Protect Your Personal Data
Be Smart on Social Media

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

Many of us use social media (including instant messaging apps) every day. The use of social media carries inherent risks to users' privacy in relation to personal data as users may over-share their information, which may ultimately fall into the wrong hands. Platform operators may also use or share users' information for gain.

Furthermore, online scams have been increasingly common on social media. The following advice helps you stay safe when using social media.

1 Signing up for a new social media account

Read the privacy policy

Find out how your personal data will be handled and shared by the social media platform.

Minimise the provision of personal data

Only minimum and necessary personal data should be provided for registration. Sensitive personal data such as residential address and full date of birth should not be handed over lightly.

Use a dedicated email account for registration

If an email address is required, set up a dedicated email account solely for the use of the social media account.

Set strong passwords

Set strong and unique passwords and change the passwords regularly. Enable multi-factor authentication to enhance security.

2 Adjusting privacy settings

Limit public access to your information

Publicly accessible information can be collected and aggregated by third parties using automated techniques such as "data scraping". In particular, do not allow everyone to have access to your contact details and your residential address.

Beware of "tag"

Do not allow other users to "tag" or "mention" you in their photos or posts without your permission, or select the setting that enables you to be alerted when you are tagged.

Think twice before granting any permission

Unless necessary, avoid granting permissions to social media platforms for using facial recognition, location tracking and cross-platform online tracking, or allowing third-party apps to access your profile.

Review privacy policies and settings regularly

Privacy policies and settings may be changed by the platforms from time to time. Examine the changes carefully to see if you agree with them. Readjust the privacy settings when necessary.

3 Posting information on social media

Beware! Information can be widely shared without your knowledge

Information shared with "friends" can still be forwarded to or shared widely with unknown third parties.

Do not tag people in photos lightly

Tagging people in photos may reveal their information to the public against their will. It may also enable social media platforms to enroll their images for facial recognition.

Minimise your digital footprints

Think twice before sharing anything on social media. An innocuous picture may tell a thousand words. There is no simple "delete" button once your personal data is disclosed online.

Review social media posts from time to time

Review your social media posts to identify and delete anything which you no longer want to share.

Report improper contents

If your information is shared maliciously on social media, report the contents to the platform, or the Office of the Privacy Commissioner for Personal Data via the general enquiries hotline (Tel: 2827 2827) or the doxxing hotline (Tel: 3423 6666) or email (complaints@pcpd.org.hk).

4 Staying vigilant on social media platforms

Be cautious about third-party apps

Third-party apps (such as add-on games) on social media platforms may have different privacy settings, including accessing your profile, and transferring your data to other parties. Check them out before installing such apps.

Other users may not be real people

Refrain from connecting with people whom you do not know in real life. The names or descriptions of other social media users may be fictitious.

Terminate unused accounts

This minimises the risks of cyberattacks and misuse of your personal data.

Stay vigilant against online scams

Beware of online scams that come in the form of unsolicited benefits, prizes, charities or hyperlinks that request you to "log-in" or provide personal data. Verify the contents of suspicious messages, such as by making telephone calls to the senders directly.

Look out for data breaches and failed log-in attempts

Once you are aware of a data breach affecting your social media platform or failed attempts to log into your accounts by strangers, change your password immediately and check for irregularities in your account.

PCPD Website:
pcpd.org.hk

Download this
Publication

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

Tel : 2827 2827
Fax : 2877 7026
E-mail : communications@pcpd.org.hk
Website : www.pcpd.org.hk

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 (Fourth Revision)