Importance of Reviewing Permissions for Applications in Android Devices

There have been reports of cyber criminals developing malicious applications (apps) for Android devices with the intent to steal personal information and infect devices through requesting excessive permissions from users.

Apps for Android devices frequently request for permissions to access various resources and data stored on devices in order to function. These could range from permission requests from photo editing apps to access your photos, to that from malicious apps to log users' keystrokes to steal personal information. It is therefore crucial to exercise vigilance when granting permissions to the mobile apps.

The following (non-exhaustive) is a list of pre-cautionary measures:

Understand the purpose

Review the app's purpose and functionality before granting permissions. Determine if the requested permissions align with the app's intended use. If the permissions are not necessary for the app to function, consider it a red flag as granting unnecessary permissions can expose personal information and increase the risk of malicious activities.

Assess critical permissions

Android devices classify permissions as "dangerous" if they potentially affect users' privacy, the functionality of other app, or the device's operation. These permissions include:

- Accessibility
- Body sensors
- Calendar
- Camera
- Contacts
- GPS location
- Microphone
- Calling
- Texting
- Storage

In particular, the accessibility permission stands out as one of the most "dangerous" permissions as it possesses a high potential for exploitation by malware, such as Remote Access Trojans (RATs). This permission provides user interface enhancements to assist users with disabilities by making it easier for them to navigate Android devices. However, this functionality also comes with potential security risks, as the accessibility service can be abused to steal sensitive information or allow cyber criminals to control the device remotely. As such, users are encouraged to exercise caution when granting access to the accessibility permission by verifying if the app genuinely requires these permissions and if the reasons provided are legitimate.

Users can adopt the following considerations when assessing these permissions:

- Grant permissions on a case-by-case basis and adopt a principle of least permissions, granting only permissions that are necessary for an app to function as intended.
- Prioritise users' privacy by denying unnecessary or excessive permissions that are not essential for the app's primary purpose.
- Select apps that allow users to selectively grant or revoke permissions as needed.

Take into account user reviews and ratings of the app

Read user reviews and ratings for an app as they can provide insights into any privacy or permission-related concerns that other users have encountered. If multiple reviews mention privacy issues or excessive permissions requests, it would be prudent to reconsider installing or granting permissions to that app.

Research on app source and developer reputation

Download apps from official app stores such as Google Play Store. Avoid downloading apps from unknown or third-party sources, as they are unverified and may contain malware that exploit permissions granted for unauthorised access to users' information and devices.

Periodically review permissions granted to all apps

Android allows users to review an app's permissions before and after installation. Leverage Android's built-in permission management features, such as permission prompts and permission usage history. After installing an app, users can review the permissions that were granted under the app's settings and revoke unnecessary or excessive permissions. Regularly check permission usage history to identify apps with excessive access or suspicious behaviour.

Users can review their permissions by going to **Settings > Apps > Select the app > Permissions.**

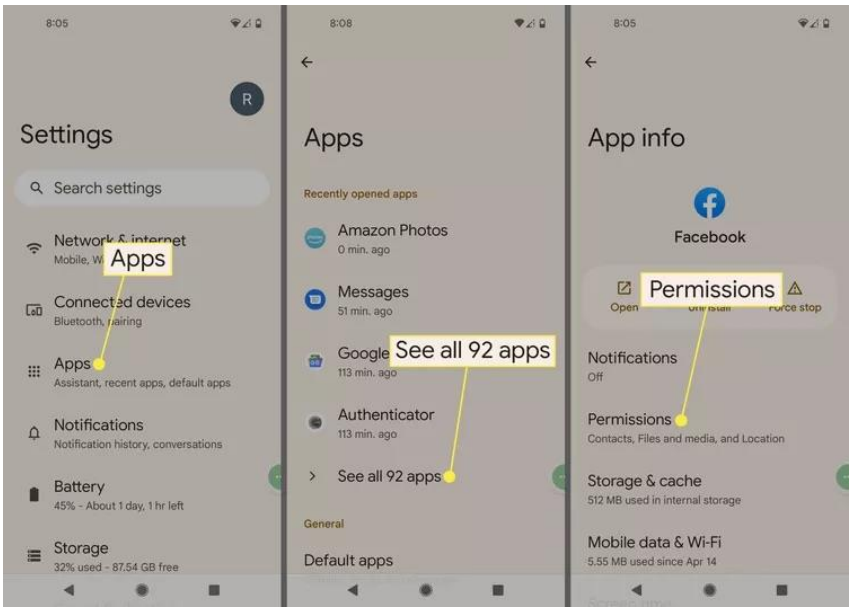

Figure 1: How to Review Permissions

By staying vigilant and taking precautionary measures, users can safeguard their devices against potential security risks while enjoying the benefits of the Android ecosystem.

More information is available here:
https://www.avg.com/en/signal/guide-to-android-app-permissions-how-to-use-them-smartly
https://www.guardsquare.com/blog/protecting-against-android-accessibility-services-threats

Issued by:

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY