GOVTECH DECODED
EPISODE 2
CYBERSECURITY CHRONICLES FROM FRONTLINERS

Host: Alicia Lee and Andre Ng
Guests: Bryan Koh and Chloe Lim
Date aired: 18 November, 2024

[Andre] People do not know, but GovTech actually has a team of people monitoring our government systems 24 by 7. And Bryan here is part of this team.

[Chloe] Oh no wonder got eyebags. Kidding kidding.

(Intro music)

[Alicia] Hi everyone, and welcome to GovTech Decoded, where we decode technical speak. In this series, we'll discuss hot tech topics and how the Singapore government leverages technologies to build tech for public good. I'm GovTechie Alicia.

[Andre] I'm GovTechie Andre. And we are your hosts for today's episode.

Today, we have cybersecurity experts Bryan and Chloe with us again. In the last episode, we heard many scary scam stories and also about the innovative ways that GovTech is using technology to stop scammers.

Scams are a big concern right now and there are many other cyber threats. So today, maybe we discuss a little bit more about the other kinds of cyber threats.

[Bryan] Yeah, definitely. So it's not just about job scams, e-commerce scams, or phishing that we should be careful of. There are other common threats out there which we observe to be on the rise in the recent years. For example, DDoS as well as ransomware attacks.

[Chloe] And I think the thing to know is that these threats don't just affect individuals, but also companies and even governments, like ourselves.

[Alicia] So now you mentioned a little bit about the types of attacks. Can you tell us what happens when an attack actually happens?

[Bryan] Right, so each attack is basically different. For DDoS, it stands for Distributed Denial of Service. The aim of DDoS is usually to disrupt a service, right? But DDoS could also be a cover for other malicious activities such as data exfiltration, where sensitive data can be exfiltrated out of the environment by the attacker while the DDoS is ongoing.

[Chloe] And in the case of a ransomware attack, these attackers, they deny access to files by encrypting the files, and then they demand a ransom payment for the release of these files.

So they try to ask companies to pay a certain amount so that they will give them back whatever access they need for their work or things like that. And in fact, the police has put out a notice that companies should not pay this ransom because you're not even guaranteed to get back access. And they might even flag you as a potential next target again. So the WannaCry attack that took place in 2017 is one of the best examples of a ransomware attack.

[Alicia] Yeah, I know right? If it was me and I got my money already, then that's it. I wash my hands off you and don't care about you already right?

Okay, so what can people do to prevent such kind of attacks?

[Chloe] So the most common defences are antivirus, encryption, firewalls, and two-factor or multi-factor authentication.

[Andre] Right. Could you share a little bit more about how these defences work?

[Chloe] Sure. So antivirus is quite self-explanatory. You know, it's like a vaccine or immunisation to keep your device healthy and to protect it from computer virus attacks.

[Alicia] Like those COVID.

[Chloe] Yeah, correct. So you must get vaccinated and then you need to make sure your antivirus is updated. So you need to get vaccinated more often, right?

And in terms of encryption, the audience might be familiar with this term if they use WhatsApp because sometimes your message says encrypted end-to-end.

[Andre] Yeah, my mom always asks me what is this encrypted end-to-end on her WhatsApp. Maybe I should just send her this episode then she will understand.

[Chloe] Okay, so your mom can play from, now. Encryption of information means that the data is scrambled and only authorised people are able to access and decipher the information.

So for example, if I'm sending you a WhatsApp text. So I text it over. I can see this message. It goes and then you're able to read the message, right? This is because we each have the key or whatever's necessary on our devices to decrypt the message.

[Alicia] So if I take the message from the middle, I will see….

[Chloe] So what do you think Alicia will see?

[Andre] Garbage.

[Chloe] Garbage, right? So it’ll just be gibberish like exclamation mark. It looks like swear words maybe, right?

[Alicia] Censored ones.

[Chloe] Yeah, but it's not because I'm swearing at Andre. It's just because you aren't able to see the actual content that's going on. What's over here is the encrypted message.

[Bryan] Right, so for firewalls, I can try to explain that. Firewalls are basically appliances which you deploy at the edge of your network to prevent malicious traffic from entering your environment. The technologies of firewall have evolved over the years quite a bit. From just basic filtering using parameters like your IP addresses and ports, they are now able to perform inspection of the traffic at the application layer.

[Chloe] So it's like you can scan and not just the police blocking you or like customs blocking you at the site. They also look inside what's in the X-ray box.

[Bryan] Yes, absolutely.

