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

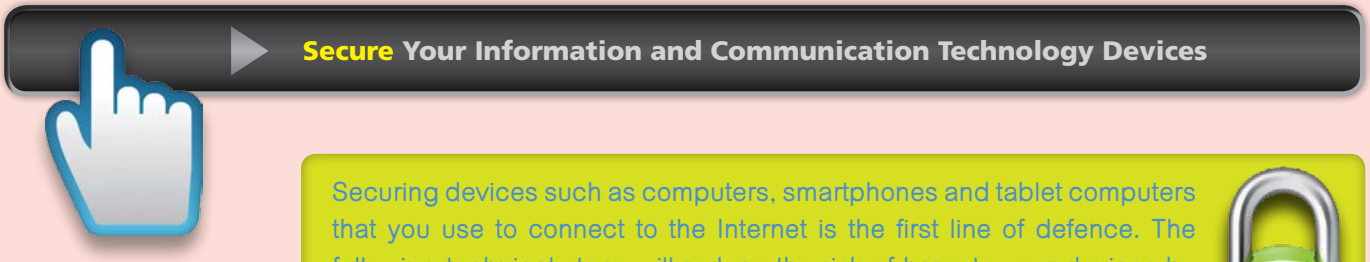
Protecting Privacy - Using Computers and the Internet Wisely

Checklist

You should pay attention to the following items before using the computer or surfing the Internet:

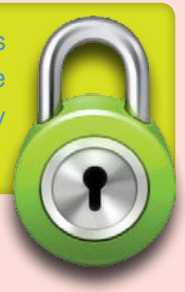
Protecting Privacy - Using Computers and the Internet Wisely

This information booklet aims to provide practical tips and advice on how individuals can protect their personal data when using information and communication technologies.



Secure Your Information and Communication Technology Devices

Securing devices such as computers, smartphones and tablet computers that you use to connect to the Internet is the first line of defence. The following technical steps will reduce the risk of harm to your devices by malicious software.



Install proper anti-virus software

- Malware is a collective term for viruses, worms, trojans[1], keyloggers[2], zombies[3], etc. that can harm your computer and / or steal your data. Install the most up-to-date anti-virus packages, either paid or free, and make sure the signature files are regularly updated according to the software vendor's recommendation.
- Anti-virus packages are also available for smartphones and tablet computers. As these devices have become popular devices for connecting to the Internet and can hold as much personal data as a computer, protecting them with anti-virus software is crucial.
- If available, you should switch on the personal firewall feature of your operating system or anti-virus package. A personal firewall controls network traffic to and from your device and reduces the risk of your devices being hacked or attacked.

1. *Trojans are software that are advertised to do one thing, but secretly also do other tasks, such as acting as a keylogger, file-sharer and / or zombie.*
2. *Keyloggers are software that capture your keystrokes, including website addresses, usernames and passwords, and send them to a hacker without your knowledge.*
3. *Zombies are software that take over control of your computer so that it can be used remotely by hackers to send spam, attack websites, etc. without your knowledge.*

Log on as a user and not an administrator

- Anti-virus software is not a fool-proof guard against all types of malware. Another effective measure that can protect your computer is to use only the 'user mode' account for everyday use. If you use a computer with administrator rights, any malware that makes its way to your computer can install itself through your account that has administrator rights. Always create a 'user mode' account (which cannot install software) for yourself and for other users of your computer in order to guard against malware. In addition, a lot of information, such as the history of websites visited, web pages read, usernames and passwords used, are stored with each account name. If you do not wish such information to be read by others, create different user accounts to ensure the information is kept to the relevant user.

Apply security updates

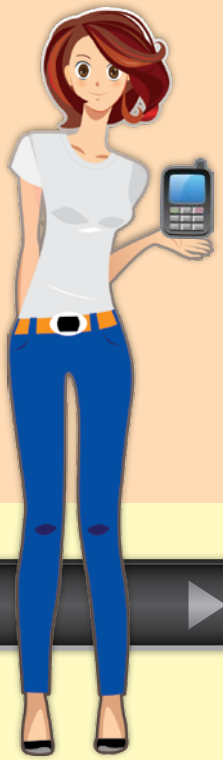
- Always apply security or version updates for the operating systems of your devices. A lot of malware takes advantage of vulnerabilities in operating systems. Updating your operating systems is a good step to reduce risks resulting from such vulnerability.

