**Keep Your Mobile Device Safe for Android User**

1. Procure Mobile Device from Official Distribution Channels
2. Restrict Installation of Applications from Unknown Sources
3. Set Strong Password and Screen Lock
4. Use Up-to-date Anti-malware Security Software
5. Update Operating Systems, Mobile Applications and Browsers
6. Encrypt Your Mobile Device
7. Remove Insecure and Unnecessary Wi-Fi Connection Profile
8. Disable GPS and Location Services
9. Remove Mobile Applications That Abuse Sensitive Permissions
10. Perform Device Backup
11. Completely Remove Data Before Giving Away Or Selling Your Devices
Index

1. Procure Mobile Device from Official Distribution Channels ......................... 3
2. Restrict Installation of Applications from Unknown Sources ....................... 4
3. Set Strong Password and Screen Lock .......................................................... 6
4. Use Up-to-date Anti-malware Security Software .......................................... 9
5. Update Operating Systems, Mobile Applications and Browsers ................... 10
6. Encrypt Your Mobile Device ............................................................................ 12
7. Remove Insecure and Unnecessary Wi-Fi Connection Profile .................... 14
8. Disable GPS and Location Services ................................................................. 16
9. Remove Mobile Applications That Abuse Sensitive Permissions .................. 18
10. Perform Device Backup .................................................................................. 19
11. Completely Remove Data Before Giving Away Or Selling Your Devices . 20
    Disclaimer ....................................................................................................... 22
### 1. Procure Mobile Device from Official Distribution Channels

**RISK**
Firmware can be modified by dishonest sellers or middlemen to steal personal information or inject malware.

**CHECK STEPS**

- **Tool(s) available**
  Users are recommended to procure mobile devices from official distribution channels such as authorised distributors, authorised resellers, or official online shop.

  If users procure brand new product but the original factory seal on the package box is broken, users may inquire the sellers and even request a new product with original and intact factory seal.

**MORE TIPS**

- ✓ Adopt the latest firmware provided by the manufacturer, and update the newly acquired mobile device as soon as possible.

- ✓ Install anti-malware security software and perform full scan for your newly acquired mobile device as soon as possible.
Restrict Installation of Applications from Unknown Sources

RISK
Mobile applications distributed from unknown sources have higher risk to contain malicious codes.

CHECK STEPS

**Tool(s) available**

Function: Detect whether system setting restricts application installation from unknown sources.

- Bluebox Security Scanner
- Secure Update Scanner

**System settings**

Purpose: Restrict application installation from unknown sources.

Go to **Apps**, tap **Settings** -> Tap **Lock screen and security** and uncheck **Unknown sources**
Purpose: Enable *Verify apps* feature to prevent and warn any potential harm at your device

Nexus device: Go to the app *Settings*, under *Personal*, tap *Security*, -> Scroll to *Verify apps* and check it.

Other devices (settings vary between different products): Go to the app *Google Settings* -> *Security*, under *Verify apps*, check the *Scan device for security threats* option.

**MORE TIPS**

- Only download mobile applications you need and only download them from official sources, such as the Google Play Store.

- Stay alert to unusual permission requests when installing new mobile applications or application upgrades and quit the installation process if necessary.
3 Set Strong Password and Screen Lock

RISK
Unauthorised person can access information in an unlocked mobile device without the owner’s knowledge.

CHECK STEPS

**System settings**

Purpose: Enable alphanumeric password protection and screen lock feature.

**Step 1:** Go to **Apps** and tap **Settings** -> Tap **Lock screen and security** -> Tap **Screen lock type**, -> Tap **Password** and type in a strong password and tap **Continue** -> Re-enter the password and tap **OK**
Step 2: Go to Settings, Tap Display -> Tap Screen timeout and select 1 minute -> Go back to Settings
Step 3: Tap **Lock screen and security** and **Lock automatically**

Confirm that Lock automatically is set to **Immediately** and **Lock instantly with power key** is enabled.

MORE TIPS

✔ Set strong password instead of unlock pattern for better security, as unlock pattern could be trivially peeked by someone around you.

