Internet Surfing with Privacy in Mind –
A Guide for Individual Net Users

CONTENTS

Introduction

The rapid development of the Internet has made an abundance of information easily accessible on-line to everyone who has a connection to it. As the Internet's information capacity increases, so too will the range of services and information available to the public. Undoubtedly, the Internet will enhance and eventually transform communication, education, commerce, the provision of government services, and virtually every other aspect of modern life.

However, accompanying these innovations are significant privacy issues. The issues relate to the risks associated with respect to the collection, use and security of personal data when one surfs the net for fun, information or to obtain goods or services. Of particular concern to individuals is the potential loss of their personal privacy if data about them are collected without their knowledge or are intercepted and misused for fraudulent or other purposes for which the individual does not intend the data to be used, e.g. profiling. This can occur when the individual provides personal details to gain access to an Internet service or when the individual communicates with someone else via Internet e-mails that contain sensitive information.

The Personal Data (Privacy) Ordinance ("the Ordinance") provides individuals with the following privacy rights with respect to organisations based in Hong Kong:

symbol 183 \f "Symbol" \s 12•} to have their personal data collected in a manner which is lawful and fair and to be informed of the purposes for which the data are to be used;

symbol 183 \f "Symbol" \s 12•} to consent to a change of use of the data;

symbol 183 \f "Symbol" \s 12•} to have their personal data kept accurate, up-to-date, secure and for no longer than necessary;

symbol 183 \f "Symbol" \s 12•} to obtain a copy of their personal data held by a data user and to require correction of any inaccuracy;

symbol 183 \f "Symbol" \s 12•} to ascertain a data user's personal data policy and practices.

The main purpose of this Guide is to raise awareness of individuals of the privacy risks in using the Internet and to assist them to protect their privacy by alerting them to the precautionary actions that can be taken.

Step 1 - Getting prepared to surf the Internet

Checklist

Is your Internet Service Provider ("ISP") privacy-aware?

Suggestions

=> Ask your ISP about its privacy policy and practices in handling personal data. The ISP you choose should be committed to protecting the privacy of your personal data and when asked, it is obliged to provide you with information on its privacy policy and practices. Satisfy yourself that your chosen ISP is privacy-aware before committing to using its services.

Checklist

Have you checked your ISP's policies on using "clicktrails"?

Suggestions

=> Ask your ISP about its use of "clicktrails" data collected about you. Your ISP can keep track of the Internet pages you have visited by looking at computer log files held in its server. These are “clicktrails” data about you and are normally used only for the purpose of system maintenance and troubleshooting. ISPs shall not use the data for other purposes, e.g. market research without your consent.

Checklist

Is your browser up-to-date?

Suggestions

=> Use an up-to-date, officially-released version of browser software. Security offered by browser software is generally improving, so you should always try to use a reasonably up-to-date version to obtain the most recent protection technology for your privacy and the security of your personal data.

Checklist

Is your password secure?

Suggestions

=> Choose a password that is hard to guess. Your password for access to the Internet and the e-mail system are the first line of defence for your privacy. Use a password that is nonsensical. Mixing numbers and special characters with letters is a good practice.

=> Change your password frequently. Ask your ISP to change the password set up when the account is first opened and change it from time to time.

=> Set your e-mail program not to remember your password. Forgery of e-mails is very easy if someone gets hold of your password. You can help avoid this risk by setting the e-mail program not to fill in your password automatically.

Checklist

Have you set your browser to ask you before accepting a "cookie"?

Suggestions

=> Set an option in your browser to ask your permission to accept a cookie, each time one is presented. Cookies are small files that can be stored in your computer when you visit a web page. They can save you having to register again when re-visiting the same site, but they can also be used to track your interests. If you have filled in an Internet form, your interests can be attached to your name. Then, a profile of your interests can be built which, after a while, may surprise you in its detail.

=> Use "anonymous cookies" software. You can search the Internet on the word "cookies" to find software that can keep your computer clear of cookies or make your cookies files ineffective for access. This would help to reduce your loss of privacy.

Checklist

Have you set your browser to tell you when a secure connection is active?

