POLICE NEWS RELEASE

POLICE ADVISORY – SCAMMERS IMPERSONATING STAFF FROM LOCAL TELECOMMUNICATION SERVICE PROVIDERS OR OFFICERS FROM GOVERNMENT AGENCIES OFFERING TECHNICAL SUPPORT

The Police would like to alert the public about scammers impersonating staff from local telecommunication service providers, or officers from government agencies who are offering technical support. Between January and March 2020, the Police received at least 125 reports of such scams, with total losses amounting to at least S$4.5 million.

2 In some of the cases, victims would receive unsolicited phone calls from scammers impersonating staff members from local telecommunication service providers such as Singtel and Starhub. The scammers would deceive victims into believing that there were issues with their Internet connection and persuade them to download and install software applications such as ‘Teamviewer’ or ‘AnyDesk’ onto their computers, to allow remote access to their computers, on the pretext that this would enable the callers to help resolve the issues.

3 In some other cases, the scammers would claim to be from the ‘Cyber Crime Department of Singapore’ or the ‘Cyber Police of Singapore’, and deceive victims into believing that they had committed a criminal offence. The scammers would then direct the victims to download and install the abovementioned software applications on the pretext that doing so would help them better assist with investigations.

4 Recently, some scammers have also taken advantage of the COVID-19 situation to deceive victims who are working from home into believing that their Wi-Fi networks had been compromised. These scammers would also persuade the victims to download the abovementioned software, on the pretext that this would enable them to assist to resolve the issues.

5 In all these cases, once these software applications were installed on the victims' computers, the scammers would use them to remotely access the victims' computers and request the victims to log into their online bank accounts. When the victims were logged into their bank accounts, the scammers would surreptitiously transfer funds out of their bank accounts without them knowing that the transfers were actually happening.

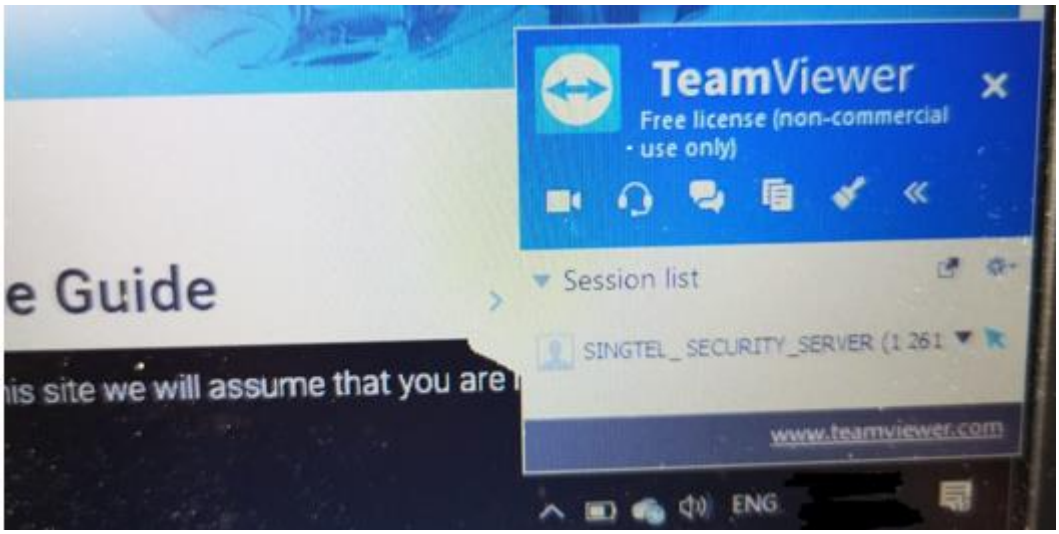

Image provided by a victim on a software application 'Teamviewer'.

6 We would like to advise members of the public to take the following immediate actions when you become aware that you may have fallen prey to such scams:

a. Log off and turn off your computer to limit any further activities that the scammers can execute;
b. Report the incident to your bank to halt further activities on your bank accounts;
c. Change your iBanking credentials and remove any unauthorised payees that may have been added to your bank accounts; and
d. Report the matter to the Police.

7 Members of the public are also advised to adopt the following preventive measures:

a. Beware of unsolicited calls from persons claiming that they are staff of telecommunication service providers or from a government agency, even if they claim there are issues with your telecommunication devices or allege that you are implicated in a criminal offence. Scammers may use Caller ID spoofing technology to mask their actual phone numbers and display different numbers. Calls that appear to be from a local number may not actually be made from Singapore.

   From 15 April 2020, all incoming international calls will be prefixed with a plus (+) sign. Stay vigilant when receiving any unexpected international calls, and reject those which spoof local numbers.

b. Do not panic and do not follow instructions to install applications, type commands into your computer or log onto your online banking accounts. No telecommunication service provider or government agency will request for your personal details or access to your online bank account over the phone or through automated voice machines. When in doubt, always call the official hotline of your telecommunication service provider to verify. It may also be wise to call a trusted friend or talk to a relative before you act on such instructions, in order to get a second opinion which can help counter possible misjudgments on your part.

c. Never provide your name, identification number, passport details, contact details, bank account numbers, credit card details, or One-Time-Passwords (OTPs) over the phone to unfamiliar or unverified persons. Such information can be very useful to criminals.

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'.

9 To seek scam-related advice, you may call the National Crime Prevention Council's anti-scam helpline at 1800-722-6688 or visit www.scamalert.sg. Join the 'Let's Fight Scams' 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.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
10 APRIL 2020 @ 4.45PM