Joint Advisory on Protecting Mobile Devices from Malicious Wireless and Wired Connections

The Cyber Security Agency of Singapore (CSA) and the Singapore Police Force (SPF) would like to highlight the possible means by which mobile devices and the data within can be compromised through malicious wireless and wired connections, and the preventive measures which can be implemented to mitigate such threats.

Mobile devices, including smartphones and tablets, are essential tools for communication and productivity. With their increasing ubiquity, they become highly attractive targets for cybercriminals due to the trove of data which they contain, such as personal data, financial data, login credentials and business information. Cybercriminals will typically leverage such information for financial gain or to carry out other malicious activities.

Mobile devices and the data contained within can be compromised via various means. Such compromises can occur when devices are inadvertently connected to rogue WiFi access points, when the device's file sharing functions are not secured, through bluebugging, or through juice jacking. The following section will provide further details on these attack vectors and specific measures on how devices can be secured.

Rogue WiFi Access Points

A rogue WiFi access point is an unauthorised wireless access point set up without the knowledge or consent of the network administrator or owner. As part of an "evil twin" attack, the rogue WiFi access point will masquerade as a legitimate access point with the same name and security settings. Once users connect their devices to this rogue network, cybercriminals can intercept and steal the data or credentials.

In order to avoid falling victim to such attacks, users are advised to avoid using public WiFi networks for sensitive activities such as online banking or to use a virtual private network (VPN) to encrypt network traffic and protect their data. Users should also disable automatic WiFi connections on their devices to prevent it from connecting automatically to unknown or rogue access points without their knowledge.

Unsecured File Sharing Functions

File sharing functions such as AirDrop on iPhones and Nearby Share on Android devices can be used by cybercriminals to infect devices with malware. When not properly secured, it may also grant cybercriminals in the vicinity access to the device's data, allowing for data exfiltration.

Users are advised to disable file sharing functions on their devices when not in use to prevent cybercriminals from exploiting them for malicious purposes. Users may also wish to configure their file sharing settings to only allow discovery by their contacts, to reduce the risk of unauthorised access.

Bluebugging

Bluebugging is a type of attack that allows cybercriminals to gain access to user devices through a detectable Bluetooth connection. Successful compromise through bluebugging may allow the attacker to steal information from the device and possibly install malware.

To avoid falling victim to bluebugging, users are advised to disable the Bluetooth function when not in use and/or to set their devices to the "non-discoverable" mode. This will prevent cybercriminals from detecting the user device and attempting to establish a connection for malicious purposes.

Juice Jacking

Juice jacking is a type of cyber-attack where cybercriminals tamper with a charging port or USB cable to infect a device with malware or steal data. Such attacks may occur when attackers tamper with USB charging stations that are available for free at public locations with high traffic.

Users are advised to use a USB data blocker when connecting their devices to publicly accessible charging ports. A USB data blocker is a device that physically blocks data transfer due to the absence of data wires. It acts as a shield between their phones and the charging port or cable, preventing cyber criminals from accessing users' data. Users are also encouraged to disable automatic file transfer in their mobile device's settings to ensure that there is no data transfer through USB connections. Users may consider switching their devices off before charging them to limit any data transfers.

Generally, there will be risks when connecting to wired or wireless points, but these risks can be mitigating by taking appropriate measures to mitigate them. Users should also employ the following non-exhaustive measures to safeguard their mobile devices and the data contained within from possible compromise:

- Keep the device operating system and applications updated with the latest security patches and fixes;
- Download and install anti-virus applications onto the device, keep it updated, and perform regular scans;
- Download applications from the official Play Store (Android) and App Store (iOS) only;
- Use a strong and unique password/passcode to protect the device from unauthorised access;
- Do not click on suspicious links or attachments and visit websites from trusted sources only.

If you suspect that you have been a victim of a cybersecurity incident, we encourage you to report the incident to SingCERT through our incident reporting form at https://go.gov.sg/singcert-incident-reporting-form.

References

https://www.cisa.gov/news-events/news/securing-wireless-networks
https://support.apple.com/en-sg/guide/security/sec2261183f4/web
https://www.androidauthority.com/what-is-nearby-share-3197368/
https://www.latestly.com/technology/what-is-bluebugging-how-do-hackers-use-bluetooth-enabled-devices-to-steal-data-how-can-you-protect-your-phone-know-everything-here-4530305.html
https://www.zdnet.com/article/fbi-warns-of-juice-jacking-charging-stations-in-public-areas-how-to-stay-protected/
https://www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008

Issued by:

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY