JOINT NEWS RELEASE BY SINGAPORE POLICE FORCE AND CYBER SECURITY AGENCY OF SINGAPORE

JOINT ADVISORY ON MALWARE SCAMS AFFECTING ANDROID USERS

The Singapore Police Force (SPF) and Cyber Security Agency of Singapore (CSA) would like to raise awareness about the increasing prevalence of malware scams affecting Android users. The purpose of this advisory is to highlight the increasingly sophisticated tactics employed by scammers to deceive users into installing malicious apps on their Android devices. Once a malicious application is installed, scammers can remotely access the victim's device and steal sensitive information, including personal data and banking credentials to perform fraudulent monetary transactions.

2 SPF and CSA have observed a common set of tactics that scammers employ for malware scams perpetrated through social media platforms and e-commerce websites. The diagram in Annex A illustrates the typical attack stages of such scams.

Social Engineering Tactics Employed by Scammers on Social Media Platforms and E-Commerce Websites

3 During the "*Delivery*" phase as illustrated in Annex A, scammers have been observed to employ various social engineering tactics on social media platforms and e-commerce websites such as fraudulent advertisements (cleaning services, food products etc.), messages from fake friends, bank or government officials, and spoofed pop-up alerts to trick victims into installing a malicious application on their Android devices:

a) **Enticing Promotions:** Scammers often attempt to lure users with attractive offers and promotions, through eye-catching advertisements or under the

pretext of joining, or voting in fake campaigns allegedly organised by local brands on various social media platforms.

b) **Inauthentic Behaviour and Bots:** To enhance the illusion of legitimacy, scammers may deploy bots or fake accounts that exhibit human-like behaviour. These automated accounts may respond to messages, leave positive reviews and even share seemingly genuine experiences from using the goods or services.

c) **Building Trust:** Scammers often try to build genuine trust with the victims via phone calls or text messages. They may use local colloquialisms or Singlish, speak with a local accent or sound professional. These serve to create a false sense of familiarity, which may lower the victims' vigilance and lead to misplaced trust.

d) **Social Engineering:** Scammers may use social engineering techniques to gather information about the victims. They may ask seemingly perceptive questions, such as the victims' address and dietary preferences, under the guise of processing their orders. Scammers may also gather personal information belonging to the victims that can later be exploited.

e) **Deceptive Tactics:** Scammers may employ other tactics to deceive victims, such as requesting a small deposit or issuing a professional-looking invoice to enhance the appearance of legitimacy and make the transactions seem genuine.

4 After successfully gaining their trust of their victims, scammers may direct the victims to download a specific app, usually from unofficial sources not through the official app stores, to finalise the orders. They may also provide instructions on how to install the app (Refer to Annex B), including how to bypass default Android security controls. Some fake apps often have interfaces that are professional looking or resemble legitimate services, giving victims a further false sense of authenticity. Scammers may also call victims who are hesitant about installing the fake app to further pressure them. If the victims use an iPhone, the scammers may recommend that the victims borrow a friend or family's Android phone to "complete the order". Victims would only realise that they had been scammed when the scammers become uncontactable.

Why Android Devices May Be More Prone to Malware Infections

5 Android's open nature allows for greater flexibility and customisation for developers and users, but it also makes it easier for scammers to develop and distribute malicious apps. Users can download and install (sideloaded) apps from sources other than the official Google Play Store, which, combined with the large number of Android users, makes Android a more appealing platform for scammers.

6 However, it is important to note that Android devices are not fundamentally less secure than other mobile operating systems, as scammers are unable to bypass Android's security controls to install the malware unless users are deceived. Users of Android devices are advised to be aware of the potential risks and to follow the best practices to safeguard their devices.

Safety Tips for Online Offers

7 SPF and CSA would like to advise members of the public to adopt the following precautionary measures:

a) **Be Sceptical — Stay Safe and Not Sorry:** If the price is too good to be true, it probably is. Stay sceptical and verify the legitimacy of the offer with the company via official sources. Consult your family, friends, or colleagues if you remain unsure.
b) **Avoid Installing Unknown Apps:** Refrain from downloading apps from third-party websites outside official app stores like Google Play Store and Apple App Store, including arbitrary file hosting services. Malicious apps will usually request for unnecessary permissions, such as "*Accessibility Services*", that are unrelated to their intended functionalities. Review app permissions carefully during installation and reject any suspicious requests.
c) **Be Wary of Unusual Payment Requests:** Be cautious if the offers require you to use unconventional payment methods, such as bank transfers, gift cards or cryptocurrency. These methods are often favoured by scammers because they are difficult to trace and reverse.

d) **Report Suspicious Content:** If you come across an offer that seems suspicious or potentially harmful, report it to the social media platform to help protect others from falling victim to scams.

e) **Share with Care:** Always verify the legitimacy of the offer before sharing with your family, friends, and colleagues. If in doubt, avoid sharing it or enlist their assistance in helping you verify the legitimacy.

