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

JOINT ADVISORY ON TECH SUPPORT SCAM

The Police and the Cyber Security Agency of Singapore (CSA) would like to alert the public to a recurring tech support scam. The modus operandi involved victims receiving pop-up alerts on their computer claiming that their computer has been compromised, with a contact number to call for technical support. Since January 2023, at least 59 victims have fallen prey, with total losses amounting to at least $1.4 million.

2 For this variant of scam, victims would receive a pop-up alert while using an Internet browser on their computer informing them that their computer has been infected with a virus/spyware. Typically, victims would encounter such pop-up alerts on movie/video streaming sites (eg: dramacool, olevod.com). Upon clicking the alert, their screens might appear to freeze and may be accompanied by a loud beeping sound. The pop-up message would typically contain a “helpdesk” or “tech support” number and include instructions for the victims to contact the software provider. The number would usually be variants of +653159(XXXX) to create the impression that it was a valid local help desk contact number. Scammers impersonating tech support personnel would engage the victims when they called the number provided.

3 The scammers, claiming that the victims’ networks/computers had been compromised, would request the victims to download a remote access application, such as Teamviewer, Ultraviewer or AnyDesk. The scammers would instruct the victims to log into their Internet banking account where victims would provide their One-Time Password (OTP). In some cases, victims may also be asked to provide their credit or debit card details over the phone. By utilising the remote access, the scammers would transfer funds from the victims’ bank accounts or make fraudulent charges to the victims’ credit or debit card.

4 In another method of operation, the victims would be instructed to login to their Singpass accounts. The scammers would attempt to use the victim's Singpass to create accounts at various crypto/fintech websites (eg: Quione, Coinhako), or remittance services (eg: Western Union) upon gaining access to their account. Victims would then receive notifications from their Singpass app that their account was used to access such services. The scammers are known to use these services to facilitate the flow of illicit proceeds.

5 Members of the public are advised to take the following steps immediately if you believe you have fallen prey to such scams:

a. Uninstall any software that you have installed at the instructions of the scammers;
b. Perform a full anti-virus scan on your computer and delete any malware detected;
c. Log off and turn off your computer to limit any further activities that the scammers can perform;
d. Report the incident to your bank to halt further activities relating to your bank account(s);
e. Change your Internet banking credentials and remove any unauthorised payees who may have been added to your bank accounts, and
f. Report the incident to the bank and the Police.

6 Members of the public are also reminded to stay vigilant and adopt the following preventive measures to ACT against scams:

a. **ADD** - Set up transaction limits for our internet banking transactions, as well as transfers made over PayNow or PayLah. This will limit monetary losses. Consider also installing reputable anti-virus software/browser security extensions in computers that can detect and deter users from visiting scam or phishing websites.
b. **CHECK** - Before logging in to a digital service with your Singpass app, ensure that the domain URL displayed on your Singpass app's consent page matches that on your browser before proceeding. If they do not match, do not tap on the 'Log In' button on the consent screen. Learn to spot the

signs of phishing and do not share your personal particulars, bank login details, or Singpass ID, passwords and Two-Factor Authentication (2FA) details such as SMS OTP and Singpass passcode with anyone.

c. **TELL** - When in doubt, always call the official hotline of your software provider or government agency to verify whether the information you have received is sent by the organisation and if the transaction involves authentication through Singpass. If you have disclosed your banking details, report this to your bank immediately. Tell your family and friends about this scam so they do not fall for it.

7 For issues relating to Singpass, you may contact the Singpass helpdesk at 6335-3533 or support@singpass.gov.sg for assistance. You may also take these steps if you suspect that your Singpass account has been compromised:

a. Reset your Singpass password at go.gov.sg/reset-sp-pw, and
b. Check your Singpass transaction history[1] for any suspicious activities.

8 If you wish to provide any information related to such scams, please call the Police Hotline at 1800-255-0000, or submit it online at www.police.gov.sg/iwitness. If you require urgent Police assistance, please dial '999'. If you encounter scammers impersonating CSA officers, you can report the incident to CSA at www.csa.gov.sg/singcert/reporting. All information will be kept strictly confidential.

9 For more information on scams and cyber tips, members of the public can visit www.scamalert.sg and www.csa.gov.sg/Tips-Resource/Resources/gosafeonline or call the Anti-Scam Helpline at 1800-722-6688. Join the 'Spot the Signs. Stop the Crimes' campaign at www.scamalert.sg/fight by signing up as an advocate to receive up-to-date messages and share them with your family and friends. Together, we can help stop scams and prevent our loved ones from becoming the next scam victim.

---

[1] Follow these steps to check your Singpass transaction history:
Step 1: Visit the Singpass website and log in to your Singpass account
Step 2: Select 'View History'
If you are a Singpass app user, you may also view your transaction history by:
Step 1: Launching your Singpass app
Step 2: Tap on 'Settings' at the top right

SINGAPORE POLICE FORCE

CYBER SECURITY AGENCY OF SINGAPORE

24 FEBRUARY 2023 @ 6.40PM

Example of a Pop-up Alert: