POLICE NEWS RELEASE

POLICE ADVISORY ON EMERGENCE OF SCAMS INVOLVING MALWARE THAT INFECTS ANDROID DEVICES TO SIPHON OUT FUNDS FROM CPF ACCOUNTS AND BANK ACCOUNTS

The Police would like to alert members of the public using Android devices on the emergence of scams involving malware which resulted in losses from victims' Central Provident Fund (CPF) accounts as well as bank accounts. Since June 2023, the police have received at least two reports of such cases, with CPF savings loss amounting to at least $99,800.

2. Members of the public would come across advertisements for groceries (e.g., seafood) via social media messaging platforms like Facebook. Victims would contact the scammers via the social messaging platform or WhatsApp and the scammers would send a uniform resource locator (URL) to the victims. The scammers would inform the victims to download an Android Package Kit (APK) file, an application created for Android's operating system, found at the URL to order groceries and make payment. Unknown to the victims, the application would contain malware that allowed scammers to access the victims' device remotely and steal passwords, including passwords (e.g. Singpass passcode) stored in the device. The scammer might also call the victim to ask for their Singpass passcode, purportedly to create an account on the application.

3. Victims would be directed to fake bank application login sites to key in their banking credentials to make payment within the application. The malware with keylogging capabilities would then capture the credentials keyed by the victim in the fake banking sites and send it to the scammer. The scammers would then access the victim's CPF account remotely using the stolen Singpass passcode and request to withdraw the victims' CPF funds via PayNow. Once the CPF funds are deposited into

the victims' bank accounts, the scammer will access the victims' banking application and transfer the CPF funds away via PayNow.

4. The victims would only realise the scam when they discover unauthorised transactions made to their bank accounts.

5. The Police would like to remind members of the public of the dangers of downloading applications from third-party or dubious sites that can lead to malware being installed on victims' mobile phones, computers, and other Information Communications Technology (ICT) devices. Scammers will trick victims into installing malware-infected applications that are outside the app store. Members of the public are advised **not** to download any suspicious APK files on their devices as they may contain phishing malware.

6. The Police would also like to advise members of the public to adopt the following precautionary measures:

a) **ADD** - anti-virus/anti-malware applications to your device. Update your devices' operating systems and applications regularly to be protected by the latest security patches. Disable "Install Unknown App" or "Unknown Sources" in your phone settings. Do not grant permission to persistent pop-ups that request for access to your device's hardware or data.

b) **CHECK** - the developer information on the application listing as well as the number of downloads and user reviews to ensure it is a reputable and legitimate application. Only download and install applications from official app stores (i.e., Google Play Store for Android).

c) **TELL** - Authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately.

7. 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'.

8. For more information on scams, members of the public can visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688. To find out more about malware and the preventive steps that users can take to protect their devices, please refer to CSA's SingCERT advisory at https:// www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008. Fighting scams is a community effort. Together, we can *ACT* Against Scams to safeguard our community!

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
17 JUNE 2023 @ 8.35AM

Annex

Advertisement for seafood on Facebook which was a victim's first contact point with the scammer