As Delivered

MINISTERIAL STATEMENT BY MRS JOSEPHINE TEO
MINISTER FOR COMMUNICATIONS AND INFORMATION AND MINISTER-IN-CHARGE OF SMART NATION AND CYBERSECURITY
FOR THE PARLIAMENT SITTING ON 15 FEBRUARY 2022

Combatting Online Phishing and Spoofing Scams

Mr Speaker, Sir

1. Scams have been around a long time. However, technology has increasingly enabled scammers to operate at scale across the globe, and their tactics have become more sophisticated by the year. Yet while the tactics have changed, at its heart, scammers use the tried-and-tested formula of exploiting their victims' fears and hopes.

2. Scammers do not respect geographical boundaries, seeking out victims wherever they can. These scams would often have originated abroad.

3. Minister Lawrence Wong has spoken about the enhanced protections in our banking system. I will focus on the upstream measures - how we can intervene through our communications infrastructure to fight scams. MOS Desmond Tan will speak later about enforcement as well as the continuing, crucial efforts in public education.

Were the OCBC scams the result of a cyber-attack or weaknesses in cybersecurity?

4. But first, let me assure members that the OCBC scams were not the result of a cyber attack or weaknesses in cybersecurity. This addresses questions by Mr Alex Yam regarding CSA's assessment, and A/P Jamus Lim on whether FIs met cybersecurity standards.

5. If I could use an analogy in the physical world, the scammers in this case did not manufacture special keys to break into the bank premises to steal from the customers' deposit boxes. Instead, they stood in front of the bank and tricked customers into

handing over their IC and keys. They then pretended to the bank teller that they were the real customers, accessed the deposit boxes and cleared them out quickly.

6. Why did the victims fall prey? Because the scammer looked real by wearing the correct uniform and name tag bearing the bank's logo. Why did the bank fall prey? Because the scammer was in possession of items that only real customers were expected to have.

7. In the physical world, the scammer's pressure tactics to hand over the IC and key might have raised an alarm. Likewise for the bank, branch managers might have noticed and made gentle enquiries as to the hurried manner in which the deposit boxes were emptied out. But in the digital world, where we have become so used to instant communications and transactions, our guard is down.

8. The OCBC scam was therefore not a result of a cyber attack or a breach of cybersecurity, which typically involves hacking or breaking into a system to steal information or assets. Instead, it was a classic case of deception, executed with speed and repeated at scale.

9. The use of SMS to reach potential victims is unfortunately becoming even more common and sophisticated. But it is not the only channel. Scammers have used it together with phone calls and emails to phish for information or spoof legitimate organisations. In other words, scammers are taking advantage of our communications infrastructure to reach even more potential victims, faster.

What measures are in place within our communications infrastructure to combat phishing and spoofing?

10. To combat phishing and spoofing by scammers, we should disrupt as many parts of their modus operandi as possible. Apart from enhanced safeguards in the banking system to prevent scams from easily succeeding, upstream measures are also needed to disrupt scammers' reach to potential victims. Ms Joan Pereira and Mr Chris De Souza are therefore right to ask how we can strengthen our defences through the telco networks.

11. It's useful to first step through how a phishing and spoofing scam is usually carried out. Typically, the scammer starts by contacting the victim, through phone calls or SMS. The victim is then tricked into surrendering their credentials or personal information.

12. In many cases, the act of surrendering credentials and personal information takes place on a scam website, something designed to look like the real website of a legitimate organisation. Compared to asking for such information by phone or SMS, no direct human interactions are required since victims themselves enter their details on a scam website. This allows such scams to be processed with greater scale and speed. This is why much of our upstream measures have focussed on blocking scam websites. It is a key part of disrupting the scammers' plans.

13. Website Blocking - On any given day, more than 90% of Singaporeans go online for various activities. SPF and IMDA work closely with Internet Service Providers to block scam websites. When consumers are led by scammers to these websites, they will be alerted to be vigilant. In 2020, we blocked about 500 suspected scam websites . By 2021, the net had been cast much more widely and 12,000 such websites were blocked. Countless more victims would have otherwise been scammed.

