



How to keep your child safe on the Internet

By now, most of you will have heard of the Internet (or World Wide Web). Indeed, some of you may already be using the Internet to send e-mail to friends or colleagues, to find out the latest news, to shop for groceries online, or a host of other things. Anyone who has used the Internet will know the tremendous benefits that it can bring. But, as with other good things in life, the Internet also has a negative side.

About This Pamphlet

This pamphlet was written by police officers to alert parents to the very real dangers posed by children browsing the Internet. Teachers, too, will find the pamphlet useful. We hope to offer common sense and practical advice on how parents can safeguard their children, and how children can protect themselves.

The pamphlet is aimed at those unfamiliar with computers right through to accomplished users. We have tried to avoid 'jargon' or technical terms as much as possible. Where technical terms have been used, there will normally follow some brief definition.

Our purpose is not to alarm you unnecessarily, or frighten you or your children away from using the Internet. Thankfully in Hong Kong we have had very few problems as yet. However, as the Internet's popularity increases day by day, we should not become complacent.

Instead, be supportive of your child and encourage them to take full advantage of the wonderful opportunities that the Internet provides. As long as you and your child are careful and remember to keep the following points in mind, then your child should be perfectly safe. Happy surfing!

Some of the Dangers when Browsing the Internet

Lack of Regulation

The Internet is essentially an ad-hoc collection of inter-connected computer networks that span the globe. There is very little regulation and no central body to govern the kinds of material that can or cannot be published or 'posted' on it.

Some jurisdictions have tried to control the kinds of material on the Internet that their citizens can have access to. This kind of government censorship has largely failed, mainly because it is so difficult to limit access to a system that crosses numerous geographical, political, and cultural boundaries. Likewise, the Internet is changing and evolving so rapidly that it is practically impossible to maintain any form of control or regulation over it.

People, too, have different ideas about what is decent or indecent, proper or improper. For example what is considered obscene in one culture or country may be perfectly acceptable in another. Other people reserve the right to decide for themselves what kind of material they or their children should have access to, and strongly object to interference by government.

Still others jealously guard their rights to freedom of speech and expression. They use the Internet to promote their own ideas and agendas, however objectionable or offensive the average person might find those ideas.

Consequently a lot of undesirable subject matter, such as pornographic, racist, violent, drug-related or otherwise objectionable material finds its way on to the Internet. Much of this material is easy to find and freely available to anyone looking for such material, or to anyone who chances upon it by accident. That includes your children!



'Cyberstalking'



On the Internet a person can withhold their true identity and purport to be anyone or anything they want to be. This is a particular problem in chat rooms where a paedophile can easily pass himself off as another child (a chat room is not a room in the physical sense of the word, but rather a 'virtual' space where groups of people with similar interests interact online by typing messages to each other).

The paedophile will typically prowl children's chat rooms until he finds a vulnerable child. He will then try to befriend the child or be sympathetic to the child's problems (most susceptible are shy, naïve or lonely children, or those with low self-esteem). Once he has gained the child's trust and confidence, he will then try to elicit personal information about them, such as their full name, address, etc.

The paedophile may content himself by becoming increasingly suggestive online. In more extreme circumstances he may arrange to meet the child in person, or encourage the child to come to him; in the USA there have been several instances where children have run away from home in order to meet online 'friends' who later turned out to be paedophiles. In the very worst cases paedophiles have been known to stalk their child victims using information gleaned from them online.

Although we refer to paedophiles here as being male, which the vast majority are, it should be remembered that paedophiles can be male or female.

Online Harassment

Online harassment is where a person harasses another person by sending rude, suggestive, or threatening e-mail or online messages, rather like an obscene telephone call. Children are especially vulnerable to this kind of harassment, for whom it can be a particularly distressing experience.

Closely related to this is 'flaming', most common in chat rooms or newsgroups (a newsgroup is an electronic notice board where people post or read messages on a shared topic of interest). A person is normally flamed (sent an abusive e-mail or online message) for saying or doing something that annoys other members of the discussion group. Again, to be flamed like this can be very distressing for a child.

