“Build a Secure Cyberspace 2023 – Protect Your Online Identity” Seminar

22 September 2023

Protect Online Identity to Safeguard Personal Privacy

Mr Brad KWOK
Chief Personal Data Officer (Acting)
(Compliance & Enquiries Division)

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

Statistics of Online Activities

Users of online shopping platforms in Hong Kong covered 76.7% of the population in 2022 and is forecasted to reach 83.8% by 2025. (Source: *Osome*)

6.73 million people in Hong Kong were active on social media. (Source: *Digital 2023 Global Overview Report*)

80% of children living in developed Western countries have a digital footprint before they are two years old. (Source: *Report on Artificial Intelligence and Privacy, and Children's Privacy*)

Risks to Personal Data Privacy relating to Online Activities

Loss of Privacy

Misuse of Personal Data

Fake Accounts and Identities

Nothing is private in the online world

Free Service having a Price Tag

Protecting Your Online Identity

1 • **Online Shopping Platforms**

2 • **Social Media Platforms**

3 • **Against Cyber-bullying/Doxxing**

4 • **Against Personal Data Fraud**

5 • **Avoid "Sharenting"**

Protecting Your Online Identity - Online Shopping Platforms

The PCPD published a report on "*Privacy Protection in the Digital Age: A Comparison of the Privacy Settings of 10 Online Shopping Platforms*" and Leaflet on "*Tips for Users of Online Shopping Platforms*" in June 2023.

- *Baby Kingdom - Bkmall*
- *Carousell*
- *eBay*
- *Fortress*
- *HKTVmall*
- *JD.COM*
- *PlayStation App*
- *Price.com.hk*
- *Samsung*
- *Taobao*

Protecting Your Online Identity - Online Shopping Platforms

Review results (non-exhaustive)

Privacy Policy Statement

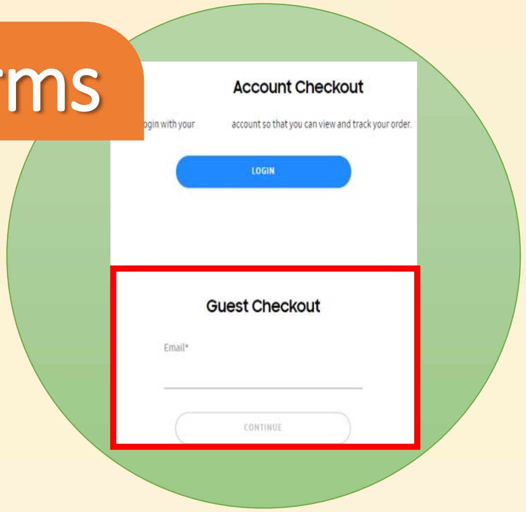
Your Privacy

We respect your legal rights of privacy when collecting, using, processing and transmitting personal data. We are legally required to comply with the requirements of the Personal Data (Privacy) Ordinance.

- All online shopping platforms reviewed:
  - have formulated privacy policies;
  - track users' activities;
  - state in their privacy policies that they transfer personal data of users to third parties;
  - allow users to delete their user accounts.

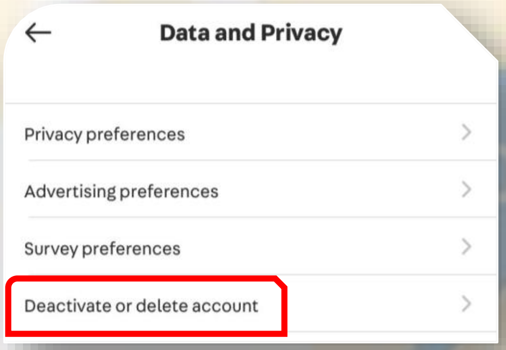
- Most online shopping platforms reviewed accept payment through third-party payment platforms.

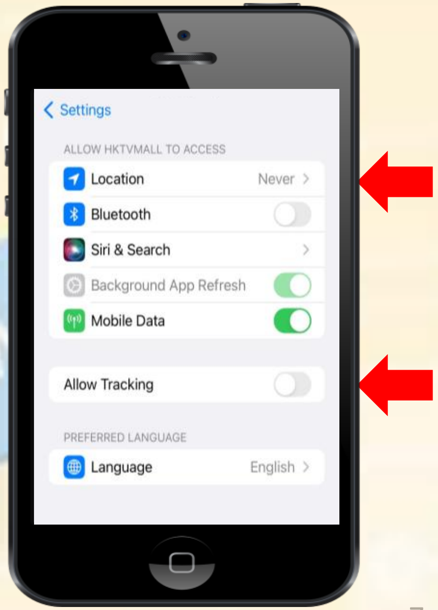
Protecting Your Online Identity - Online Shopping Platforms



Protecting Personal Data Privacy

1. Provide the minimum amount of personal data
2. Pay attention to direct marketing settings
3. Consider using third-party payment platforms
4. Read the privacy policy
5. Adjust privacy settings
6. Delete unused accounts





