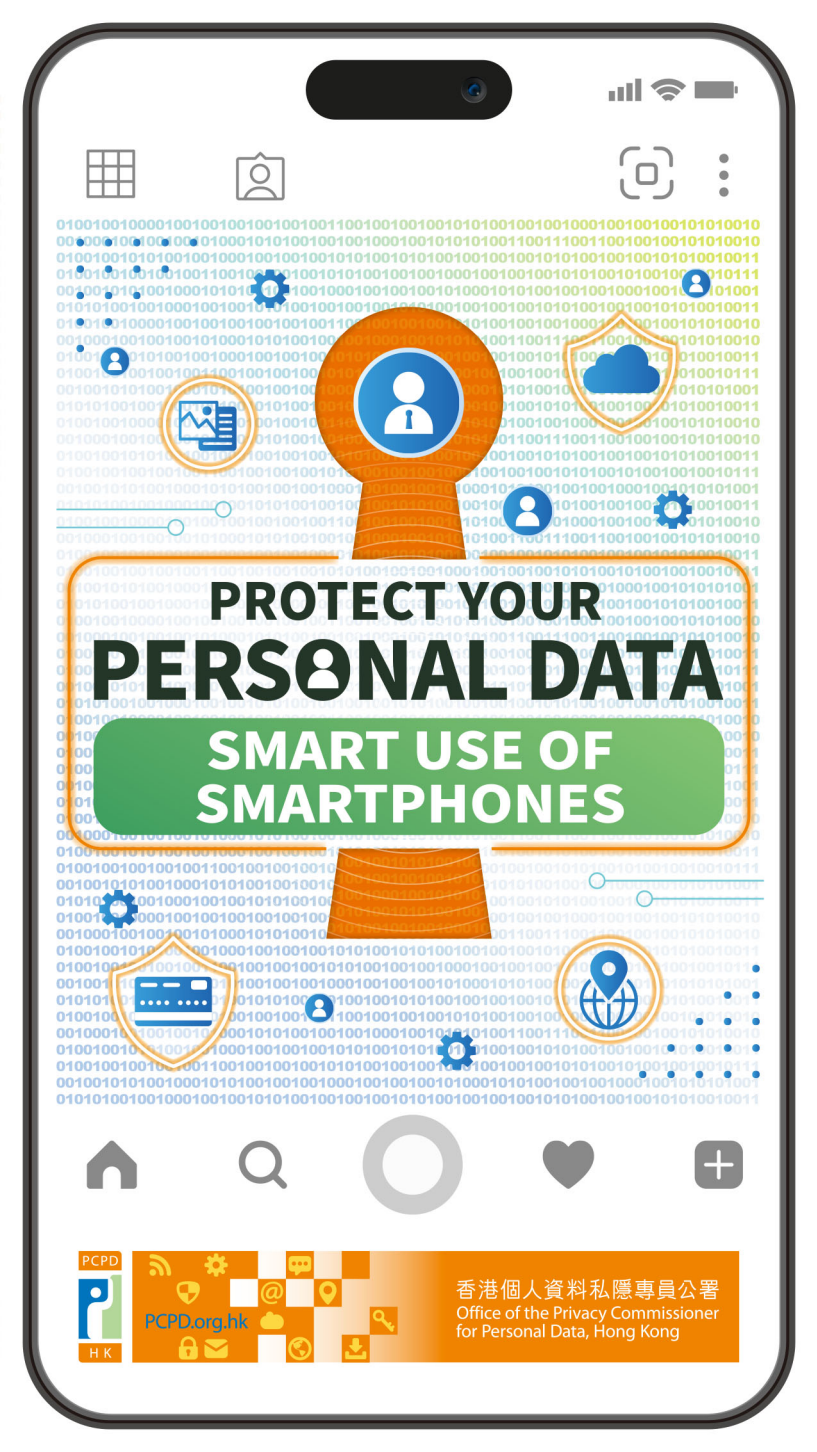
PROTECT YOUR
PERSONAL DATA
SMART USE OF SMARTPHONES
PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

We are now spending more time with our smartphones and tablets (collectively referred to as "smartphones" in this leaflet). While smartphones make our lives easier and bring us fun, they also carry risks to personal data privacy which we cannot ignore. For example, your smartphone may store large amounts of sensitive data, such as text messages, photos, contact list and places where you have visited. The apps installed on your smartphone may collect a lot of information about you as well. This leaflet provides smartphone users with practical advice to protect their personal data privacy while using smartphones.

Securing Your Smartphone

Never "jailbreak" or "root" your smartphone

Do not remove security restrictions imposed by the manufacturers of your smartphone (commonly known as "jailbreaking" or "rooting") as this would make your smartphone vulnerable to malware.

Install anti-malware software

Ensure the anti-malware software runs properly and is up-to-date. Beware of free software as the files may contain malware.

Enable screen lock by passwords and/or biometrics

Using strong and unique passwords can help prevent unauthorised access to the content of your smartphone. Remember to change your passwords regularly and you may use biometrics (e.g. fingerprints or facial recognition) to unlock the screen.

Install the latest system updates

Keep an eye on updates to the operating systems and install them promptly to ensure that your smartphone is secured against the latest security threats.

Turn off wireless communications when not in use

Only switch on Wi-Fi, Bluetooth and Near-Field Communication (NFC) when they are needed to prevent unauthorised tracking of or connection to your smartphone.

Avoid using public chargers

Malware can be transmitted to smartphones through shared chargers or power banks provided in public places. If necessary, use a charge-only USB cable which cannot transfer data.

Turn on the "find my device" function

This allows you to remotely locate and lock your smartphone, or erase data stored inside the smartphone in case it is lost or stolen.

Erase data before repair or disposal of smartphone

Use the factory reset function to erase all data before disposing of your smartphones or sending them for repair to prevent data leakage.

Securing the Data Stored on Your Smartphones

Beware of public Wi-Fi

Connecting to unreliable Wi-Fi networks exposes your smartphone and personal data to the risk of unauthorised access. Instead, use your mobile data for sensitive activities, such as online banking.

Perform regular backup of your data

This can alleviate any potential impact caused by loss of smartphone or ransomware. Encrypt the backup files with strong and unique passwords if they contain sensitive data.

Minimising the Risks of Using Apps

Review privacy policies of the apps before download

Understand how the apps collect and use your personal data. Study also the permissions requested by the apps and other users' comments on the apps. If possible, choose the apps which request the least amount of essential permissions.

Protect the accounts of your apps

Set strong and unique passwords for each account, and change your passwords regularly. To further enhance security, enable multi-factor authentication (such as one-time passwords received through SMS or email) and install updates for the apps when available.

Download apps only from official app stores

Disallow installation of apps which are not downloaded from official app stores as these apps may contain malware.

Adjust the permissions and privacy settings of your apps

Allow apps to access only minimum, necessary data. In particular, do not allow apps to access sensitive information such as your location, phone book and calendar unless it is necessary.

Remove unnecessary apps

Review apps installed on your smartphones from time to time and delete those that you no longer use or are reported to contain security vulnerabilities in order to stop them from accessing or sharing your data.

Tel : **2827 2827**

Fax : **2877 7026**

Address : **Unit 1303, 13/F., Dah Sing Financial Centre,
248 Queen's Road East, Wanchai, Hong Kong**

E-mail : **communications@pcpd.org.hk**

PCPD Website:
pcpd.org.hk

Download this
Publication

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

March 2024 (Second Revision)