CyberFirst Podcasts
'Tackling tricky tech terms' transcript

00:07 **Anne Marie** - Cyber security, it can seem like a closed off world. You might think it's just for boys, or just for coders or just not for you. Our podcast, created by CyberFirst is here to change that. In today's episode we're breaking down barriers, there might be a lot of cyber security concepts you've heard of but just don't understand. We're going to explain what they actually mean so that you know more about what you could do in our industry.

I'm Anne Marie, from the Stemettes, and I'm joined by…

00:31 **Emma** - I'm Emma, I work in the comms team at the National Cyber Security Centre, which is part of GCHQ.

00:36 **Amy** - I'm Amy, I'm a former GCHQ apprentice, and I work within the CyberFirst team.

00:41 **Michala** - I'm Michala, I'm the head of Information, Governance and Security at Marie Curie, we're the UK's leading end of life healthcare charity, and we're also one of CyberFirst's industry members.

00:51 **Anne Marie -** And additionally, I'm joined by Ethan and Olivia, who are two current CyberFirst bursary recipients.

00:57 **Ethan** - Hi, I'm Ethan, I study computer science at University and I'm currently on a year long industry placement that was organised through the CyberFirst bursary scheme.

01:04 **Olivia** - Hello, I'm Olivia, and I'm graduating university with a degree in chemistry this summer, and I've secured a graduate role through the CyberFirst bursary scheme.

01:16 **Anne Marie** - CyberFirst bursaries and degree apprenticeships are open to everyone, but often, people don't apply because they don't think they know enough about key tech concepts. The reality is, you don't need to know. Our training will help you understand. So, to kick things off with a bang, and break down a few of those trickier terms, we are going to set our guests a challenge. Explain a common cyber security concept in 15 seconds, in a way that beginners can understand. Ethan, you've got 15 seconds, take it away!

01:48 **Ethan** - I've chosen the term firewall. The way to describe this is to imagine you're at a club, and there's a bouncer, basically the club is your computer and your network, and the bouncer is the firewall, they're basically responsible for letting things in or out, so depending on the properties of the firewall, it controls what comes in or out of your network.

02:07 **Anne Marie** - Awesome, thanks Ethan! Amy – what's your chosen term?

02:10 **Amy** - I'm going to go with phishing.

02:12 **Anne Marie** - You've got 15 seconds, starting now.

02:15 **Amy** - So phishing is where somebody sends you a message, usually via email, in an attempt to get your details from you or get some kind of money from you so they could send you a malicious link to click on, some malicious software or try and trick you by using their language.

02:31 **Anne Marie** - Michala, you're up next, what's your chosen term?

02:35 **Michala** - It's IP address.

02:37 **Anne Marie** - You've got 15 seconds starting now.

02:39 **Michala -** Your home has a house or flat number, so the postman knows where to deliver your mail, so think in the world of the internet, each device connected to the internet has a unique number so that network traffic knows where to deliver it to.

02:54 **Anne Marie -** Next up we have Emma, what's your chosen term?

02:58 **Emma** - Compliance budget.

03:00 **Anne Marie** - Ok, 15 seconds on compliance budget. Emma, go.

03:03 **Emma** - Compliance budget is a term from people centred security, it means the mental amount of time and effort you're able to allocate to doing security activities, so if you've been knocking yourself out trying to deal with a website's password policy, you're going to have no energy left over to deal with a phishing email.

03:19 **Anne Marie** - Finally, we've got Olivia, what's your chosen term Olivia?

03:23 **Olivia** - DDOS attack.

03:25 **Anne Marie** - Ok, 15 seconds on DDOS attack starts now.

03:28 **Olivia** - DDOS attack stands for distributed denial of service. It's a form of cyber-attack that aims to make a service such as a website unusable by flooding it with malicious traffic or data.

03:42 **Anne Marie** - Thank you so much everyone, I wish all terms could be described in 15 seconds. We've covered off a fair few examples, but as specialists in the industry, what would you all say are the most commonly misunderstood technical terms? What would you say to help young people understand them, if they aren't from a technical background?

04:01 **Emma** - Can I chime in with an early smarty-pants answer? I think the word technical is quite commonly misunderstood. I think when people hear technical, they often hear 'has to do with technology' or 'has to do with computers', and that's not my understanding of

the word technical. I mean technical as any kind of set of really deep specialist knowledge basically, so the work I do in people centred security is very technical, even though it's not always directly to do with computers or technology. You can take this as wide as you like, you could argue that human resources is a technical pursuit because it relies on a lot of specialised knowledge.

04:40 **Anne Marie** - It's that use of technicalities almost, when you think of technicalities you don't always think of technology.

04:47 **Emma** - Exactly, yes, you think of it as something that's quite nerdy or quite intricate and deep. I worry about this; I think people do see that word technical and think of it as a barrier if they don't think of themselves as a technical person. I never thought of myself as a technical person growing up, ever. It really is just about how you think about it, everyone has something to contribute here no matter what their specialist knowledge is.

