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

JOINT ADVISORY ON THE DANGERS OF DOWNLOADING APPLICATIONS FROM THIRD PARTY OR DUBIOUS SITES

The Police and the Cyber Security Agency of Singapore (CSA) would like to remind the public of the dangers of downloading applications from third party or dubious sites that can lead to malware installed into victims' mobile phones, computers, and other Information Communications Technology (ICT) devices. Such malware have resulted in confidential and sensitive data, such as banking credentials, being stolen.

2 Malware may infect ICT devices through various means, including through the downloading of software or applications from unknown sources, opening of attachments from unsolicited emails and accessing malicious websites. Users should also be wary if they are asked to download suspicious Android/Chrome/Google-related updates or any dubious Android Package Kit (APK) files onto their mobile devices, even with seemingly genuine naming conventions, such as the following:

- GooglePlay23Update[.]apk[1];
- GooglePlay.apkUpdate[.]apk;
- Chrome_update1123[.]apk;
- Chrome-upd13111[.]apk; and
- Chrome-update10366[.]apk

[1] Notwithstanding the references to "GooglePlay", these are not official APK files released by Google.

3 Upon installation of the malware, users' ICT devices may be exposed to the following risks:

a) Significant decline in the devices' performance;
b) Unauthorised access to the devices' systems/data that allow attackers to remotely control infected devices, possibly resulting in loss of user control;
c) Unauthorised installation of applications such as an additional Google Play or Chrome App on the device;
d) Interception of SMSes in mobile devices;
e) Persistent pop-ups from the application requesting for permission to access the device's hardware or data which may not be necessary for the application's function; and
f) Exfiltration of confidential and sensitive data stored in infected devices such as banking credentials, stored credit card numbers, social media account credentials, private photos and/or videos, etc. Attackers can then use such information to gain unauthorised access to users' social media accounts to perpetuate impersonation scams or perform fraudulent financial transactions that result in reputational and monetary losses.

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

a) Only download and install applications from the official application stores (i.e., Google Play Store for Android). As an added precaution, 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;
b) Disable "Install Unknown App" or "Unknown Sources" in your settings; (Refer to Annex A);
c) Exercise caution when clicking on advertisements embedded within applications that lead to a third-party website that prompts download of files;
d) Do not grant permission to persistent pop-ups (Refer to Annex B) that request for access to your device's hardware or data;

e) Ensure that your devices are installed with updated anti-virus/anti-malware applications that can detect and remove malware; and

f) Ensure that your devices' operating systems and applications are updated regularly to be protected by the latest security patches.

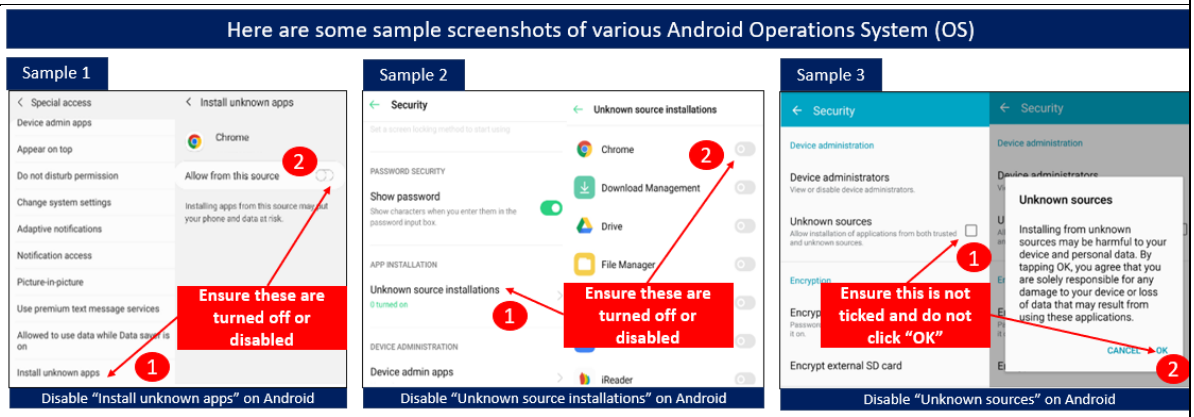
5 Users are advised to turn their mobile devices to 'flight mode' and perform an anti-virus/anti-malware scan on their device if they suspect that they might have been exposed to malware infection. Users are advised to uninstall any unknown applications that are found in their devices immediately (Refer to Annex C). Users can contact their product manufacturers for assistance directly or consider reformatting the affected device to factory default if their device still shows signs of malware infection. They are advised to back up the data from their device on an external storage device before reformatting.

6 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.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
11 APRIL 2023 @ 6.10 PM

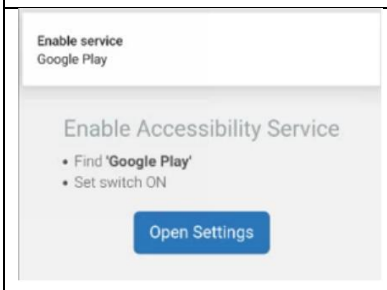
Annex A

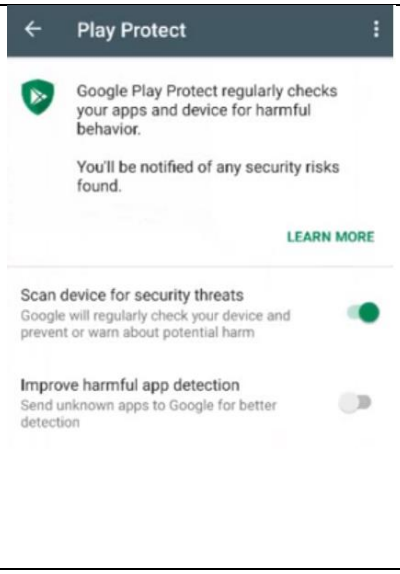
Examples of Disabling “Install Unknown App” or “Unknown Sources” in Settings

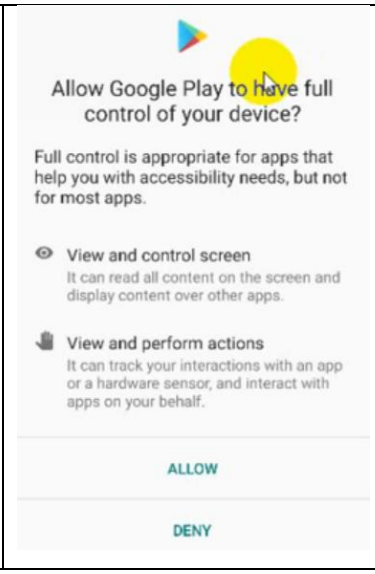


Annex B

Examples of Pop-Up Notifications







Annex C

Screenshot of How Genuine and Fake Apps Appear in Your ICT Devices