Do not install pirated software

- Nearly all pirated software and their hosting websites contain malware. As you have to log in as administrator when installing such pirated software, malware can install itself as part of the pirated software. Not all types of malware can be detected by anti-virus software. Therefore, it is extremely risky to visit piracy websites, download pirated software, music or videos, and / or install them.
- Remember there is no free lunch when it comes to downloading commercial software, music or videos for free. If the deal is too good to be true, then it probably is not true.

Protect Your Information and Communication Technology Devices

Physically protect your devices to prevent others from accessing any stored personal data if the devices are lost or out of your sight.



Lock your device when it is not in use

- For smartphones and tablet computers, always enable a password-protected screen lock so that others cannot use them without your permission.
- For computers, apart from setting a log-on password, you should also enable a password-protected screensaver so that they cannot be accessed without your permission.

Install anti-theft software

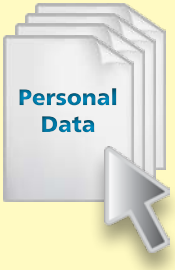
- Consider installing anti-theft software that may allow you to track the location of your device if it is lost or stolen. Some of them allow you to write a message on the screen to alert the person who has picked up the device, or allow you to remotely erase all the data stored in the device.

Think Twice Before Providing Personal Data Online

It is difficult to ascertain the identities of those who request your personal data over the Internet. Be a wise Internet user and question why websites are collecting certain types of personal data from you. Beware of fake email messages and websites.

Since it is virtually impossible to stop information released on the Internet from circulation, think carefully about the possible consequences before providing or disclosing personal data over the Internet.

Know who you are supplying personal data to and why



- Think twice before agreeing to supply your personal data to any party who requests them. Ask yourself if they have genuine reasons to ask the type of personal data from you.
- Think twice before supplying personal data of your friends or relatives in exchange for privileges. Ask yourself how you would expect your friends or relatives to guard and respect your personal data.
- Before you provide your personal data to a website or via email, ask yourself if you really know to whom you are providing the information. Legitimate websites can easily be copied, and fake websites are made to look professional and authentic.

Think about the implications of disclosing your personal data

- Think twice before posting any personal data on social networking sites. Once disclosed, there is no way to stop such information from being circulated or searched on the Internet. Read the leaflet "Protecting Online Privacy – Be Smart on Social Networks" [4] issued by the Office of the Privacy Commissioner for Personal Data (the Commissioner) for more details.
- You may disclose innocent information such as your pet's names on one site and use it as the answer to the question for password recovery on another site. Think twice before disclosing such information or choosing the right questions for password recovery.

Are you requested to provide excessive data?

- Learn to question whether personal data requested over the Internet by websites or other data users is excessive for the purpose of collection. For example, why do you need to provide your full date of birth if a website only wants to confirm that you are old enough to use it? If you are not purchasing goods, why should a website ask for your credit card number and / or residential address in advance?
- Do not be too ready to provide personal data in exchange for privileges. Consider what the other party may want to use the personal data for. For example, he or she may use it for profiling purposes or even fraudulent activities.