Protecting Your Online Identity - Online Shopping Platforms

Safe Online Shopping

7 Verify the authenticity of the platform

8 Use the platform securely

9 “Stop and think” before clicking

10 Regularly check online shopping accounts and report problems

Protecting Your Online Identity - Social Media Platforms

The PCPD released a report on "*Comparison of Privacy Settings of Social Media*" in April 2022 after a review of the top ten most commonly used social media platforms, including:-

- *Facebook*
- *Facebook Messenger*
- *Instagram*
- *LINE*
- *LinkedIn*
- *Skype*
- *Twitter*
- *WeChat*
- *WhatsApp*
- *YouTube*

Protecting Your Online Identity - Social Media Platforms

Review results (non-exhaustive)

- All the social media reviewed:
  - have privacy policy in place;
  - collect users' location data;
  - state in their privacy policies that users' personal data would be transferred to their affiliated companies.
- In terms of the default privacy settings, the age and telephone number of a user are not disclosed by Skype and YouTube, while the other social media reviewed disclose users' personal data such as location, email address or telephone number by default.

Protecting Your Online Identity - Social Media Platforms

Review results (non-exhaustive)

- Apart from WeChat, all other instant messaging applications reviewed deploy end-to-end encryption in the transmission of messages between users.
- Except for LINE, all other social media reviewed provide two-factor authentication.
- Most of the social media reviewed would retain users' credit card data.
- Facebook, LINE, WeChat and YouTube all allow users to disseminate posts to specific individuals or groups and modify the privacy settings of the contents after posting.

Protecting Your Online Identity - Social Media Platforms

Before registering an account

- ✓ Read the Privacy Policy of the social media carefully
- ✓ Open an email account dedicated for social media
- ✓ Only provide the required personal data

When using social media platforms

- ✓ Check the default settings and the ways through which individual users may be searched on the social media
- ✓ Consider turning off the location tracking function if you do not need the function
- ✓ Select the appropriate settings before posting the contents on social media

Protecting Your Online Identity - Social Media Platforms

Pay attention to whether the instant messaging application provides end-to-end encryption forms of transmission

Use strong passwords and enable two-factor authentication for social media

Avoid transactions on social media platforms over public Wi-Fi or unsecured Wi-Fi connections

Parents/ guardians may consider enabling parental controls

Protecting Your Online Identity against Cyber-bullying/ Doxxing

Cyber-bullying

- The infliction of harm on victims wilfully and repeatedly using online communication platforms such as email, discussion forums, online gaming network, messaging or social media platforms
- Victims may experience psychological, emotional and even physical harm

Doxxing

- The gathering of the personal data of target person(s) and disclosure of the personal data on the Internet, social media or other open platforms (such as public places) without the data subjects' consent and with intent to cause specified harm or being reckless as to whether specified harm would be caused

Protecting Your Online Identity against Cyber-bullying/ Doxxing

Cyber-bullying

A grumpy customer posted a video to rally netizens' opposition against a shop for its poor customer service. She expressed her anger at the shop with nasty words.

Netizens found her actions unreasonable and she became the target of attack.

Her photo, home and office addresses were published on the Internet. A social network group was set up calling for her apology.

Protecting Your Online Identity against Cyber-bullying/ Doxxing

Doxxing Offences (non-exhaustive)

Dec 2022	The defendant disclosed on four social media platforms the personal data of his ex-girlfriend without her consent. The defendant also impersonated the victim to open accounts on three of the said platforms and stated in the relevant messages that the victim welcomed others to visit her at her residential address. The court convicted the defendant of seven charges of the doxxing offence under section 64(3A) of the PDPO upon his guilty plea and sentenced the defendant to **eight months' imprisonment**.
Jun 2023	The defendant and the victim were former co-workers in a school. When their relationship turned sour owing to work grudges, the defendant displayed posters near the school on two occasions, disclosing copies of the victim's Hong Kong Identity Card with some negative remarks against the victim. The court convicted the defendant of two charges of the doxxing offence under section 64(3A) of the PDPO upon her guilty plea and sentenced the defendant to **160 hours' community service**.

NOTE

As of end of June 2023, the PCPD handled more than **8,600** doxxing cases

Protecting Your Online Identity against Cyber-bullying/ Doxxing

DON'Ts

- Disclose unnecessary personal or private information online ✗
- Post online any information that you would not share publicly offline ✗
- Join a heated online discussion or post overemotional comments and messages ✗
- Disseminate or share offensive, rude, insulting or doxxing messages, photographs or videos ✗
- Participate in cyber-bullying activities (e.g. doxxing) or encourage cyber-bullying ✗

DOs

- ✓ Properly configure privacy settings of online communication platforms
- ✓ Keep abreast of the latest guidelines and regulations on cyber-bullying-related topics

