus software that comes with Microsoft Windows nowadays is just as good as the other software. So as long as you've got an antivirus, whether it's the built-in one from Apple or Microsoft or something else, I'm very happy with that. The free stuff is perfectly good enough. So as long as you have antivirus software, absolutely fine, no problem whatsoever. I don't encourage anyone to go out and buy McAfee or Norton or anything like that. You just don't need to nowadays. The free stuff for people like us is perfectly good enough. That doesn't apply to you as a business. As a business, you do need to invest in the upgraded versions that Microsoft has, etcetera. But as an individual, I'm absolutely fine with using the free stuff that's built into those platforms.

Steph: Thank you. The next question is just around password managers. What do you think about them?

Rob: I'm happy if you use password managers. So for those of you who don't know, a password manager is an app that is installed on your mobile phone, your tablet, your laptop, and it kind of stores all your passwords inside like a vault, effectively like a bank vault, and you unlock it with your fingerprint or your face ID or a master password. Then when you visit a website, the software automatically fills in all the passwords for you. And what that means is you can have a unique password for every single website. That can be really complicated because you don't have to remember it. So I'm absolutely happy. I think they're a great solution. Password managers, alongside my memory-based system I talked about, are the best way to do it. So if you want to use a password manager, if you're already using one, then brilliant. What I find with a lot of non-IT people is they don't want to use them because there's a level of like, oh, I can't be bothered with that app and things like that. And there's a level of trust, as in like if the app got broken into, they have access to all of my passwords. It's like all eggs in one basket. So for those, I recommend the memory system I talked about. We have five different passwords, but those of you that want to use a password manager, please do. I'm not allowed to recommend any particular ones just because, you know, imagine if they got hacked and I've recommended that to a million people. I'm going to be in a lot of trouble. But just Google the top password managers of 2024 and look for a company that you recognize.

Steph: The next one is when a phishing attack virus has been installed on your laptop. Will a standard virus scan find it? And as an example, Windows Defender.

Rob: Yeah. So in the majority of cases, the answer to that is yes, Windows Defender is very good. It will pick up on the vast majority of viruses will be able to be picked up by defenders. They probably won't even activate. At the point where they, where you open up the attachment, defender will kick in and block it. But that's not always the case. Okay, so in some cases, it's able to evade Defender, which is why when we're talking about defending a company, we talk about having layers of defense. So the first layer is your email defense systems that quarantine dodgy-looking stuff. The next layer is the staff's awareness. That looks like a phishing attack. I'm not going to open that. The third layer is

the antivirus. The fourth layer is detection systems on the network that you might have. The fifth layer might be something that stops stuff from leaving the network. We have all these different layers in place. If you want to ask me more about those layers, please feel free to drop me an email, because it gets a little bit complicated. But in your personal life, we have to rely on that antivirus a bit, combined with our own knowledge of something looking like a phishing attack. Which is why I mentioned checking that bit after the @ sign because that combination of our verification of whether the email is real combined with the antivirus is how we stop stuff. So we have to trust Defender to a certain extent in our personal life.

Steph: Okay, you mentioned having a backup plan and you said about a tape to recover information. How does it work if it is based in the cloud?

Rob: Okay, so modern backup systems mostly rely on cloud backup solutions, right? Which are great. There's no problem inherently with a cloud backup solution, it's good because it's somewhere else. The problem is, if you think about it from a criminal perspective, I've hacked into your network, I now have access to all sorts of passwords and things like that. Now, in order to restore your backups from the cloud, there has to be a way for you to access them. If I can steal your password, I can also access those so I can then go and delete them. So first thing I do as a criminal is I try and find as many passwords as I can, I get access to the backups and I delete them. Now that doesn't happen in every instance, but that's one of the things criminals do. The criminal groups nowadays employ specific, they call them backup destruction specialists. They learn about all the different backup systems that enterprises and organizations use in order to learn how to delete them and destroy them. So cloud backup systems are fine, but I would always recommend that you have a completely air-gapped, off-site physical backup somewhere. It doesn't have to be updated every hour, it can be every day, every week, or whatever. That's your emergency thing. If the criminal breaks into your network, gets access to the cloud backups and deletes those, you don't want to be in a situation where you've got to pay 100,000 pounds ransom fee. You can go to your vault, literally like a bank vault, pick out your tape or your CD or whatever, plug it in, restore the entire network from that or the key data, the stuff that allows your business to operate. And actually, when you look at what the criminal groups recommend themselves, and they sometimes when you pay the ransom fee, they'll give you security advice. Their number one thing is you need a physical backup like that they used to have in the olden days, you know, we used to do it years ago. Some of you probably remember you'd literally take a tape off-site every day. The criminal groups that do the hacking attacks recommend that you do that. So I'm a big advocate of having this off-site backup. Use the cloud stuff as well because they usually won't get to that and it's much quicker and easier to use, but as a backup of a backup, have that physical thing as well.

Steph: One of the organizations is in the process of introducing multifactor authentication for Office 365 at a charity, should they be insisting on using that every single time? Every single time they log in? And how can they make sure that all of their employees are using it?