05:09 **Ethan** - I think I'd say similar to Emma, another of those terms is cyber security in general, everybody thinks, particularly when you're younger, that it's just hacking or defending a network, or something just really pigeonholed, when actually it covers a lot of things. Loads of the jobs you find in any other industry are in the cyber security realm as well, so it should put people off if they don't like the sound of it, you just need to do a bit more reading into it.

05:37 **Anne Marie -** That's a brilliant point Ethan, we've actually got another podcast coming up which covers where cyber seeps into everything, so that's fantastic. I definitely agree with you on that one.

05:48 **Emma** - Another one would be the word hacker, I think that's a misunderstood term where we think of some teenage boy sat in the basement in the dark, when ethical hacking is a totally different side of that, doing things and finding vulnerabilities for good reasons, rather than exploiting them.

06:09 **Anne Marie -** Our white hat hackers, definitely something we don't see in Hollywood often enough.

06.15 **Michala** - Can I just pick up on something Ethan said there on the different roles. One of the things I often find people misunderstand, and it's technical in Emma's definition, but probably not in most members of the public minds, and that is risk vs. issues. So, risks looking at day to day things that could happen vs. an issue that's something that has happened, that's something we find quite a lot. At the end of the day cyber security is fundamentally about risk management.

06:49 **Olivia -** A lot of people might misuse the words virus and malware, or might interchange them when actually a virus is a specific type of attack.

07.02 **Emma** - I think that's a really interesting point, I work in advice and guidance in NCSC comms, and we are very conscious of that as a language issue for the different audiences we talk to. If we are putting out advice for the general public we might want to talk about

malware, but we will hardly use the word malware, or say run your anti malware software, because we know that as a term malware isn't as accessible as virus. People know what anti-virus is, so we say anti-virus, even though we are conscious that it's not perfectly accurate, but it does the job we need it to do at the time.

07.34 **Amy** - That's probably one of the most confusing things really, when there are multiple different groups who are using the same word to mean different things. The word platform comes to mind, some people say the word platform and literally mean the floor that you stand on, some people mean a website, some will mean a phone or an operating system, so it can create some language barriers within technical groups, like intergroup confusion.

07:54 **Anne Marie -** Brilliant thanks very much, I think we can end that one there. The aim of our challenge is to point out the sheer number of terms that can be alienating if you're new to cyber security, and sometimes even if you're within cyber security. Our audience can often feel like they will never catch up. Did any of you have that experience before you joined the cyber security industry?

08:15 **Michala** - Could I just chip in with this and I say I thought this was a really interesting question, I actually think that we never catch up, cyber security is always changing, and we learn new things every day. Take today for example, I've just learnt from Emma what the term compliance budget means!

08:30 - **Emma** I was going to say the same thing actually, that pressure to catch up is something that a lot of people feel, we are always comparing ourselves with the people around us. As is the nature of imposter syndrome, you notice what people can do that you can't do yet. You notice what they know that you don't know yet, so you can feel enormous pressure to know everything that every single other person knows, otherwise you're not good enough, and I think trying to let go of that pressure is one of the biggest gifts you can give yourself. You're here, you are good enough, you've got a role and a contribution to make. There will always be someone who knows more than you do, it's a big world out there, but the important thing is what do you know? How can you contribute?

09:13 **Amy** - I definitely identified with that before I joined, every time I was meeting new people, clearly very intelligent people, which GCHQ is obviously full of, you feel like you're the stupidest person in the room sometimes it's a skill that you have to try and hone to acknowledge what you can contribute, and not the things you don't know.

09:34 **Ethan** - When I first started my placement, and I was in meetings there were acronyms being thrown around every two seconds, I wasn't afraid to ask 'what does that mean?'. That type of stuff you learn on the job anyway, a lot of technical skills, unless you learn them in your spare time, you won't be an expert in them. But as long as you've got the passion and drive to want to learn, then I feel anybody can get to any level of expertise, but it's realising you don't have to have those gifts from the get-go. Some people might, but that's good for them, they might just learn a bit quicker but you can still get to the same place.

10.06 **Amy** - GCHQ is particularly bad for acronyms I have to say, we are really keen on them. It can feel difficult to ask in a big meeting 'what does that mean?', I still do it now, I'm still afraid of asking these things.

10:18 **Olivia** - I definitely agree with everyone just then, because I come from a non tech background and initially when I saw this opportunity I was hesitant to apply because I thought I couldn't do that, but actually it was my passion and ambition to get into cyber that pushed me to apply, and just getting across that I'm very interested and I've got skills that will apply, I might not know all the techy stuff just yet but I am willing to and like you said no one is going to know everything, but as long as you have that curiosity within you.

11.00 **Emma** - I will hire someone with curiosity over someone who has a tonne of existing skills but no curiosity and no willingness to learn, and no willingness to be wrong. People like that find it difficult to grow, but if you have that curiosity and that willingness and that keenness you can go as far as you like, I'd hire anyone like that at any time.