[Chloe] Quite cool, right? So the next thing I think I can talk about is also multi-factor authentication. We call it 2FA because usually we have two factors. I think everyone's familiar with some sort of 2FA when you use your Singpass. You know, like we said, scammer and hacker methods have improved and become more sophisticated. So we need to improve our security as well. So what different authentication factors mean, the different factors are like who you are, let's say like in terms of your thumbprint, right, your eyes, your retina. What you have in terms of your phone or different things. Sometimes it's like your additional token, right? Or what you know. So usually that's like a password.

So as you now use your Singpass app, it's no longer just username and password, which was a thing of the past. We still have it, but it's only one layer. But in addition to that, when you open your Singpass app, you're prompted, you need to verify and authenticate using either your thumbprint or your face. And this is what you know, sorry, who you are. And then sometimes you need to type in a passcode. So that is what you know.

And then the fact that you have the phone and the app itself, that is what you have. So it's encompassing these multiple factors that helps to enhance security, because it's hard to both steal what you know in your head and kidnap you and steal your phone at the same time. So that's why multi-factor authentication helps.

[Andre] Since we have been talking about scams, let's put our guests to the test and see how good they are at spotting scams. Game time!

(Transition music)

[Andre] We'll now play a game of real or fake. In essence, Bryan and Chloe will choose between real or fake for the websites that they see in front of them. Bryan, Chloe, are you ready?

For the first website, is this real or fake?

[Chloe] Fake.

[Andre] And why do you say that? Why is it fake?

[Chloe] Because the ‘please type your username’ and ‘please type your password’ something like that. One is capital letter, one is small letter.

[Andre] Well, I think... So this is, you're right. First of all, it's fake. The reason why it's fake is because the Singapore Police Force website doesn't look like this. And what happens in this scam is that they’ll phish user credentials from these input fields.

[Alicia] Okay, number two.

[Andre] Number two. Is this real or fake?

[Bryan] Fake.

[Andre] *(to Bryan)* And why do you say that?

[Chloe] *(to Bryan)* Bro, bro.

[Andre] *(to Bryan)* Bro, I think this one is…I think...So, Bryan, this one is actually real. You know why? Because if you look at iras.gov.sg...

(Guests and Hosts laugh)

[Andre] But so, Bryan, this time... Sorry, you're wrong.

[Bryan] It's real.

[Andre] Yeah, so we go on to the next one, okay? Is this real or fake? This Ticketmaster. Think very carefully, just now got one wrong already.

[Bryan] Fake.

[Andre] Fake, and why do you say that? So there are some grammar errors like the pre-sale.

[Andre] Yeah, correct. So you're right. I think there are some grammatical errors from this website. And in this case, it was a fake e-commerce website where they will phish credit card information from the victims as well. So this is a fake website.

[Alicia] So when you're buying tickets for your favourite concert, please be careful.

[Andre] Yeah, absolutely. Absolutely.
So the next one, is this real or fake? Singapore Police Force website, e-service arrest warrant.

[Chloe] Fake.

[Andre] And why is that so?

[Chloe] The boxes look a bit ugly.I believe in... I believe in the SPF’s UX designers.

[Andre] Yes, so in this case, it is a fake one. But maybe not so much of the UX, because I think the scammers can easily also make a nice website.

The reason why it's fake is because there isn't such a service, first of all, for you to key in an arrest warrant and search for details. So typically, this website is used in scam cases where they will impersonate as authorities and require the victims to enter their personal information, sometimes even bank account information, inside these seemingly authoritative websites. So you got to be really careful with these lookalikes as well.

So the next one, real or fake? This one looks quite interesting. Yeah, take your time, take your time.

[Chloe] *(to Bryan)* I give you chance.

[Andre] Yeah, Bryan you want to take this, you know right? You sure or not?

[Chloe] *(sound effects)* They give you one loading gif.

[Bryan] Um, it's fake.

[Andre] Okay, why?

[Bryan] There's a capital letter in the Gov.sg.

[Andre] Well done, well done. So the real one actually is a lowercase character. So gov.sg, the g in gov is a small letter. So well done, you redeem yourself. Good job.

[Chloe] I thought it's because they spelled the CPF, the provident, wrongly.

[Andre] Oh, really? Yeah, and provider for... Yeah, yeah, that too, that too. Well done. Okay, good, good job.

[Alicia] Security experts for sure.

[Andre] Yes, okay. Congratulations, you have come to the end of the quiz. So thank you very much, and well done. We spotted at least most of them. One wrong.

[Chloe] Because you never pay taxes. Kidding, please pay taxes

[Andre] *(joking)* What is IRAS? I never pay taxes before.

[Chloe] *(joking)* It’s what pays us.

(Transition music)

[Andre] So you both have shared quite a bit on cyber security defences. Can we talk about what is GovTech's role in all of this though?

