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

JOINT ADVISORY ON THE DANGERS OF DOWNLOADING FILES FROM UNKNOWN SOURCES TO MOBILE DEVICES

The Police and the Cyber Security Agency of Singapore (CSA) would like to remind the public of the dangers of downloading files from unknown sources that can lead to malware installation on victims' mobile devices, which may in turn, result in confidential and sensitive data, such as banking credentials, being stolen.

2 Malware may infect mobile devices through various means, including through the downloading of free software from unknown sources, opening of unknown email attachments and visiting of malicious websites. Users should also be wary if they are asked to download unknown or suspicious Android Package Kit (APK) files, even with seemingly genuine naming conventions, such as GooglePlay23Update.apk or GooglePlay.apkUpdate.apk onto their mobile devices. Notwithstanding the references to "GooglePlay", these are not official APK files released by Google. Upon installation of the mobile malware, users' mobile devices may be exposed to the following risks:

a) Significant decline in the mobile devices' performance;
b) Unauthorised access to the mobile devices' systems/data that allow attackers to remotely control infected mobile devices, possibly resulting in loss of user control;
c) Unauthorised installation or uninstallation of applications;
d) Interception of SMSes;
e) Receipt of unwanted push notifications or warnings; and
f) Exfiltration of confidential and sensitive data stored in infected mobile devices such as banking credentials, stored credit card numbers, social media account credentials, private photos and/or videos, etc. Attackers can use such information to gain unauthorised access to users' social media accounts to

perpetrate impersonation scams or perform fraudulent financial transactions that results in reputational and monetary losses.

3 Members of the public are advised to follow the steps below to ensure that their mobile devices are adequately protected against malware:

a) Only download and install applications from the official app stores (i.e., Google Play Store for Android and Apple App Store for iOS). As an added precaution, check the developer information on the application listing and confirm it is the official developer before proceeding with the download;
b) Review the security permissions required by application and/or its privacy policy before installation;
c) Avoid clicking on pop-up ads, suspicious links or opening files or email attachments from unknown senders;
d) Ensure that your mobile devices are installed with updated anti-virus and anti-malware applications that can detect and remove malware; and
e) Ensure that your mobile devices' operating systems and applications are updated regularly to be protected by the latest security patches.

4 Users are advised to perform an anti-virus and anti-malware scan on their device if they suspect that their mobile device might have been exposed to malware infection. Users are advised to uninstall any unknown applications that are found in their devices immediately. Users can contact their vendor for assistance directly or consider reformatting the affected device to factory default if their mobile device still shows signs of infection. They are advised to back up the data from their device on an external storage device before reformatting.

5 To find out more about mobile malware and the preventive steps that users can take to protect their mobile devices, please refer to CSA's SingCERT advisory at www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
21 FEBRUARY 2023 @ 4.25PM