Rob: Okay, so you need to enroll everyone in multifactor indication. So when you're rolling out, you need to make sure every single employee account is enrolled in multifactor indication. For sure. Then I don't necessarily require you to do it every single login. So you can either put it on a time so it activates every couple of months or every month and asks you to do it. Or anytime they access from a new device. Because in the vast majority of cases when a criminal guesses username and password, they're coming from a completely separate device.

So then it prompts the multi-factor authentication. So that's usually what it does. It's what my company does. When you come in from a new device, you're asked for the multifactor. When you're coming in from the same device, it doesn't ask you for it regularly. So that's the way that I would do it. But you're absolutely doing the right thing with multi-factor authentication. I just add to that, make sure you're doing a bit of education for staff alongside it, that they are the, when they ask to log in, they enter their credentials. If someone else phones up and says, can I have your multi-factor code or can you press this button for me? They don't do that for any reason. And make sure your IT is never asking your staff to authenticate them through the Microsoft Authenticator.

Steph: Thank you. Another question here. You said your boots password doesn't matter. Who cares if you bought a perfume? But isn't this the info they use for phishing attacks? For example, a spoof email from boots saying the product in this order you purchased on this date has been recalled?

Rob: Yeah, I mean that's a potential for a phishing attack, but your password associated with boots is not massively relevant to that. And if I'm using a phishing attack like that, I'm probably trying to get you to open up some sort of attachment because that gives me access to your computer rather than a link through to Boots's website, because the information stored in Boots's website is of no value to me unless you're storing your credit card details, things like that. I'd recommend you not to store credit card details inside of shopping websites like that. Amazon may be an exception because they've got very good security, but other ones not so much. So I wouldn't worry too much. There are a thousand different ways I could phish you with a thousand different companies I could pretend to be boots probably isn't going to be one of them. I'm not interested in your boots password. So the phishing attack is going to be to do with Google or Facebook or your bank or something like that. So that's why I said the boots kind of stuff. And those other shopping websites don't really matter because the criminals have no interest in them, really.

Steph: Thank you. The next question is around email addresses. So you said that we should pay attention to the ends of email addresses. What are the chances that the end part could be masked by scammers in the near future?

Rob: It's possible. There are a number of ways to mask that. So one of the primary things that criminals do is they make it look as close as possible to the real name. So they use a very small spelling mistake. So, for example, if you've got an M like M for mother in your email address, they use an R and an N next to each other because it looks like an M, or they swap out an L for a 1 or an I for an L, etc., and things like that. So you'll be quite diligent in how you're checking that email address. The other thing they might do is add something to it. So let's say you work for Apple. I can't send an email to you from apple.com, but I could send it to you as IT-apple.com, for example, making it like the IT department of Apple. So you need to, when you're getting in the habit of checking this bit off the outside, you're looking for this kind of lookalike thing going on. And that's how most criminals do it. Now, there are some slightly more sophisticated attacks that might be able to make you look even closer by using, like, Russian characters that look almost identical to an A, but they're very difficult to do and not very common at the moment. So keep looking at the outside and looking for any differences in the company and looking for these kinds of close differences where they use a spelling mistake or an extra bit added into that email address. And then when you combine that with all the other layers I talked about earlier, then you should be okay.

Steph: Brilliant. I do just have two more really quick ones if that's okay. So the first one is, would you use a password created by a password manager or have our own and store it?

And the second one is, if you already have card details stored on sites like boots, how do you get that cleared away?

Rob: Okay. Yes. The first question, I'm happy for you to use the passwords created by pass managers. They're very, very good. One little trick that you can do if you like, is to use the generated password and then add to the end a couple of letters that are yours that you use for all your passwords. So let's say you have these random characters stuck together and then you'd add on a couple of B's at the end or something like that. What that means is if that password manager were ever hacked into, they still haven't got your passwords because you put a little variant in there. It means you've got to enter that double B at the end of every single one. But it's one little trick. But in general, I'm happy if you use the passwords generated by the password manager. That's absolutely fine. And. Sorry. Remind me about the second question around card details?

Yeah, so most websites when you go into your account page on the website, there'll be a list of your stored cards and you can just delete them from there, I think. I don't think I've ever seen a website. It doesn't allow you to edit those card details. If you can't do that, then just contact them through their customer services and ask them to remove it. Now, in many cases, it's not the full card details that are stored. It misses the three-digit CVV number from the back of the card, so it's not too bad. But I still personally prefer not to do that. I don't mind if you want to store your card details on your phone though. So when you use the website you can use Apple Pay or whatever. That's absolutely fine. But yeah, I don't like storing them on the website itself.

Steph: Thank you. Well, thank you so much for a really helpful and insightful session. I know I learned a lot and we hope you all did too. We will be sending out a short survey by email after this presentation, so if you wouldn't mind completing that and giving us some feedback, we would really, really appreciate it. It just helps us shape future sessions that we will organize. But thank you very much for attending and we hope you have a great rest of the day.