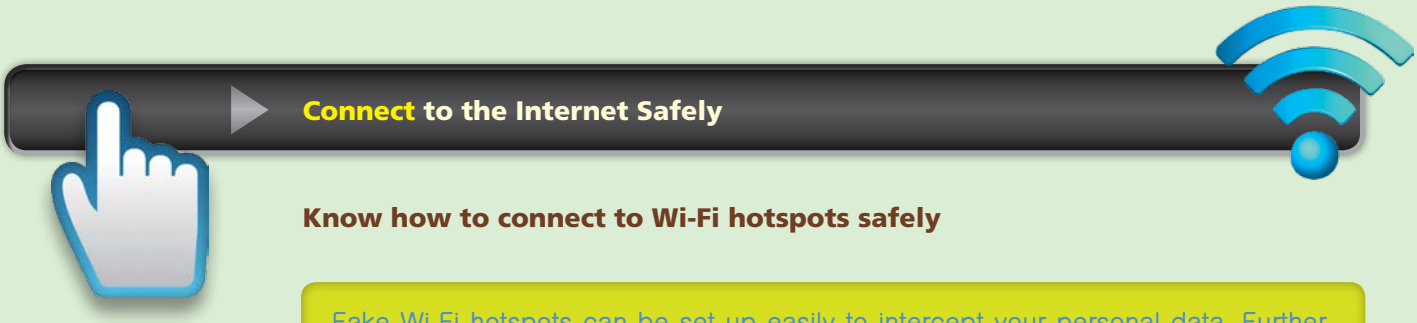
4. *See http://www.pcpd.org.hk/english/publications/files/SN_e.pdf*

Read the Personal Information Collection Statement ("PICS") and Privacy Policy Statement ("PPS") before providing personal data

- The PICS explains whether it is obligatory for you to supply your personal data, the purpose of collecting the data, the class of transferees of the data, and whom you can contact to get access to, and correction of, your personal data.
- The PPS explains the privacy policy and practices of an organisation. It normally covers topics beyond data collection, including how the organisation would handle, use and retain the personal data it holds.

Do not trust unexpected email messages

- Email messages can be fake and senders can be impersonated. Think twice before acting solely on email requests. Do not click on any link in unexpected email messages that ask you to log on to services such as online e-banking / payments, email, social networks, etc. Instead, use your own bookmarked links to access those sites. If the message is genuine, you should see the same request after using your own bookmarks to log on to those services.
- Similarly, do not open any attachment in email messages that you are not expecting.



Connect to the Internet Safely

Know how to connect to Wi-Fi hotspots safely

Fake Wi-Fi hotspots can be set up easily to intercept your personal data. Further, unencrypted Wi-Fi connection allows others in the same Wi-Fi network to listen to your communication. Adopting the following Wi-Fi related measures will reduce such risks.

- Always make sure you are not logged in as administrator for your computer when you access the Internet via public Wi-Fi, in order to reduce the risk of malware exploitation.
- Whether you are using public Wi-Fi or your own, always make sure that you are using SSL encryption (see below) when you use Wi-Fi to access websites with sensitive information (e-banking, webmail, social networks, on-line shopping, etc.) in order to avoid interception of your information.
- When setting up your own Wi-Fi, always enable WPA or WPA2 encryption to protect your data. When accessing public Wi-Fi, such as Government Wi-Fi, always connect to WPA or WPA2 encrypted access points if available.

Know what not to use public computers for

As there is no guarantee that public computers have not been tampered with, they should not be used to communicate sensitive or personal data.

- Do not use public computers to access websites with sensitive information (e-banking, webmail, social networks, on-line shopping, etc.) because you do not know if these computers have malware such as keylogger installed. Use of public computers with unknown security level will increase the risk of exposing your personal data to unknown parties.

Do not allow devices to remember your login details

The "remember me" box stores your username and password to the browser so that you do not have to log on again in the future. Though convenient, it enables anyone who has access to the computer to operate your account.

- Do not tick the "remember me" option for websites if you are not using your own computer to access them.

Use SSL to protect online information

SSL is an encryption technology used in accessing websites. If you use https:// instead of http:// at the beginning of the web address to visit a website, then the communication is protected by SSL encryption to prevent eavesdropping. This is very important if you are using Wi-Fi to connect to the Internet, as many Wi-Fi hotspots have not enabled built-in encryption.

- Always make sure https:// appears at the beginning of the web address before you provide any sensitive personal information (such as credit card numbers) over the Internet to trusted websites. When you are accessing a website through https://, the identity of the website is also checked by the browser. You can learn from the browser's Help menu how to read and confirm the identity of the website through a padlock / key icon displayed on screen.

- You can enable automatic https:// access for many popular email and social networking sites. Make good use of this facility whenever possible. Check the respective sites on how to enable this function. Once enabled, communications via mobile applications (apps) of these services will also be protected by encryption.