14. In fact, we have the capacity to block many more suspicious websites. However, this does not mean they will completely disappear from our screens. This is because scammers react quickly and dynamically to such blocks. In the OCBC case, more than 350 scam websites have been blocked. At the peak, we blocked around 52 sites in a single day,or 1 every 30 minutes. But the scammers were quick to create new websites over the course of their campaign. This pattern of behaviour will persist.

15. Nonetheless, website blocking remains important. We will continue to strengthen detection and reporting mechanisms to be more responsive. As mentioned by Minister Wong earlier, the banks will be enhancing their fraud surveillance systems. Government agencies will also explore the use of artificial intelligence to more quickly identify and block scam websites.

16. In addition, the National Crime Prevention Council will start a WhatsApp channel to crowdsource from the public, information on scam websites and messages. To ensure processes are in place for proper follow-up, this channel will be launched by the third quarter of this year.

17. Website blocking is part of the suite of upstream measures to disrupt the scammers' plans. But before they are lured to a scam website, victims may have been contacted by phone or SMS. Sometimes, the scammers get what they want without even leading the victim to a scam website.

18. Call blocking - Members will be familiar with scam callers impersonating officials from China. These scams started several years ago. During Covid times, the scam callers switched their masquerades, pretending to be the Police or other trusted organisations such as the Ministry of Health. Their messages were adapted to exploit concerns about vaccination or other Covid-related measures. These calls deploy what is known as "social engineering" techniques to cause fear and panic in their victims, using topical concerns that scammers know people are worried about. As most of these calls come from overseas, scammers will often seek to appear more credible by spoofing local numbers.

19. An important set of upstream measures therefore involves blocking these suspicious calls. Every month, the telcos block around 15 million, or one in seven of all incoming overseas calls to Singapore. We expect the number of scam calls to rise, given the changing tactics of scammers to increase their reach. They include, for example, incoming overseas calls that resemble phone numbers of our local Government agencies or emergency services. Overseas scam callers may also add a prefix "65" – without the "+" prefix – to give the impression they are calling from within Singapore. Since April 2020, telcos have also added the "+" prefix for all incoming overseas calls, to help alert their customers.

20. Many scam calls were averted through such measures. But more is needed. Our telcos plan to incorporate additional analytics to block more of these suspected scam calls. We estimate that up to 55 million calls will be blocked each month.

21. Mr Saktiandi Supaat and Assoc Prof Jamus Lim asked about the Do Not Call (DNC) Registry. The DNC Registry was not designed to prevent scam messages. Instead, it was created to allow individuals to opt out of receiving unsolicited telemarketing messages or calls. Scammers will of course, not take the trouble to check this registry before conducting their illegal activities.

22. Mr Speaker, the extent of call blocking needed shows just how persistent scammers are in reaching potential victims. Even if our telcos can block millions of incoming overseas calls, we must not be lulled into a false sense of security. Moreover, as each avenue becomes harder to break through, scammers turn to other channels. In the case of the OCBC scams, the SMS channel was exploited.

Is it safe to use SMS, and can we make it safer?

23. To better understand how it happened, it is useful firstly to recognise that SMS is an old technology. For many Singaporeans, it is more common these days to communicate with each other using messaging platforms such as Whatsapp and Telegram. Nevertheless, SMS is still being used by many organisations because it is a cheap and convenient way to reach many customers. All handphones, whether smart or not, can receive SMS. But the SMS system was never designed for secure communications. Together with its widespread use, this makes it an attractive channel for scammers to reach potential victims.

