GOVTECH DECODED

EPISODE 1
AI A DOUBLE-EDGED SWORD IN THE FIGHT AGAINST SCAMS

Host: Alicia Lee and Andre Ng
Guests: Bryan Koh and Chloe Lim
Date aired: 28 October, 2024

[Alicia] Like one of my friends also recently got scammed. She met this guy on an online dating app. All her life savings are basically, like, gone….

(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 host for today's episode.

Hey, Alicia, have you received one of those messages to tell you ‘last chance to invest’ or like ‘jobs immediately available’?

[Alicia] Yeah, I keep getting them leh. Do you know how to stop (them)?

[Andre] You know what? I have some idea. But I'll let our guests here, Bryan and Chloe, explain a little bit more. Welcome, Bryan and Chloe.

[Bryan] Hello everyone, Bryan here. So I'm from the Government IT Security Incidents Response (GITSIR) team. We are responsible for incident response and investigations against cyber threats in the Singapore government.

Chloe, how about you?

[Chloe] Hi, I'm Chloe. I'm from GovTech's Anti Scam Products (GASP) team, and we mainly look at developing products that detect, disrupt, and deter scams.

[Alicia] So for a start, maybe we can share with our audience. What exactly is cyber security, and why is it important?

[Andre] Yeah, so actually, I'm a cyber security specialist myself, and most of the time, people associate cyber security with hacking or some other cyber crime. But

actually, cyber security is more than that. It is about protecting your data, your apps, your systems, networks. Bryan, what do you think though?

[Bryan] So to me, cyber security is not just about us protecting the systems against cyber threats, but it's also about empowering the people to protect themselves against threats and scams through the necessary awareness campaigns or even education.

So actually, my mother-in-law also fell prey to a scam recently. So it all started with a Facebook advertisement, advertising on roasted meat, and the seller insisted for my mother-in-law to perform a deposit of $5 through an Android application. So once the app is installed, her phone basically got compromised, and the scammer started to send messages to all her contacts to borrow money. So it was a very traumatising experience for her, and the lesson learned from this is that we should never download and install applications that we are not familiar with.

[Alicia] This roasted meat is very expensive. Somebody's favourite…somebody's favourite.

(Guests and Hosts laugh)

[Chloe] Yeah, but actually it's not just the older people who get scammed. Even among my friends, whom I consider quite tech savvy, I've heard of similar stories involving bank phishing scams. Like one of them was quite high profile. Think a couple of years back during December there were a few banks that got compromised. And yeah, I had a friend who actually lost a sum. But thankfully during that period it was also recovered. It's really like any one of us can get scammed.

[Alicia] Like, one of my friends also recently got scammed, and she lost the money and didn't get it back. So it was like a long-drawn con I guess. So she met this guy on an online dating app, and then, like, they had a textual relationship, right? And he showed her pictures of himself and all that. And then he said that he was working at a bank and they had this special product. So it started small, right? You went to a link, and then it was like a trading platform. You put in $1000, then you got back a bit more than $1000. So okay, you try again, $2000, then you got more than $2000. So I put in, like, all my money, then it got locked. Say the password has some issues. And that was when like they realised that it was a scam, and then they reported to the police, but they never got it back.

So, all her life savings are basically like gone. And she's not that old, but you know, it's like, you're 20 something, and then you have to start all over from scratch.

[Andre] So these are also reflective of the national crime statistics that the police have released last year. So last year, they reported 50,000 scam cases and cyber

crimes. The top three scam cases were job scams, e-commerce scams, and fake friend call scams. And you know what, guys, 40% of these scam victims were aged 30 to 49. So that's not old people. That's us.

[Alicia] *(sound effects)* Everybody is like, come and scam us.

[Chloe] Yeah. I think a big reason why all these scams have grown so big is because of the nature of social media platforms. Nowadays, it's very hard to catch them due to the sheer volume of messages, ads, posts that are on social media, and this makes it very difficult to discover them. At the same time through social media platforms, these scams are very easily propagated to a larger audience.

[Alicia] Like roasted meat.

[Chloe] *(to Bryan)* Yeah, like your mom-in-law.

[Bryan] And I also thought that it is also the challenge for these platforms to really combat the scams, because the moment when these are posted, let's say on Facebook, they seem pretty legit. So it's really hard to stop them.

[Alicia] So actually, I want to ask. If people, touch wood, are in a situation where they get scammed…So Bryan, you mentioned your mother-in-law, phone got hacked, and the hacker also messaging her friends. So if I get caught in such a situation, what should I do?

[Bryan] So in such circumstances personally what I would do is, the first step I will do is I will cut off the scammer's access to my phone. I'll do that by removing the SIM card, disabling all the Wi-Fi access. Once that's done I will then use a spare phone to log into my existing applications. And then from there, I will terminate any existing sessions on other devices. And once these are done, I will then check for any suspicious transactions. For example, are there any suspicious transfers on my ibanking application. And then lastly, I will proceed to file a police report.

[Chloe] So methodical, you know. Cut your phone, burn it.

[Alicia] Everybody must put down all these, like, 3, 3, 4, 5, steps that y'all must do. Okay?

[Andre] It sounds like almost Bryan has rehearsed this, or like, you know, thought about this a long time.

[Bryan] I went through for my mother-in-law.

[Chloe] So that's what you did for your mother-in-law.

[Bryan] Yes.

[Alicia] First hand experience.

[Alicia] Okay, so now scammers are also getting more sophisticated, right? Last time, they used to be very dodgy kind of URLs, and it's HTTP, not HTTPS. But now everybody is like upgraded.

