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 modus operandi where scammers would approach victims under the pretext of assisting them to resolve computer or Wi-fi network issues. Since January 2022, at least 154 victims have fallen prey to such scams, with losses amounting to at least $7.1 million.

2 The Police and the CSA have observed two methods through which this tech support scam may occur:

a. In the first method, victims would receive a pop-up alert while using an Internet browser on their computer. The alert would indicate that their computer has been compromised, and include instructions for them to contact the software provider, such as Microsoft, at a stated number for assistance. The number would usually appear as variants of +653159(XXXX), leading victims to believe that it was a valid local help desk contact number. Victims who called the number provided would speak to scammers impersonating tech support personnel.

b. In the second method, the victims would receive an unsolicited call from scammers, who would claim that they are working for Internet Service Providers (ISPs) such as SingTel. The scammers would indicate that the victims' Wi-fi network had been compromised by hackers and they were calling to assist in resolving the issue. In some instances, the scammers would claim that there were fraudulent transactions made from the victims' bank account and that an investigation officer purportedly from government agencies such as the CSA or Police was investigating the incident. In such cases, the scammers might also send fake verification emails from spoofed email accounts such as “investigation@csa.gov.sg” to the victims.

3 In both methods, the scammers would request the victims to download a remote access application, such as Teamviewer, Ultraviewer, or AnyDesk. Under the pretext of resolving the issue, the scammers would instruct the victims to log into their Internet banking account, and provide their credit or debit card details and One-Time Password. Thereafter, utilising the remote access, the scammers would then 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 directed to scan a Singpass QR code on a phishing website with their Singpass app, claiming it was part of the verification process. By scanning the QR code and authorising the transaction, the victims would unintentionally give the scammers access to create cryptocurrency wallets with their details. These cryptocurrency wallets would later be used by scammers to facilitate the flow of illicit proceeds.

5 The Police and CSA would like to remind the public that no telecommunications service provider or government agency will request for your personal details, access to your online bank account over the phone or through automated voice machines, or ask for payment for services rendered.

6 We would like to advise members of the public to take these immediate steps 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. Log off and turn off your computer to limit any further activities that the scammers can execute;
c. Report the incident to your bank to halt further activities relating to your bank accounts;

d. Change your Internet banking credentials and remove any unauthorised payees who may have been added to your bank accounts, and

e. Report the matter to the Police.

7 Members of the public are also reminded to stay vigilant and adopt these preventive measures:

a. Ignore such calls and the caller's instructions. The '+' sign prefix indicates that it is an international incoming call. Domestic calls will not display the '+' sign prefix.

b. Do not panic and do not follow instructions to install applications, type commands into your computer or log onto your Internet banking accounts.

c. When in doubt, always call the official hotline of your software provider, telecommunications service provider or government agency to verify whether the information you have received is sent by the organisation and if the transaction involves authentication using Singpass.

d. When 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 not, do not tap on the 'Log In' button on the consent screen.

e. Never allow others to watch you enter your personal particulars, bank login details, or Singpass ID, passwords and Two-Factor Authentication (2FA) details such as SMS-One-Time-Pin and Singpass passcode.

f. Report any fraudulent activity in your bank account to your bank immediately.

8 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.

[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'

9 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 the CSA at www.csa.gov.sg/singcert/reporting. All information will be kept strictly confidential.

10 For more information on scams, you may call the National Crime Prevention Council's Anti-Scam Helpline at 1800-722-6688 or visit www.scamalert.sg. Together, we can help stop scams and prevent our loved ones from becoming the next scam victim.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
26 APRIL 2022 @ 8.40 PM

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