24. For example, legitimate senders can use an alphanumeric ID to make themselves more easily known to customers. Instead of a string of numbers, customers receive an SMS from a sender identified as, say, “ABC company”. However, this alphanumeric ID is not automatically protected as part of the SMS protocol. This means, unfortunately, that a scammer can use the same alphanumeric ID “ABC Company” and enter the message thread between the legitimate business sender and its customer. Members know by now this was what happened in the OCBC scams. As a result, the victims did not even realise they were communicating with the scammer, rather than OCBC itself.

25. SMS measures - Mr Desmond Choo, Mr Yip Hon Weng, and Mr Melvin Yong asked how SMS could be made safer. The gap I described above had in fact been identified by MAS and IMDA. Last year, the agencies started a pilot for SMS Sender ID protection. An organisation can register the alphanumeric ID that they use, thus reducing the risk of an illegitimate sender spoofing the same alphanumeric ID, and having the message appear within the same message thread. MAS has decided that all major retail banks must sign up to register the alphanumeric IDs they use to communicate with their customers. The Government has also committed that all its agencies will do likewise.

26. In addition, IMDA will require SMS service providers and telcos to check SMS senders against the Registry. SMSes that try to spoof registered IDs will thus not be delivered, as the sender details would not match Registry records. All organisations seeking to send SMSes using registered IDs to phone subscribers in Singapore must also have a valid UEN. This will help Police with investigations in the event of a scam.

27. Once these immediate measures are completed, the threat surface will be reduced. However, if an alphanumeric ID is not placed by an organisation into the registry, it cannot be protected. Observers have also pointed out that scammers can still use similar-looking alphanumeric IDs that are not in the registry, to trick potential victims. To further close these gaps, we will consider requiring all users of alphanumeric IDs to be registered. Scammers will then not be able to send SMS using alphanumeric IDs except by joining the registry. This protects legitimate senders. It will also provide more assurance to receivers of SMS messages, that an alphanumeric ID indicates a registered source.

28. These further measures will take time to implement and come at a cost, including to businesses. Businesses that choose not to register alphanumeric IDs will have their SMS messages appear only with their telephone number. Their customers can then choose to save the number in their own contact list to help them recognise future messages.

29. Given the implications, IMDA will study the matter carefully before deciding whether or not to mandate the registration of all alphanumeric IDs.

30. At the same time, organisations should rethink how they use SMS to communicate with their customers. As I mentioned earlier, SMS was never meant for secure communications. Where the message contains or will lead to the transmission of sensitive, confidential information or high value transactions, there should be more restraint. It is like postal services. They are generally safe, but we would not send very valuable items even using registered post.

31. One other area that Dr Shahira Abdullah asked about was clickable links. Although her question related to its use by MOH, the considerations are applicable to many other agencies and companies.

32. Members will know that clickable links are everywhere. They appear on websites, in our emails and of course our SMS messages. You find them too in WhatsApp, Telegram and many other apps. They are used extensively, because they are highly effective in getting people to take action. For example, using such links, millions of vaccination appointments were quickly and conveniently booked.

33. Unfortunately, clickable links have also been used for criminal purposes. MAS has ensured that banks discontinue their use in SMS communications with customers. However the removal of clickable links in many other settings will only erode convenience. More importantly, the loss of effective outreach in cases like vaccination registration could be detrimental to our people. A blanket removal must therefore be very carefully considered.

34. Mr Speaker, please allow me to briefly summarise in Mandarin.

35. 议长先生，有议员问，这次华侨银行诈骗案是否涉及网络袭击，或是因为银行的电脑系统出现疏漏，才会让不法分子有机可乘？

36. 事实并非如此。在这系列的诈骗案中，不法之徒并没有潜入银行的电脑系统，盗取财物。他们用的是典型的诈骗手法，让受害者误以为自己在跟银行沟通，因此提供了账户资料；然后在利用偷来的资料，登入受害者的银行户口，通过电子转账的方式，盗取受害者的血汗钱。