[Bryan] So GovTech is a key agency that drives digitisation across public service, and we support the agencies in their digitisation journey. In the process of helping them to digitally transform, it's important that we also make sure that these systems are secure.

So firstly, we make sure that the environment which our public officers work in is secure. This includes having the necessary security controls on the corporate desktops and laptops that they use, as well as having the controls over the network as well. But having security controls are not enough.

We also monitor the government system and networks for cyber threats, and promptly respond to these threats, should it happen.

[Andre] So many people do not know, but GovTech actually has a team of people monitoring our government systems 24 by 7. Around the clock, every day of the year.

[Alicia] So even Christmas, New Year, public holiday, National Day?

[Andre] Yes. Every day. And Bryan here is part of this team. So I'll let him share more about that.

[Chloe] Oh no wonder got eye bags. I'm kidding, kidding, kidding.

[Alicia] You're on call 24/7, and no wonder just now your phone beeped.

[Bryan] So in 2022, we commissioned the Government Cybersecurity Operations Centre, GCSOC, to strengthen our monitoring and defence against cyber threats to the Singapore government. Beyond just monitoring, there is a team of dedicated specialists behind the scenes which supports incident investigations and response efforts during cyber incidents. And ensuring that the weaknesses are identified timely, and remediated to prevent future occurrence.

[Alicia] Wow. That's really impressive. I'm glad to know that our systems are safe in the hands of you and your team.

[Bryan] However, it's no longer sufficient to, you know, just set up the SOC and hoping that we could really catch the bad guys. So as such, there are capabilities within GovTech such as the red teaming, which continuously validate our defences.

[Andre] I also understand that red teaming is also not something most companies emphasise on.

[Bryan] Similar to how the military conducts exercises to prepare them for the war, we also conduct exercises to prepare us. So a red teaming exercise is having the team playing the bad guy and attempt to attack the system. And by conducting our own attacks, it helps us to discover the weaknesses in our defences and fix them before the bad guys do.

[Chloe] Sounds quite fun to be a red team person. You can be a bad guy but you're paid by the good guys.

Bryan, based on what you shared, it almost seems like the government should know everything because, you know, we're red teaming and discovering vulnerabilities and all. But I think it's quite an unrealistic expectation to have. And I feel that cybersecurity should be a partnership and a shared responsibility between the public and the private sector, and even individuals, right?

And hey, this actually sounds pretty familiar. I feel like Andre told me about this a few years back. So how about you tell us right now?

[Andre] Right, okay. So back in 2018, we started a programme called the Vulnerability Disclosure Programme. It essentially means anyone who sees a vulnerability or spots a vulnerability on the government systems can report it and the government will fix it as soon as possible.

If you see something, say something, as simple as that. And I remember it was still quite a controversial topic back then. And my supervisor genuinely thought I was delulu (delusional) because he said, who will exploit the vulnerability and tell you that there's something wrong with it? But to me, I thought, you know, prioritising the security of the system was the most important. So we should have as many pairs of eyes looking on the system as much as possible. I explained to him that, you know, it's akin to having a good neighbour to look after your front gate and front door when you're away. So having more pair of eyes is always a good thing. So maybe guys, the lesson here is, delulu is the solulu (solution).

[Chloe] Yeah, so it's a bit like a whistleblowing programme, of sorts, but open to the public and people and trusting in the goodness of people to report and not exploit.

And let's not forget, you know, our Government Bug Bounty Programme and Vulnerability Rewards Programme, GBBP and VRP respectively. These programmes invite highly skilled white hat researchers to come and test selected systems for bugs. And since the launch, more than 2,100 local and international researchers have participated in these two programmes. And over 160 vulnerabilities have been discovered, and we have paid out more than USD $150,000 to these participants.

So I think it's really a good way of involving highly skilled people to come and help us test our systems and make it better.

[Andre] Yeah, absolutely.

[Alicia] Like you said, it's a partnership, right, between public and private sector as well.

[Alicia] So thanks Bryan and Chloe for sharing more about scams in Singapore and our Government's cybersecurity efforts. It's very insightful and I feel a lot safer knowing that you guys are working really hard to protect all of us.

[Andre] We have come to the end of this episode. If you are keen to find out more about what we have discussed, you can check out our website at https://go.gov.sg/GovtechDecoded.

[Alicia] If you enjoyed this episode, do support us by sharing it with others and on social media. You can also connect with our speakers on their LinkedIn pages and follow GovTech on our social media platforms at https://go.gov.sg/ConnectWithGovtech. We will leave the links in the description. I'm Alicia.

[Andre] I'm Andre. And we will “cache” you in the next GovTech Decoded.

(Outro music)