What to Do if You Fall Victim

8 If you suspect that you, or someone you know have fallen victim to a similar scam, do take the following steps:

a) **Switch your Device to Flight Mode:** If you suspect your device has been infected by malware, switch your device to the flight mode immediately to disconnect from the Internet. This will prevent the scammers from further accessing your device remotely.

b) **Run an anti-virus scan on your device:** Use an anti-virus software to scan and remove any malware detected in your device to ensure that all malware in your device is identified and removed.

c) **Check For Unauthorised Transactions:** If there are unauthorised transactions detected in your bank account(s) and/or Singpass account, contact your bank and inform them of the incident. Your bank should be able to freeze your bank account as a precautionary measure until investigations are complete.

d) **Report the Incident:** Further to informing your bank, report the incident to the relevant authorities and lodge a police report at any Neighbourhood Police Post or online at https://eservices.police.gov.sg. You may also wish to report the incident to SingCERT at https://go.gov.sg/singcert-incident-reporting-form.

9 After completing steps a) to c), if you believe that your phone has not been infected with malware, you may resume usage of your device by booting your device in safe mode to disable third-party apps temporarily, uninstall any suspicious apps, and install mobile security software from a trusted source to scan for remaining

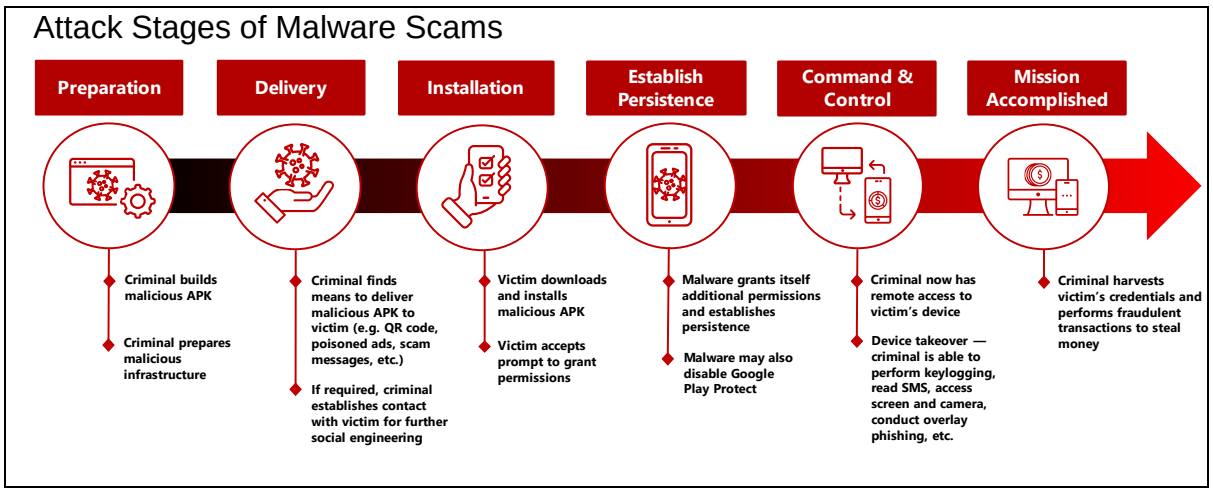
malware. As a further precaution, you may also consider doing a “factory reset” of your device and changing important passwords.

10 If you have any information relating to such crimes or if you are in doubt, please call the Police Hotline at 1800-255-0000, or submit it online at www.police.gov.sg/iwitness. All information will be kept strictly confidential. If you require urgent Police assistance, please dial ‘999’. For more information on scams, members of the public can visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688.

11 The rise in online scams requires vigilance and awareness to protect yourself from falling victim to cybercriminals. Stay informed, stay alert, and share this advisory with your family, friends, and colleagues. Together, we can raise awareness about the threats we face and foster a collective effort in combating ever-evolving malware scams.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
15 AUGUST 2023 @ 8.10 PM

Annex A



Annex B