Suggestion

=> Set an option in your browser to display a message each time you enter and leave a secure zone. Special software programs called "sniffers" can monitor passing messages on the Internet. They can be made to recognise specific patterns of numbers, such as credit card numbers, which can then be noted and later misused. An alert message from the browser can help you to decide whether it is secure for you to send sensitive data over the Internet.

=> Check the browser window for the secure connection symbol. Most responsible sites requesting confidential information arrange for security encryption of such information automatically. If https:// instead of http:// is shown at the beginning of the Address line at the top of your browser window, or if you see an unbroken key or closed padlock symbol at the bottom of the browser screen, then messages sent to the site will be encoded. Encoded messages are much harder to spot. You should only send your credit card number and other sensitive data if they will be transmitted in encoded format.

Checklist

Are you asked to provide your personal data on-line?

Suggestions

=> If yes, do the following before you press the "Submit" button to provide your personal data via an on-line form or send an e-mail containing your personal data:

Checklist

Do you know the identity of the site requesting your personal data?

Suggestions

=> Look for identity details of the site. It is possible that a site appears to be at an electronic address that does not belong to it. Visit the "About the Organisation" page and check its identity details such as the name, physical location, and contact telephone/fax number.

=> Look for the site's privacy policy notice. It is also safer to know what the site's policy is in handling personal data before you provide them with your own. The Ordinance requires that organisations in Hong Kong should be open about their policy and practices in handling personal data.

Checklist

Are you told the purposes for which your personal data are to be used?

Suggestions

=> Search for an on-line notification of a Personal Information Collection (PIC) statement. The PIC statement is a means by which the site should inform you how your data are to be used, to what other parties they may transfer your data, your rights to request a copy of your personal data and correct any errors, and who should be contacted for such requests. Under the Ordinance, organisations in Hong Kong should provide this information on or before the time they collect your data from you.

Checklist

Are you asked to provide personal data not relevant to the purpose of collection?

Suggestions

=> Avoid providing excessive data that are irrelevant for the purpose. Check the on-line form which asks for your personal data and make a distinction between data that are mandatory and data that are optional. Beware of giving full personal details for recruitment on-line, lucky draw forms, dating or pen pal services, gambling web sites, on-line credit card and other service applications that ask for more information than is needed. Take care too, when registering to enter a site where apparently irrelevant personal information is requested. Consider giving your office instead of a home address or adding a statement in the address box, saying that the details given should be used for the stated purpose only.

Checklist
Are the data you provide of a sensitive nature, such as your credit card number or your ID card number?
Suggestions
=> Assume your communication is not private. Security is weak on the Internet unless you take precautions. Consider sending data of a sensitive nature only when you are sure that a secure means of transmission is used. Your browser can be set to say when you are about to enter or leave a secure communications zone. (see previous section on "Configure your system before connecting to the Internet").
=> Take precautions when you make on-line payment using your credit card. Your credit card number is a sensitive item of personal information. Before you provide your credit card number in making an on-line purchase, consider the use of tradition payment methods of using cash or cheque, and whether the vendor provides a secure environment for the transmission of you credit card number, e.g. transmission with the card number encrypted to minimise the possibility of security breaches. Another approach is to use a commercially available intermediary who will make payment from your credit card account, on your authorisation, but without the need for your card number to travel on the Internet. You can find out more about such services by searching the Internet using keywords "INTERNET CREDIT CARD PAYMENT".
=> Do not give out your ID card number easily. Organisations may ask for your ID card number when you deal with them via the Internet, for example, when you register with it for access to a service. However, not all of them have a justified or lawful purpose for doing so.

Checklist
Do your Internet e-mails sometimes contain sensitive personal data of yourself or others?
Suggestions
=> Consider using privacy protective tools to encrypt your e-mails. Every plain (unencrypted) e-mail you send can easily be intercepted and read. Encryption programs encode messages or files, making them difficult to be read by anyone including interceptors other than the intended recipient who has the decryption software. If necessary, protect the integrity of your e-mails by using some form of authentication mechanism. You can find out more about encryption by searching the Internet using keywords "INTERNET ENCRYPTION".
=> Consider using privacy protective means to remain anonymous. It is possible to send e-mails, and receive replies, anonymously on the Internet using an anonymous re-mailer. Anonymous re-mailers are intermediaries who shield the true e-mail addresses from being revealed with substitutes when correspondents exchange e-mails. This is an important aid to privacy, if you trust the anonymous re-mailer who makes this possible. If you are serious about complete anonymity, you can consider using multiple re-mailers services. You can find out more about these techniques by searching the Internet using keywords "INTERNET ANONYMITY".