37. 通信系统再一次成为他们快速联系到大批受害者的渠道。但是和以往相比，诈骗过程的逼真程度高出许多。

38. 金融管理局因此进一步加强应对措施。于此同时，资讯通信媒体发展局也提升了通信系统方面的防范。加上内政部的公共教育计划，多管齐下，打压诈骗集团的作业方法。

39. 不过，我们都知道“道高一尺，魔高一丈”，这些诈骗者干案时，跨越国界, 目无法纪；想必在我们推出新措施的同时，他们也在摩拳擦掌，想出各种新方法，继续干案。

40. 尽管有了新的应对措施，我们也必须上下同心，方方面面的提高防线，才不会让这些不法之徒轻易得逞。

41. Mr Speaker, our additional safeguards underscore the importance of telcos in combatting phishing and spoofing scams. As part of our efforts to continuously strengthen our defences, we will require telcos to put in place enhanced safeguards in our networks. This includes blocking scam calls, SMSes and websites. We also expect them to do more to help their customers avoid becoming victims. Scammers change methods and tactics to evade detection, and our capabilities will need to likewise adapt. IMDA will work with the telcos to continuously strengthen their anti-scam capabilities.

42. We should recognise that even with best efforts, the network defences alone cannot block all scams. At every part of the chain, upstream and downstream, we are taking steps to reduce the risk. The measures in our communications infrastructure for example, reduces the available avenues for scammers to reach victims. As mentioned

by Minister Wong, MCI is also working with MAS to consider the shared responsibilities of all the key stakeholders in the ecosystem. Taken together, we should be able to significantly reduce the risk of consumers falling victim to scams.

Multi-pronged/ Multi-layered approach

43. Mr Speaker, I believe Mr Christopher de Souza has correctly characterised the problem of scams as one needing a multi-pronged response. Indeed, I would add that our approach is an ecosystem approach as what was described by Minister Wong. This has multiple layers of defence: no single layer providing a complete answer, but all layers reinforcing each other to disrupt the scammers' plans. To Mr Sitoh's question, this will prevent some types of scams from recurring. But our best defence against new types of scams is a vigilant public. Ultimately, they determine the extent to which we can prevent scams.

44. The public should therefore, also arm themselves with knowledge on scams and how to protect themselves and their loved ones, who might be less tech-savvy. There are tools such as ScamShield that can help to prevent some scam calls and SMS. MOS Desmond Tan will say more on these later.

45. At the same time, for our own long term success as a nation, digital transformation must continue. Mr Alex Yam is rightly concerned about the impact of these scams on digital adoption. We will strengthen public confidence in online transactions, raise awareness on good cyber-hygiene habits, and bolster the digital resilience of our citizens, a call also made by Ms Cheng Lihui. This is part of a whole-of-nation approach to safeguard Singaporeans against online threats, especially for the more vulnerable groups.

46. As part of these efforts, IMDA launched the Digital for Life (DfL) Movement to galvanise the people, private and public sectors to provide Singaporeans with skills, tools, and habits to navigate the digital domain safely and confidently. Many partners have kickstarted projects related to digital literacy and wellness. For example, the Lions Befrienders led a project – "Say No To Scams", where staff and volunteers teach

seniors about staying safe from online scams and harms. This included measures such as changing settings and installing apps to increase security on smartphones. They are also working on a scam simulation app to help seniors identify scams.

47. The DfL Movement will do its part to complement efforts by SPF, the National Crime Prevention Council and CSA. For example, the curriculum for seniors offered by the SG Digital Office has been updated to provide cybersecurity tips in topics such as, Digital Government Services, E-payments and Digital Transactions. The Media Literacy Council (MLC) has also produced tipsheets on e-commerce scams, online impersonation scams and loan scams. These are available and translated to the vernacular languages for different audiences.

Conclusion

48. All of us – banking institutions, telco operators, Government, businesses, individuals - have a role to play in the fight against scams.

49. Across the ecosystem, making these changes may result in additional cost and some loss of convenience. But they are necessary to better safeguard our people from scams. Equally important, they will help to uphold confidence in our digital journey.

+++