✔ Create passwords that are easy for you to remember but difficult for others to guess, with assistance of free online tools to learn and practice.

✔ Don't leave your mobile device unattended.
Cyber Security Information Portal (www.cybersecurity.hk)
Keep Your Mobile Device Safe for Android User

4 Use Up-to-date Anti-malware Security Software

RISK Mobile applications and files that look innocent can contain malicious codes and may not be easily noticed by user before it causes significant damages.

CHECK STEPS Tool(s) available
Function: Detect malware attack and remove malware from infected mobile device.

- Avast! Mobile Security
- ESET Mobile Security & Antivirus
- Other anti-malware security software

Note: Please be aware that the exact process for applying the security features will vary between different products. It is recommended that users follow the instructions contained in the official user manual where possible.

MORE TIPS

- Enable auto-update features of the anti-malware security software to keep the software and its definition up-to-date.
- Enable real-time protection feature and perform full scan of mobile device in periodic basis (e.g. weekly).
- Stay alert to symptoms that might indicate a malware infection, such as battery drain, performance clogging, unusual large data usage, etc.
- Be aware that fake anti-malware software and rogue pop-up security alerts are popular ways for tricking users to download malware onto their devices.
Update Operating Systems, Mobile Applications and Browsers

Mobile devices with known security weaknesses are more susceptible to malware infection and other cyber attacks.

**CHECK STEPS**

**Tool(s) available**

Function: Detect outdated Android OS, browser and application.

- [Check and Secure website](#) (Detect outdated Internet browser and plug-in)
- [Google Play](#) (Detect software updates)
- [Security update scanner](#) (Detect outdated Android OS)

**System settings**

Purpose: Update Android OS from the device manufacturer.

Go to **Apps**, tap **Settings** -> Tap **About device** and **Software info** for displaying the current Android version -> Go back to **Settings** -> Tap **Software update** and **Download updates manually**
MORE TIPS

✓ Uninstall end-of-support software products or upgrade to another software product that has security updates.

✓ Avoid performing online banking and other sensitive operations from mobile devices without security updates.

✓ Beware that some mobile devices may not support the latest version of Android OS due to incompatible hardware or lack of support by device manufacturer.

✓ Do not visit suspicious websites or follow the links provided in those websites, as they may force a browser to download files without user's knowledge.
Encrypt Your Mobile Device

**RISK**
Data in a mobile device can be leaked out, if it is lost or stolen.

**CHECK STEPS**

**System Settings**
Purpose: Enable device encryption feature.

Go to **Apps**, tap **Settings** and tap **Lock screen and security** ->
Tap **Secure startup** and check **Require password when device powers on** on -> Enter lock screen passcode or password when prompted -> Tap **Next** to finish.
Note: When encryption is enabled, Android uses your password to generate an encryption key that is then used to encrypt the device. This password is then required every time the device is powered on.

MORE TIPS

 ✓ Enable encryption for the external storage card in your mobile device before storing sensitive information on it.

 ✓ Use security software that allows you to remotely track, lock or erase your mobile device in case it is lost or stolen.
Keep Your Mobile Device Safe for Android User

Remove Insecure and Unnecessary Wi-Fi Connection Profile

RISK

Mobile devices with insecure Wi-Fi connection profile have higher risks to join untrusted or spoofed Wi-Fi networks automatically.

CHECK STEPS

Tool(s) available

Function: Detect insecure Wi-Fi connection profile.

- Bluebox Wi-Fi Cleaner

System settings

Purpose: Remove insecure and unnecessary Wi-Fi connection profile.

Go to Apps, tap Settings and tap Connections -> Tap Wi-Fi -> in the Wi-Fi settings, locate the Wi-Fi network that you wish to forget, tap on that entry and tap Forget.
MORE TIPS

✓ Avoid handling personal or sensitive information when using public Wi-Fi

✓ Disable wireless connection after use.
Keep Your Mobile Device Safe for Android User

Disable GPS and Location Services

RISK
Mobile device allow installed applications and visited websites the ability to know and track user location without users’ knowledge.

CHECK STEPS

System settings

Purpose: Disable GPS and Location Services.