An easy way to avoid being flamed is to read the FAQ (Frequently Asked Questions - a document containing rules of the newsgroup and answers to the most commonly asked questions) and to observe 'Netiquette' (Internet etiquette - for example typing in upper case letters during an online discussion is akin to shouting at someone and is considered rude).

Hackers and Hacking

Hacking can be broadly defined as the act of gaining unauthorized access to remote computer systems, usually via the Internet. It can be likened to electronic breaking and entering. A hacker is the person who gains such access.

Hackers need only standard computer equipment and rudimentary knowledge of computers to begin hacking into systems. Much of this knowledge can be gained through the Internet itself. Some hackers relish the intellectual challenge or thrill of hacking whilst others do it to cause mischief or as part of a criminal enterprise.

Children have keen and inquiring minds and are easily captivated by the excitement and challenge of hacking. Be warned; in Hong Kong, as in many other countries, hacking into computer systems is a serious criminal offence that carries with it potentially heavy penalties! Sadly, it is a fact that a large percentage of detected hacking cases in Hong Kong involve young persons or students. More often than not, these youngsters do not realise that they are committing criminal offences in performing such activities over the Internet. The Police are capable of detecting these offences, and the arrival of Officers to take inevitable enforcement action can obviously have devastating effects for that child and household.

Encryption

When you send information via the Internet, for example an e-mail message to a friend, it can be intercepted and read at any point along its journey. Normally this isn't a problem. Consider, though, if you were buying something online using your credit card. If this credit card information were to be intercepted by a third party, then that third party could potentially use your details to make purchases over the Internet.

The only way to prevent information sent via the Internet from being compromised is to use encryption. Encryption is the process whereby information is encoded so that only the intended recipient can decode (read) it using a key or password. Without the key or

password, the information will appear as scrambled or garbage characters to the casual observer.

You may be wondering how this is relevant to you and your child's safety on the Internet. Firstly, it is important you realise that information sent via the Internet is not secure unless it is encrypted. Secondly, as more and more companies are engaging in e-commerce activities, you may be tempted into buying goods online without realising the inherent risks of such transactions.

Before buying goods via the Internet, first check that the company with whom you are doing business is well known and trustworthy. Secondly, make sure that they are taking appropriate security measures to safeguard your personal information, such as the use of encrypted secure transaction methods. More information on tips for using e-commerce safely can be found on the [Computer Security section of the Crime Prevention Bureau web-site](#).

A word of warning! Should your child want to buy something online, and you agree to it, then you and not your child should complete the order form, bearing in mind the above advice. Another good reason to keep credit card numbers secret is that some children have been known to steal this information from their parents so that they can order goods online without their parent's permission!

Other Considerations

Many companies now use the Internet to promote, advertise or sell their products. This is generally a good thing. However, some unscrupulous companies use their Web sites to deliberately target children in the hope they will pester parents into buying their company's products. Obviously most parents would rather their children avoid such overtly commercial sites.

Other companies use 'spam' to sell or promote their products or services. Spam or 'spamming' is the practice of sending unsolicited e-mail to newsgroups or to a personal e-mail address. Spam is considered a breach of Netiquette and an invasion of privacy by some. If you do receive spam, either ignore it or report it to your ISP (Internet Service Provider) which may be able to prevent further occurrences of spamming. We recommend that you do not reply to spam e-mail, as this will only confirm your e-mail address as being viable.

Other Web sites ask for personal information (online profiles) before allowing access to their site or services. Most sites use this information for market research purposes only, although some unethical sites will sell this information to direct sales or marketing companies. As a rule of thumb, before releasing personal information, check to see if that company has a privacy policy stating what it will do with your data. Also, only submit those details which are required to perform a transaction, and do not submit optional data.

