RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 014 – 22 January 2024

Combatting Mobile Phone Scams

By Damien D. Cheong

SYNOPSIS

Online scammers have been manipulating victims to install malware on their mobile phones, which facilitate unauthorised access to bank and other accounts as well as data theft. Financial losses among Singapore mobile phone subscribers have been significant. Installation of antivirus software and the Scam Shield app on mobile phones is a crucial first step to mitigate such threats.

COMMENTARY

Despite numerous anti-scam campaigns and initiatives by the relevant authorities in Singapore (e.g., CSA's Unseen Enemy Campaign in September 2023), many individuals are still falling victim and losing substantial sums of money. For instance, over the last few months of 2023, more than US$110,000 have been lost to scams involving mobile phones. While the execution modes of the scams appeared different, with some in the form of discounts on eggs, luggage, seafood, Chinese Lunar New Year goodies, and others impersonating representatives of banks, government agencies and even telcos, the scammers' ultimate aim was to get the victims to install malware on their phones to facilitate data theft or unauthorised access to their bank accounts or social media accounts.

Why Victims Get Scammed

In many cases, the victims, no matter how careful or technologically-savvy, are manipulated into complying with the scammers' instructions. This cunning social engineering utilises knowledge of the targets' specific traits to tailor the scams to particular contexts. Recent cases suggest that:

(i) *Love of a good bargain*: Scammers exploited Singaporeans' love of a good bargain and perhaps the rising cost of living to trick some into installing malware on their phones with the promise of substantial savings.

(ii) *Respect for authority*: Generally, Singaporeans have strong confidence and trust in government and public institutions. They also have high levels of trust in banks. By impersonating such institutions or the agents of such institutions (e.g., police officers), scammers were able to execute some scams successfully.

(iii) *Fear*: Related to the above, scammers capitalise on fear such as fear of non-compliance, and ironically, fear of one's account (bank or otherwise) being compromised, and other insecurities, to con victims, especially when they posed as agents of a trusted entity such as a bank, telco or law enforcement agency.

(iv) *Overconfidence*: Being technologically-savvy and relatively shrewd, many Singaporeans are overly confident that they would not fall for scams. Scammers know this and have shifted their operations to mobile phone apps such as Facebook, WhatsApp and SMS, where people are less guarded.

Compromise of Security

Apart from malware aimed at monetary theft, bad actors could deploy malware to undermine national security using the same social engineering techniques. For example, a user's phone if compromised via installation of malware could result in the user's data or identity being stolen. Furthermore, the phone could be used to eavesdrop on privileged conversations, to extract privileged information or to track movements.

Antivirus Software and Scam Shield App are Key

The Cybersecurity Agency of Singapore (CSA) has recommended that individuals install antivirus software and the Scam Shield app on their mobile phones as a key step to combat scamming. The agency has also compiled a list of recommended apps. The telcos – Singtel, Starhub and M1 – have antivirus apps and suites that customers can subscribe to for a small fee. This approach offers basic protection for mobile phones similar to having an antivirus software installed on any laptop or desktop system. If having antivirus on these systems are now the default, why not for mobile phones?

To encourage more people to install antivirus software and Scam Shield on their mobile phones, it is proposed that:

(i) Telcos, institutions, and organisations facilitate the installation of these apps on customers' and employees' phones that have not been tampered with (i.e., jailbroken). Counters and booths could be setup in public areas and manned by professional staff to guide and help with the installation of the apps on an individual's mobile.

(ii) Subscription to antivirus software, which is very affordable, can be borne by the telco, institution, or organisation for the first year, with the customer and/or employee bearing the cost of subsequent annual renewals.

The above proposal has its challenges, which include the costs related to manning of the counters and booths, providing the one-year antivirus subscription, promotional activities related to the exercise, and other associated costs. There is also the question of the individual's willingness to continue with the antivirus subscription after the first year. Furthermore, antivirus and the Scam Shield app do not provide "100 per cent protection" against infection.

These are valid concerns, but they are not insurmountable, and some can be addressed at a later stage. The aim of the exercise is to ensure that more people have a basic level of protection on their mobile phones as the cost of not doing so is very high. Although individuals must remain vigilant and adopt good cyber hygiene habits to protect their devices, having antivirus and Scam Shield app mitigate against inadvertently clicking on a malicious link and downloading malware.

Moving Forward: In-depth Research Needed

Security experts and public officials alike have warned that AI will make it more challenging to detect frauds and scams. Scams using deepfake images and audios are expected to grow, and malicious actors will constantly hone their craft to uncover vulnerabilities and to exploit them.

It is therefore proposed that more in-depth research into Singaporean traits and psyche be undertaken to identify possible avenues of exploitation and manipulation. This will help those working to combat scams to detect behavioural anomalies and to provide insights for developers to build anti-scam AI tools.

The battle against scammers is ongoing as they will continue to devise ways to circumvent existing defences. They will continue to cast their nets widely to steal money and information. It is up to consumers and mobile phone subscribers to frustrate their attempts as much as possible.

Meanwhile, it is increasingly necessary for more inter-governmental cooperation to manage the rapid spread of online scams and thefts. Recent actions by China and its neighbouring states to shut illegal online activities and industries along their respective border areas have been widely reported in regional media outlets. More cross-border actions must be taken, and the relevant preventive laws be entrenched to contain this huge challenge to digitalisation across the region.

Damien D. Cheong is Senior Manager, Horizon Scanning in the Executive Deputy Chairman's Office, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. His current interest is on emerging technologies relating to national security challenges.