Go to Apps, tap Settings and tap Connections -> Uncheck Location
<table>
<thead>
<tr>
<th>MORE TIPS</th>
<th>✓ Remove applications required location tracking, if no operational needs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓ Disable GPS function and location services after use.</td>
</tr>
</tbody>
</table>
Remove Mobile Applications that Abuse Sensitive Permissions

Mobile applications, obtained sensitive permissions can perform high risk actions without user knowledge, such as enable camera and send SMS.

**CHECK STEPS**

**Tool(s) available**

Function: Detect and / or remove risky mobile applications that can access personal and location information, use camera and audio recording or change system settings.

- **F-Secure Mobile Security** (Detect and uninstall risky mobile applications)
- **Avast! Mobile Security** (Detect risky mobile applications)
- **Google Play** (Uninstall mobile applications)

**MORE TIPS**

- Before installation, research for whether the mobile application is reputable by researching via public search engine using the application name with other keywords for example "review", "complaints", "compare", etc. You can make reference to the [Hong Kong Google Play Store's Apps Security Risk Report](https://www.cert.gov.hk) at the HKCERT website to get more information on high security risk mobile application.

- Inspect thoroughly all permission requests during the process of installation, in particular those involving sensitive permissions.

- Review if any additional permission request is necessary when updating applications.
Perform Device Backup

Data cannot be recovered in case of malware infection, hardware failure and device loss.

**Tool(s) available**

Function: Backup data in mobile device to your computer and restore data.

- HTC Sync Manager
- LG PC Suite
- Sony PC Companion
- Samsung Kies

Note: You can conduct data backup and restore by using other backup solutions –

**Step 1:** Go to *Applications* and tap *Play Store*

**Step 2:** Search for "Backup and restore mobile to local"

**Step 3:** Research for which listed mobile backup software is suitable to your mobile device and whether it is reputable by researching via public search engine using the software name with other keywords for example "review", "complaints", "compare", etc.

**Step 4:** Follow instructions in the official user manual to conduct data backup and restore.

**MORE TIPS**

- Backup regularly and protect your backup data securely.
- Test the restore procedures to ensure the backup data can be restored.
- Assess security risks before synchronising data to cloud services and avoid automatic backup of sensitive data to them.
- Protect your online user account with a strong password and enhanced authentication mechanism such as 2-factor authentication if available, in particular those for cloud backup. Please visit InfoSec website for more good practices on *Handling User Account and Passwords*. 
Completely Remove Data before Giving Away or Selling Your Devices

Data can be accessed or recovered by data recovery applications.

Tool(s) available

Function: Securely delete data in mobile devices’ storage.

- Secure Wipe (Sanitize free space)
- Secure Delete (Securely delete files or folders)
- Andro Shredder (Securely delete files and sanitize free space)

To ensure all the information stored in the mobile devices is completely deleted, in addition to "Factory Reset", please take following steps before handover or disposal of the mobile devices:

Step 1: Run the mobile device "Factory Reset" function;

Step 2: Fill up all storage space with large dummy files;

Step 3: Use secure deletion application (above are some examples) to erase all data;

Step 4: Repeat step 2 and step 3 for external storage (e.g. SD card);

Step 5: Enable full disk encryption with strong password; and

Step 6: Run the mobile device "Factory Reset" function again.
**MORE TIPS**

- You may connect your mobile device to your personal computer and manually shred files on your device using computer’s file shredding software.

- Timely update your device’s operating system.

- Do not "root" the mobile device to override usage and/or access limitations.

- Perform backup before erasing the data.

- In order to protect data, enable full disk encryption with strong password for new mobile device after purchase.
Disclaimer

The health check settings here are proactive in nature and intended for improving mobile device security, as they may change the user experience and interfere with the functionality and utility of some applications. The exact process for applying the security features during the health check will vary between different products. It is recommended to follow the instructions contained in the user manual provided at the official website of the manufacturer where possible.

Users are also recommended to observe the Important Notices of Cyber Security Information Portal and read the user agreements and privacy policies of the security software and tools before download and use them.