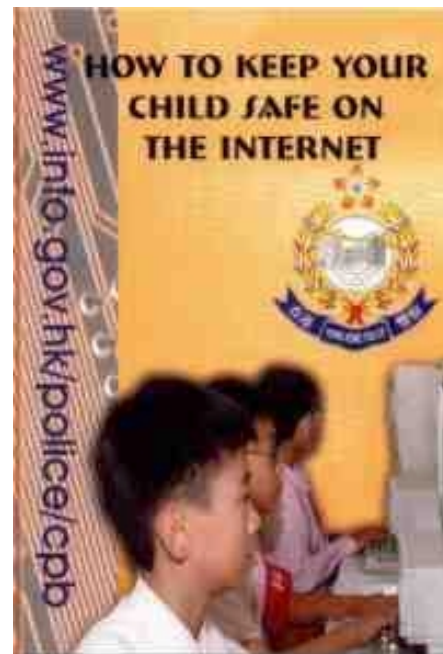
What you can do as parents



- It is important for parents or guardians to become more computer literate. If you are unfamiliar with computers or the Internet, have your child teach you. Spend time with your child online and let them show you their activities, the Web sites they visit and learn something about the electronic pen pals with whom they communicate.
- Talk to your child about the kind of Web sites, newsgroups and material that they are allowed to visit and view, and those they are not. Encourage them to visit Web sites designed especially for children (there are many such sites that are both educational and entertaining). Show them this pamphlet and discuss with them the dangers they can face online and how they can protect themselves.
- Encourage your child to discuss with you if they find something online that seems strange to them, or makes them feel embarrassed, angry, confused or uncomfortable. Don't blame or punish your child for stumbling across such material and then coming to you for guidance.
- Agree with your child a set of rules, or 'dos and don'ts'. Post these rules next to the computer for your child to see every time they log on. At the back of this pamphlet you will find some suggested ['dos and don'ts'](#) that you may care to use.
- Put the computer in a family area of your home, not your child's bedroom. This way you can always keep an eye on your child's activities, even if you can't monitor them directly. Remember, though, that children do need some space and privacy occasionally, if only to show that you trust them.
- Monitor the length of time your child spends online, and at what times of the day and night they are using the computer. Too much time on the computer can be unhealthy and detrimental to your child's social development. *It may be possible to check with your ISP to find out how many hours per month the Internet account is being used.*

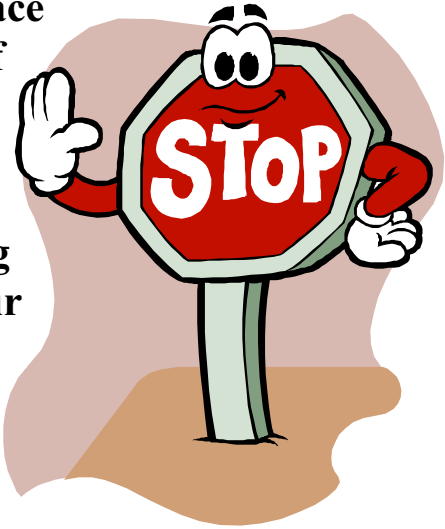
- Where relatives or domestic helpers are looking after children, consider giving them guidelines on how and when your child should use the computer.
- Consider using parental filtering software. Parental filtering software programs block access to objectionable Web sites, chat rooms or newsgroups, or filter out certain subject matter. Other such programs will prevent your child from divulging personal information about themselves online, or log what Web sites they have been visiting. *The Hong Kong Telecommunications and Licensing Authority provides a list of such filtering software at their Web site http://www.info.gov.hk/tela/f_care.html.*
- Be aware that parental filtering software is not always 100% effective and can sometimes block out perfectly innocent subject matter. Even if you do decide to install such filtering software, you will still need to monitor your child's activities.
- Many Web sites voluntarily evaluate their site content against industry rating standards, for such things as nudity or offensive language. Some Internet browsers (the programs that let you view documents, or navigate from one document to another on the World Wide Web) then give you the option to prevent access to particular Web sites depending on these ratings. Make sure to enable these options on your browser.
- For the more accomplished computer users amongst you, check your browser cache or history lists to find out which Web sites your child has been visiting.
- Tell your child, when online, not to reveal personal information about themselves or your family such as full names, telephone numbers, home address, the school they attend, credit card numbers, etc. This is especially true of online profiles. Likewise they should never reveal to anyone their intended movements or the places they frequent.
- Except with persons you know or trust, don't allow the online exchange or posting of personal photographs of your family, your home, your child's school, etc.
- The use of chat rooms should be discouraged as much as possible. If you do allow access, make sure that the chat room is specifically for children, and that they are moderated (monitored for improper behaviour by those running the chat room). In any case, monitor your child's online chat and NEVER allow your child to enter a 'private' (one on one) chat room.