Know your website cookies

A cookie is a file stored in your computer by the website you have visited. It may contain your online behaviour such as your preferences, shopping cart choices, and/or your browsing history. There are many types of cookies. Some are necessary for accessing websites while some are just used to track your web behaviour. You need to know the basics of cookies and which type to accept and which type to reject.

- There are different types of cookies. Session cookies are required for many websites that require a log-in, so that you do not have to enter your username and password for every page you intend to visit. Session cookies are deleted by your browser as soon as you close it. You should consider allowing session cookies; otherwise, you will be denied access by many websites that require you to log in.

- Another type of cookies is called persistent cookies, which remain on your computer even after you have closed the browser. First-party persistent cookies contain your viewing preferences or browsing activities related to the website you have visited. You may choose to accept or deny them, but denying them may disable your access to certain websites or parts of them. The website should tell you whether you can still use it if you disable the cookies.

- Third-party persistent cookies are often placed by online advertising companies who have purchased "space" on the websites you are visiting. If you do not wish to be tracked by a third party, you should deny third-party cookies. This should not affect your browsing experience. You should check your browser on how to configure it to block third-party cookies.

- Some websites deploy techniques such as Flash cookies, which ignore the browser settings and remain on your computer. If you have the latest version of Acrobat Flash installed, you can deny Flash cookies by configuring the Flash Player in the Control Panel. Techniques to create such "super / zombie cookies" (cookies that ignore user settings and are difficult to remove) are evolving all the time. If you are concerned about your web behaviour being tracked, you should study this topic regularly on the Internet to understand the latest developments.

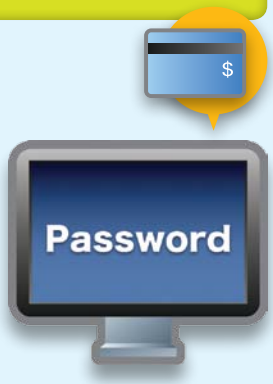
- Many browsers offer a "privacy / safe-browsing mode" which should enable you to leave no trace after you close the browser (that is, there is no retention of any browsing, form-filling, download history, cached files and stored password, etc.) and cookies are disabled. The level of privacy protection, however, varies from browser to browser. You should familiarise yourself with the level of protection before relying on their protection. Using the privacy mode may slow down your browsing experience, as the browser does not remember any pages you have visited or your viewing preference.

Handle Account and Password Safely

Know how to protect your account and password information

Use of the same account name and password for multiple services means others can access all your accounts once they know your password (through leakage or by guessing). Many sites , however, allow logging in using the registered email address. Even if you use the same email address to register for different account names in multiple sites, hackers who know the password can still gain unauthorised access to your other accounts using the registered email address / password combination.

Similarly, others can link your online identities together and collate information about you if you use the same email address or the same account name for multiple website registration.



- Develop a method to change passwords regularly yet ensuring you remember them without having to write them down. Do not use the same password for all accounts, particularly for those that contain sensitive personal data.
- Do not open online accounts with the same name and do not use the same email address for multiple account registrations.
- Use complex passwords that are at least eight characters long, with a mixture of numbers and letters, or follow the password policy as suggested by the website.
- Do not reveal or provide your password to anyone including those who claim to represent the websites. If you think your password is leaked, change the password in all the accounts using the same password immediately to protect yourself.

Handle Portable Storage Devices ("PSDs") Properly

Know how to use portable storage devices

PSDs are USB drives, tablet computers, smartphones, or any other device that has storage capacity. Always think about the consequence of losing your PSDs (which is not uncommon).

- As PSDs can easily be lost, always keep a backup copy of the data stored in them.
- Always encrypt files stored in PSDs (see below on file encryption) so that information stored in it cannot be read or understood by those without the password.

Understand the Use of Foxy

Know the pitfalls of using Foxy

The use of Foxy is fraught with danger as many versions of this software automatically run and share the files of your entire hard disk by default. Once a file is shared via Foxy, there is virtually no way of stopping it from spreading.