So what are some precautions that we should take in the first place to prevent ourselves from getting from getting into this kind of situations?

[Chloe] Something like what Bryan was saying just now, just don't download anything that looks sus(picious). You know, if it's from an unknown source, if somebody sent it to you, especially with .APK, and you need to install it and give it extra permissions. Like it's just a food purchasing app, but then they need your location, contacts, access to files, and everything. Then this is no no, just, just don't do it guys don't do it.

[Andre] And also watch out for time pressure tactics. So these scammers, they like to use time pressure tactics or you know, things to make you feel FOMO*, and then you act rashly and regret later. *(*FOMO - Fear of missing out)*

[Alicia] I think recently scammers have also started using AI right, in their scam. So that's why you have, like, last time you can see them from the bad grammar, and now they can use ChatGPT and fix all the grammar, make it look super professional. How else can they be using AI to scam us?

[Bryan] So, circling back to the scam which happened to my mother-in-law, what amazes me was that the scammer was actually able to send voice messages to her contacts which really resembled her voice. And even speaking the dialect that she used to speak. So this is likely the application of the deep fake audios, that's created through AI. And if I reference to a report that was shared by the Cyber Security Agency of Singapore, one three, 13% of the scams evaluated in 2023 were likely generated by AI.

[Alicia] Wah, there's a lot.

[Chloe] So if your mother-in-law like just sends you "Hello, send me money", then you will just send her money. But it was so real that you would believe it.

[Andre] Confirm one you see, you look at his face.

[Chloe] Best son-in-law in Singapore.

[Alicia] 40% - you will be one of them already.

[Andre] In that case, would you then think AI is detrimental to cyber security?

[Chloe] Well, we can't really always wear that lens right, with technology. So I personally don't think so. I think you know as much as malicious actors, which is like bad guys, use AI to improve their scamming techniques, we can also use AI to improve our scam detection and cyber defence. It's a double-edged sword. The problem is not the technology itself but in how the technology is used. And I think AI is here to stay, it's so ingrained in our lives now. So what we should focus on is not just being scared, but we should focus on how we can best use AI for good.

[Andre] You mentioned that AI has improved cyber defence. Could you elaborate more about it?

[Chloe] Of course, happy too. In fact, it's something you might be familiar with, because I'm from the GovTech Anti Scam Products team, and so are you, and we focus on anti-scam products. So one product that I'm working on is the recursive ML, Machine Learning Site evaluator, which is essentially a URL classifier that leverages machine learning to evaluate potential scam sites using their technical attributes. So these sites are then submitted by SATIS to Google Web risk, which then blocks these sites. So Andre, you're more familiar with SATIS as it's your brain child, so how about you tell us more about it.

[Andre] So SATIS stands for Scam Analytics and Technical Intervention System. It is the collaboration between MHA**, GovTech and the industry. So just now, earlier, I shared that there were 50,000 scam cases reported last year. That translates to 130 cases each day. So that's actually a lot of scam victims a day, and a lot of workload on the police officers as well. So we thought to ourselves, why not fight tech with tech, right? So, if the scammers are using deep fake AI, we should also have our own AI to combat this. So we built a system to proactively hunt for websites in the World Wide Web, and take them down automatically using AI. And today, I'm proud to tell you that SATIS, together with rMSE, analyses more than 1 million sites a month. And when we block those websites automatically, it's promulgated to more than 5 billion devices worldwide. *(**MHA - Ministry of Home Affairs)*

[Alicia] Saving the world guys, superhero.

[Chloe] 5 billion not, 5 million. 5 billion.

[Alicia] So, we have rMSE and SATIS to block malicious sites. To block scam calls and messages there's the ScamShield app that identifies and blocks them on your phone.

Recently, the government also introduced a common SMS Sender ID to help users identify legit SMSes from the government, which is from “gov.sg”. This is to counter the common tactic used to impersonate government agencies or public officers.

[Bryan] So, another tip for users is (to) look out for “go.gov.sg” links in various government-distributed messages. So this is a URL shortener that can only be used by public officers. So if you receive them, you can be sure that it will be from a trustworthy source.

[Alicia] It's very easy to fall prey to messages when it's regarding something like getting your vaccination or redeeming your CDC vouchers, especially when there's money involved. So remind people around you to only click on go.gov.sg links.

[Andre] Yup, absolutely.

[Chloe] Okay, noted.

[Alicia] So Chloe, earlier, you also mentioned that a lot of scams take place on social media. So you guys think, like what's the role of the companies in preventing scams?

[Chloe] Well, I definitely think they have a big role to play, because you know, with great power comes great responsibility.

So I don't think users will want to use an app or a platform if they're not assured that the platform is secure enough to use, where they can confidently use it and be assured that they're not likely to get scammed, or at least a very, very low likelihood.

So I think it is definitely in these companies, social media companies, best interest to really deploy whatever tech they can, and whatever operations or initiatives they can to reduce scams on these platforms.

[Bryan] I agree with Chloe. So there needs to be a balance between efforts put in from these platforms in actively preventing scams. Versus users who need to also stay vigilant when they are using these platforms.

[Andre] We have come to the end of today's episode. If you are keen to find out more about what we have discussed, you can check our website at http://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 http://go.gov.sg/ConnectWithGovtech. We will leave the links in the description. I'm Alicia

[Andre] and I'm Andre, and we'll catch you at the next GovTech Decoded.

(Outro music)