Checklist
Do you give out personal details at search sites, newsgroups or chat areas?
Suggestions
=> Think carefully before revealing details about yourself. If you use one of the popular search facilities and you register your name with them as well, then consider this: Every time you make a search, your inquiry can be added to the list of topics that interest you. Your name, contact details, and that growing special interest list may become a detailed profile of you.
=> Respect others' privacy before revealing their personal data. Newsgroups or chat areas are services that allow simultaneous conversation between many users using the Internet. It is important to remember that, when you take part in these types of open discussion, data you provide about yourself or others are open to the rest of the participants and can be accessible over a long period of time. They are also Internet sites which provide a service whereby the messages you post in newsgroups can be searched and listed. Under the Ordinance, you have an obligation not to reveal the personal data of another individual to a third party (via newsgroups or chat areas) unless those data were collected for the purpose for which this is done or that individual has given express permission voluntarily for you to do so.

Checklist
Do you let your children surf on the Internet?
Suggestions
=> Teach and guide your children when they use the Internet. Children face special privacy risks on the Internet. Cartoon characters on a web site may seem, to your child, to respond directly to them. The characters may ask questions with enticing rewards and your child may give away personal and family details in response. The result may just be direct mails or advertising e-mails, but the abuses may be worse. A suggested rule for you to give your children is that no details should be given without your permission. Also, make sure they learn about privacy issues and supervise them in their first few on-line sessions on the Internet.

Checklist
Are you annoyed about direct marketing mails addressed to you?
Suggestions
=> Request marketers to stop sending you marketing mails. Under the Ordinance, an organisation in Hong Kong that makes a direct market approach to you has an obligation to offer you an opt-out opportunity not to receive further marketing approaches. This gives you the right to request the marketer to stop annoying you.
=> Take precautions to avoid receiving unsolicited advertising e-mails. To reduce the chances of making yourself a marketing target, you should avoid registering with free e-mail services and 'white pages' or e-mail directory services. If you use a signature file in your e-mail correspondence, be careful not to provide unnecessary details about yourself in the signature file which may expose you as a marketing target.

Checklist
Do you share your computer with somebody else?
Suggestions

=> Disconnect yourself promptly from the Internet. Remember someone with access to your computer can impersonate you under your e-mail address if your password is easy to guess or you remain logged on to the Internet with your computer unattended.

=> Clear your e-mail folders. Not only are e-mails vulnerable as they travel on the Internet, they reside on computers at the beginning and end of the journey for long periods. If others may use your computer, make it a habit to clear your e-mail folders and make sure you empty the "Trash" folder immediately afterwards. These folders are vulnerable, like all unprotected personal data.

Checklist

Do you know and are you worried that your computer retains a record of your surfing activities?

Suggestions

=> Avoid leaving an electronic trace in your computer. When you connect yourself to the Internet, your computer keeps track, not just of the pages you visit, but even of their content, for a while. If this is a privacy threat that concerns you, you can at least clear your temporary storage areas, for example, the "cache", "followed links" and "history" areas using options in your browser software. Alternatively, you can delete unwanted information from these areas periodically.

Conclusion

=> Security on the Internet is weak. You need to beware of the potential risks to your personal privacy every time you surf the Internet.

=> Every time you surf the Internet for fun, to obtain information or goods or services and when you are asked to provide your personal data, think about the potential risks that might affect your personal privacy before you press a "Submit" button or send off a message.

=> The Personal Data (Privacy) Ordinance protects your privacy interests in respect of your personal data with respect to Hong Kong based organisations. However, it would be in your own interest to take appropriate and "practical" precautions to minimise the privacy risks associated with your personal data with respect to such organisations as well as those organisations outside Hong Kong with whom you may interact on the Internet.

=> If you have queries about your privacy rights under the Ordinance, contact the Office of the Privacy Commissioner for Personal Data (PCO) for assistance.

[The information provided in this Guide is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of the law, direct reference should be made to the Ordinance itself.]