- Too many incidents of data leakage have occurred with Foxy, with the users having no idea that Foxy was sharing their sensitive data. You should ask yourself if you really know how Foxy works and how to configure it before using it.
- As the vendor that produced Foxy is no longer in business, there is no more reliable source from which to download Foxy. You should therefore ask yourself how you can be sure that the copy of Foxy you have downloaded has not been tampered with and is not infected with malware.

Know How Encryption Can Help

Understand how encryption can help to protect information

Encryption is an effective way to prevent data from being understood when your computer is hacked or when your PSDs are lost. Remember to safeguard the encryption password and do not store it in the computer or PSDs, and do not record it in a manner which makes association with the equipment apparent.

- There are many methods and software programmes you can use, both paid or free, to encrypt files stored in your computers and PSDs, including smart phones. You should familiarise yourselves with at least one way of encrypting files. For example:

  - You can use TrueCrypt (www.truecrypt.org), a free, open-source and multi-platform software, to create a "container" in your hard drive or USB drive, and everything stored in it will be encrypted.
  - For the encryption of individual files, you can install 7-Zip (www.7-zip.org), another free, open-source and multi-platform software program that compresses files and folders, and supports encryption.

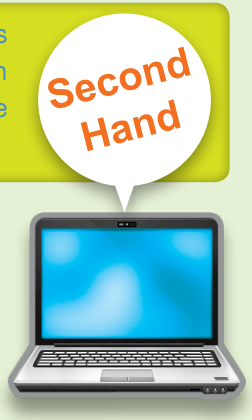
- You need to use a strong encryption algorithm such as "AES". Make sure you have chosen this algorithm when creating the "container" in TrueCrypt or encrypting a file in 7-Zip.

- If you need to send personal data by email, you should store the personal data in a file and encrypt it before sending it. In addition to securing the personal data during transmission, encryption protects the data from possible data leakage at the recipient end (for example, if the receiving computer is hacked or inadvertently shares the file via Foxy or other file sharing software). You should not send the encryption password by email. Sending it by other means will prevent both the file and password from falling into the wrong hands (e.g. as a result of a typo in the recipient email address).

Arrange Equipment for Repair / Sale / Disposal Safely

Understand what precautions to take before handing over equipment

Many people may not realise how much personal data they have stored in their computers or PSDs. As you may not be able to remove the data storage device or erase the data in such equipment, disposing, selling or sending the equipment to a third party without due precautionary measures means you may be giving your personal data away.



- You should ensure that you choose a reputable repair provider. You should also check that you are happy with their pledge on the protection of personal data before entrusting them with the data.
- If the problem is not related to the removable storage device in your equipment, you should remove it before sending it for repair. If you must send the storage device away for repair, try to erase all personal data whenever possible using a secure, permanent method (such as DBAN from www.dban.org for drives or FileShredder from www.fileshredder.org).
- Similarly, if you are selling or disposing any device that has memory or storage, remember to erase all the data stored in it. Some device manufacturers (such as those of mobile phones) provide steps for users to erase all stored data on their phones. These steps should be followed. Also remember to remove the removable memory cards or old SIM cards installed in these devices, or to erase the data.

Protect Your Children

Teach your children to protect their personal data

Children may be less aware of the privacy concerns and pitfalls of using the Internet and information technology. They should be educated early in their lives to protect themselves.

- Discuss with your children how the advice in this booklet can help them protect their personal data when using the Internet. Teach them that once their personal data is leaked or openly shared on the Internet, it may be there for the rest of their lives.

Use Your Smartphones and Tablets Safely

To learn how to protect yourself in the use of smartphones or tablets, please read the leaflet "Protect Privacy by Smart Use of Smartphones"[5]. The leaflet provides guidance on how to protect mobile devices and data stored in the devices, and how to use mobile applications safely.

5. *http://www.pcpd.org.hk/english/publications/files/smartphones_smart_e.pdf.*

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

Think Privacy! BeSmartOnline

www.pcpd.org.hk/besmartonline

Copyrights

Reproduction of all or any parts of this booklet is permitted on condition that it is for non-profit making purposes and that an acknowledgement of this work is duly made in the reproduction.

Disclaimer

The information provided in this booklet 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 the law, refer 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 power conferred to the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong

April 2014 (First Revision)