- Make sure your child informs you if they are invited to meet an online friend face to face. If you decide it is OK for your child to meet that person, then make sure it is in a public place and that you are present, at least for the first meeting.
- Encourage your child to observe 'Netiquette' and be as polite online as they would be in person. Likewise tell them to inform you of any rude, suggestive or abusive e-mail or postings that they receive.
- Be aware of changes in your child's behaviour. Uncharacteristic or anti-social behaviour such as sullenness, depression, secretiveness, violence, improper physical contact etc may be indicative of a problem.
- Use the Internet to find out how to protect your child. There is a wealth of software and information available online, from government agencies, filtering software companies, children's foundations, to concerned parents themselves. You owe it to your children to stay informed.
- And remember, should you come across pornographic or indecent material involving minors, or discover any instance when your child is put in harm's way, then make a report to police immediately.
- Should you have any queries in connection with this subject, the Computer Security Unit of the Crime Prevention Bureau is available to assist. We can be contacted via e-mail at csucpb@police.gcn.gov.hk, or by phone on 2301 1601 (English) or 2301 1654 (Cantonese).
- The following summarised advice on some “dos and don'ts” for kids, can also be found on a leaflet “How to keep your child safe online” produced by the Crime Prevention Bureau. If you would like to have copies of this leaflet, please contact the Computer Security Unit using the details above.



Kids, there are some people in cyberspace who like to harm or take advantage of children if given the chance. DON'T give them that chance!

Here are a few reminders about using the Internet safely. Keep them by your computer so you don't forget them. And remember, if you are unsure about something, then ask your parents, guardian or teacher for advice !



Some DOs



DO use the computer for school projects, homework, to learn about new things like sports and hobbies, or to play games.



DO tell your parents or guardian if you find something online that seems strange to you, or makes you feel angry or uncomfortable. Remember it's not your fault if something like this happens.



DO be as polite to people online as you would be in person. You wouldn't like people to be rude to you.

Some DON'Ts



DON'T spend too much time on the computer, it's unhealthy and there are plenty of other interesting things that you could be doing.



DON'T look at stuff that you're parents or guardian don't want you to. If you find it by accident, hit the back button on your browser and look for something else.



DON'T respond to messages that are mean or rude. Tell a parent or guardian immediately.



DO tell your parents if an online pal wants to meet you in person.



DON'T meet your online pal in person unless a parent or guardian is with you, at least for the first time.



DO use the computer to keep in touch with your friends and relatives, and online pen pals.



DON'T reveal personal information about you or your family, or exchange personal photos with strangers.



DO be wary of new people that you meet online, as you would be in real life. Remember that online a person can pretend to be anyone or anything they want to be. Perhaps they are being nice to you because they want something.



DON'T enter chat rooms unless they are specifically for children and you have permission from your parents or guardian. **NEVER, EVER** enter a private chat room.



DO change your passwords frequently



DON'T disclose your passwords to anyone, not even your best friends.



DO ignore 'spam'. Spam is e-mail from people who you don't know who are trying to sell you something.



DON'T answer e-mail from strangers or people who don't identify themselves. Tell a parent or guardian immediately.



DON'T try to gain access to other computers unless you have permission.



DON'T order or buy anything online without first getting permission from a parent or guardian.



This pamphlet was produced by the Computer Security Unit, Crime Prevention Bureau, Hong Kong Police.

The information contained in this pamphlet is given freely and in good faith, and is for information purposes only. The Hong Kong Police accept no legal responsibility for the advice given.

Permission is hereby given to reproduce all or part of this document, provided that such material is used in the manner for which it was primarily intended.