Protect Privacy by Smart Use of Smartphones

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Smart mobile devices such as smartphones and tablet computers are now commonplace. While these smart mobile devices (collectively referred to as smartphones in this leaflet) are making lives easier for the busy Hong Kong public, they do store unprecedented amount of sensitive information about you, such as where you have been, photographs you have taken and where they have been taken, text messages you have sent and received, and address book contacts and social network user names/passwords you have saved that are often considered very private and personal to the individuals concerned.

This leaflet aims to familiarise you with the pitfalls of using smartphones so as to avoid falling victim to unauthorised access or loss of personal data stored in them.

England
Shanghai
Hong Kong

Securing your smartphones

- **Install Anti-virus Software –** There are more and more viruses targeting smartphones so you should install reputable anti-virus software.

- **Install Anti-theft Software –** You should install and configure anti-theft software that could help you locate lost smartphones or erase all data (e.g. phone contacts, photos etc.) stored in the smartphones should they be lost. Remember to carry out regular backup of your smartphone data so that you don't lose your data if you lose your smartphone.

- **Enable Automatic Screen Lock –** A screen lock with complex password is your first line of defence against prying eyes when you leave your smartphones unattended or if they are lost.

- **Do not tamper with the operating system –** Jailbreaking or rooting smartphones generally would weaken the security protection and open the back doors for hackers, and should not be attempted.

- **Erase information stored in the smartphones before repair/disposal –** Remember to follow the manufacturers' instructions to wipe the memory (and remove any memory cards) of smartphones before disposal or sending for repair. If it is not possible to wipe the memory, make sure you only send them to reputable service centres.

- **Record the IMEI number[1] –** Record the unique IMEI number of your smartphone. It may be very useful if you need to identify your smartphone later.

[1] International Mobile Equipment Identity number is a unique identification number of many types of mobile phones and can be displayed on the phone screen by entering *#06# on the keypad.

Securing data stored in smartphones

- **Phonebook is for contact information only –** Many apps would upload and share your phonebook so do not store sensitive information (such as PIN, building access code, account name/number/password) in phone books.

- **Use encryption –** If you need to store such sensitive information in the smartphone, make sure it is protected by encryption offered by the smartphone or a third-party.

- **Don’t use untrusted Wi-Fi –** Public Wi-Fi hotspots could be faked for capturing your communications. If you are not sure, use the data access plan of your mobile service or do not visit any websites or use any apps that require logging on when using public Wi-Fi.

- **Clear browser history –** Consider the need to regularly clear the browsing history in the browser (through the browser setting) to avoid them from being accessed by others.

Safe use of apps

- **Is it a genuine app? –**

  Not all smartphone application stores verify their apps and it is a well-known fact that there are fake apps around. Make sure you know what apps you are downloading before installing them. Don't download or use preloaded software from unofficial channels.

- **What could an app access? –**

  Before installing an app, you should learn what information it will access, upload and/or share from your smartphone and decide if it is worthwhile to exchange your privacy for the use of the app.

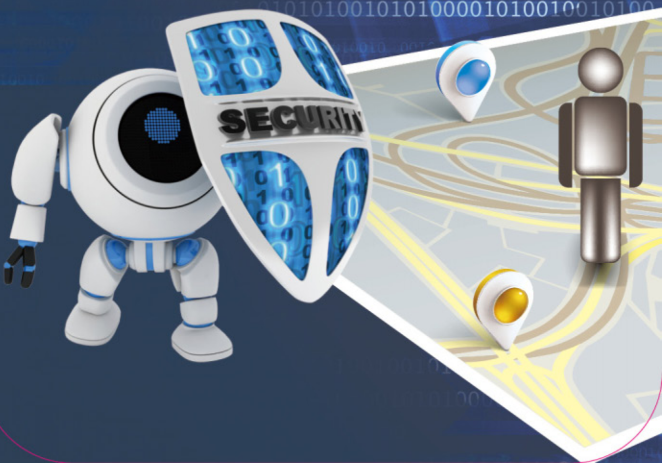
- **Review your apps –**

  You should regularly review what apps you have installed on your smartphone and uninstall those that you no longer use to avoid information from being accessed/shared/uploaded by apps unnecessarily or inadvertently.

Location information

- **Tagged pictures –**
  By default, many smartphones automatically tag all pictures taken with geo-location information (i.e. where they were taken). You should consider if you want this feature and switch it off as necessary.

- **Permission –**
  If supported by the operating system, you should regularly review what apps are accessing your location service and decide if you want to remove the permission.



- **Tracked trails –**
  If you leave the location service switched on, some apps may upload or keep your trail without your notice. Consider switching off the location services when not needed. If your trail has been uploaded to a server, find out how to remove past records if it bothers you.

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Enquiry Hotline:	(852) 2827 2827
Fax:	(852) 2877 7026
Address:	12/F, 248 Queen's Road East, Wanchai, Hong Kong.
Website:	www.pcpd.org.hk
Email:	enquiry@pcpd.org.hk

Disclaimer

The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.