Enquiry/Complaint Hotline About Doxxing
☎ 3423 6666

Protecting Your Online Identity against Personal Data Fraud

8 Tips Against Personal Data Fraud

On Receipt of Suspicious Calls, Emails or SMS Messages

1. Beware of calls with "+852" prefix
2. Verify authenticity
3. Be vigilant
4. Be careful with links

Protecting Your Online Identity against Personal Data Fraud

8 Tips Against Personal Data Fraud

Use of Online Personal Accounts

5. Keep an eye on your accounts
6. Password protection

Keeping Abreast of the Latest News

7. Pay attention to
   fraud prevention information
8. Reminding friends and relatives

Protecting Your Online Identity against Personal Data Fraud

Privacy Commissioner Calls for Greater Vigilance
Beware of Phishing Emails or Messages Issued by
Bogus Government Departments or Banks

Relevant Examples

- Impersonating an officer of government department(s)
- Impersonating a law enforcement officer of Mainland
- Impersonating an employee of a courier company

Protecting Your Online Identity – Avoiding "Sharenting"

A portmanteau of "sharing" and "parenting"

Over-sharing children's daily lives online may encompass long-term consequences

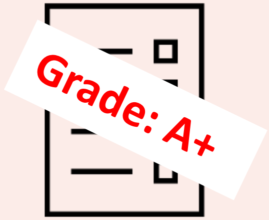
Might affect children's future education or work prospects

Protecting Your Online Identity – Avoiding “Sharenting”

Relevant Examples

- Parents opened fan pages for their children on social media platforms and share their daily lives.

- Parents uploaded transcript of their children online which contained personal data of other students.



- A court in the Netherlands ordered a grandma must delete the photographs of her grandchildren that she posted on social media platforms without their parents' permission.

Protecting Your Online Identity – Avoiding “Sharenting”

DOs

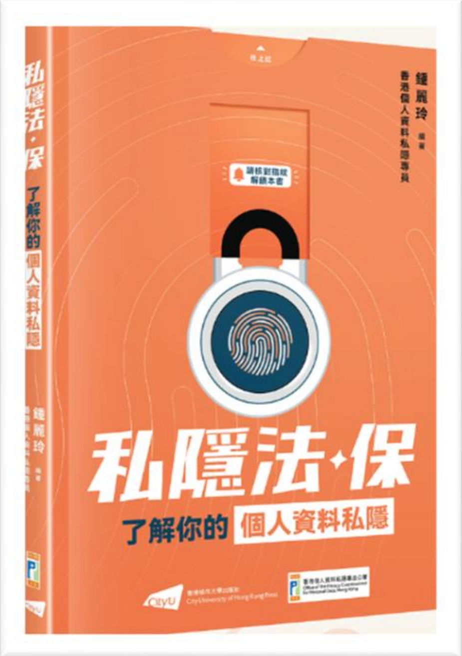
- Beware of the details of disclosure ✓
- Communicate – Seek agreement ✓
- Double check your privacy settings ✓
- Think about the future ✓

DON’Ts

- ✗ Overlook your children’s privacy
- ✗ Live for the “likes”
- ✗ Overshare
- ✗ Post photos of other children without permission from their parents

Resources

- "The Treasure-trove of Privacy – Understanding Your Personal Data Privacy"
- Be Smart Online
- Doxxing Offences
- Anti-fraud Tips
- Children Privacy
- "Information Security Guide - Stop Cyber-bullying"
- "Children Online Privacy - Practical Tips for Parents and Teachers"



Thank you!

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

2827 2827

2877 7026

www.pcpd.org.hk

communications@pcpd.org.hk

Rm 1303, 13/F, Dah Sing Financial Ctr., 248 Queen's Road East, Wanchai

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

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

About PCPD | Data Privacy Law | News & Events | Enforcement Reports | Frequently Asked Questions | Compliance & Enforcement | Doxxing Offences | Anti-fraud Tips NEW! | Complaints | Education & Training | Resources Centre | Contact Us

A Quick Guide | Hot Search | Advanced Search | Keyword Search

Follow

RSS A A A 繁 簡

Data Scraping on Social Media Raises Concerns
Twelve Privacy Protection Authorities
Promulgate Global Privacy Protection Expectations and Principles
to Social Media Platforms

What's New

More

- Reaching Out to the Community – Legal Counsel of the PCPD Interviewed by RTHK Radio 3's "Backchat" to Explain the Pamphlet on "Sharenting Dos and Don'ts"
- Data Scraping on Social Media Raises Concerns The PCPD, together with Other Privacy Protection Authorities, Promulgates Global Privacy Protection Expectations and Principles to Social Media Platforms
- Enhancing Awareness to Prevent Fraud – Privacy Commissioner's Office Launches the Second Episode of Anti-fraud Promotional Video
- Reaching Out to the Community – Representatives of the PCPD Interviewed by the Media
- A 28-year-old Chinese Female Arrested for Suspected Doxxing Offence Relating to Emotional Entanglements
- Reaching Out to the Community – Privacy Commissioner