11.20 **Anne Marie** - Would any of you say that's the nature of the industry, there is always something new on the horizon? Things are continuously evolving, so you can't really be a cyber security professional if you're not continuously learning?

11.33 **Emma** – Exactly, It's a bit of a, they call it in nature a red queen scenario, you know the attacks are constantly evolving so the responders have to respond in accordance, and then the attackers move onto something else, so It's a constant race of everyone having to keep up with everyone else, things move on very fast.

11.48 **Amy** - I think it's bittersweet in a way because you do have that constantly changing nature of risks and attacks that you have to mitigate against. But on the flip side it's the constantly evolving technical landscape, it becomes really interesting if you have that passion for all things technology then every day can be new.

12.11 **Ethan** - I was going to say, equally I don't want people listening to this to think it changes so much that you're always going to be on the edge of your seat, not in a good way. That you're always going to be worried going into work about things changing, like with any line of work, things like programming languages or whatever, there are always new ones coming out and updates being made, but there are always core foundations that you can learn. The more you get into work and see new things, there are common themes that run throughout that you will have seen before. It can seem scary at first because there is so much going on, but you do just pick it up I think. You've got a group of people who are all in the same boat with you, so it's a bit easier.

12.55 **Emma** - As much as stuff moves on quite fast, also a lot of things stay the same. There is quite a bit of consistency over time in terms of the sheer volumes of different kinds of attacks we see. Phishing has been a problem for a long time, and will continue to be a problem for a long time in the future I think. Patching is hard, keeping all your software updated, asset management is hard, these are long standing issues that need innovative approaches and you can see that because we haven't solved these things yet. We need better ways of dealing with them. As problems go, they are relatively consistent and it's

interesting the degree to which these things that have always been big problems remain big problems.

13.32 **Anne Marie -** Some things are continuously changing, and some things stay the same.

13:37 **Emma** - The more things change the more they stay the same.

13.38 **Anne Marie** - There you go that's it, you said it better than I did! We've obviously tried to break down a few of the key concepts of cyber security but with CyberFirst you don't have to know everything straight away, as a bursary student or degree apprentice you'll be supported to learn the things you don't know. This is a question specifically for the bursary recipients who have joined us today, can you tell us about the atmosphere on your placements, are you able to ask questions and get straight forward answers when you need them? And what about on the academy, are you able to get up to speed on basic concepts so you don't feel left behind?

14.13 **Ethan** - I guess I will go with the academy first because that was the first thing I did, I had no cyber security experience whatsoever when I joined and I said that in my interview for the bursary, I was saying how I wanted to learn and that is probably why I got it. When I was at the academy you get a broad range of skills in lots of different areas, and have the opportunity to talk to the trainers to say 'I'm quite interested in this' and then they might give you some more resources. You get sent a lot of things that would be hard to find otherwise, even to this day on Slack talking to the admins or other people with the same interests, if you say you are interested in something there will be 4 different people responding to you with links to things you might never have seen so in terms of that you are 100% supported and it's a lot easier way in, equally with the placements I have it's almost like being part of the family, if I can say it like that, for the whole time because there is no awkwardness, you can just ask things. They want to help you, they'd rather you asked stupid questions than kept them to yourselves for six months when you really need the answers. You have to be honest, and if you do that, everyone is mature enough to get along with you. Olivia, I don't know if you found it the same?

15.24 O**livia** - I definitely agree, there's always the opportunity to ask supervisors or colleagues, and don't be afraid to. They have been in the same boat I'm sure. But also make the opportunity of the other students who are working with you, we all come from different backgrounds and have different ideas and points of view, so don't be afraid to ask them as well. I know I did, even if it's technical or non-technical, they are there to support you as well.

16.03 **Anne Marie** - This is a question for former apprentice Amy, what was it like working and studying in GCHQ, and how were you and your fellow apprentices supported?

16.09 **Amy** - The thing I really enjoyed about the studying side of things was they took us from very base level knowledge and helped us gain a little bit of expertise in lots of different areas so it wasn't in the deep end at all, there were people who didn't take maths at a-level and lots of people who did for example. There was a whole module getting people up to the same speed, it was a very supportive atmosphere. Similarly, on our placements when we

would be injected into various teams within the organisation, I was one on the very early years of the apprenticeship, so I think people in those teams didn't really know what to expect from us yet. They perhaps expected very little, so they were pleasantly surprised when we would achieve things, help them with projects and contribute to their work, so that felt very satisfying!

17.05 **Anne Marie** - So it's a fantastic arena to be learning in. That's all we've got time for on this episode, but if you're listening and want to know more about key concepts of the cyber security world we've gathered all sorts of explanation and insight on our website, https://cyberfirstcareers.co.uk/ where you will also find out more about the CyberFirst university bursary and degree apprenticeships. Thanks to all of our guests and thanks to you for listening as we open up the world of cyber security!