FACT SHEET

Personal-use Computers

Operating Safety & Security

Many of us take our computer security for granted. After all, the computers are housed in our homes where we tend to feel secure. Problems can develop without taking proper precautions. Here are some of the basics you need to keep your computer operating smoothly and minimize the risk of computer related crime.

PASSWORDS

Basic computer security starts with a password. Care should be taken when choosing a password so that the password is unique and not predictable. The best passwords often include a combination of letters and numbers. It is a very good idea to change your password regularly. Never share your password with anyone or leave a password in a visible place tacked up next to your computer.

COMPUTERS AND THE INTERNET

The risk of problems greatly increases once you're on the internet. The internet is a two-way form of communication with a culture of anonymity and/or false identities that can breed criminal activity. This can lead to serious problems including loss of privacy and/or control from both known and unknown sources. Computer "hackers" can electronically access and use your computer by virtue of it just being left on without your even knowing it.

FIRE WALLS

In order to protect yourself against people trying to "hack" their way into your computer, you should consider obtaining software commonly known as a firewall particularly if you store sensitive information on your computer (such as bank account numbers) or have high speed internet access.

The primary purpose of the firewall is to act as a filter to discourage "hackers" from breaking into your computer. Firewalls can also:

- help to minimize "cookies" (tiny scraps of program code placed on your computer when you visit web sites),
- block/alert you to spyware, and
- guard against viruses that use a direct attack.

Some firewalls can be downloaded for free, but they are not as effective as store bought filters. If you don't have firewall software, unplug your internet connection when not in use. This will limit your exposure to the times that you are actually using the internet.

VIRUSES

Viruses are a criminal act of mischief that can do considerable damage to stored information and impair the use of your computer. To protect yourself against viruses, follow these do's and don'ts:

DO

- Install a firewall.
- Install anti-virus software.
- Update the "definitions" stored within anti-virus software on a monthly basis.

DON'T

- Open an e-mail from a source you do not recognize.

E-MAIL

"Spam"

"Spam" is the term used to commonly refer to unwanted e-mails. Unwanted e-mails typically result from our having visited a website (an electronic record having being made of your computer's "signature") or leaving your personal e-mail behind. "Spam" can be managed by:

- purchasing software that works like anti-virus software,
- never open or reply to these messages (this includes responding to the "click here to remove me from the list" messages as this tells the person who sent it that their message is getting through), and
- limiting use of your personal e- mail by setting up a hot-mail address and using this instead.

Fraudulent Messages & Solicitations

Almost any crime committed in society, can be enhanced through the use of computers. Fraud artists regularly utilize computers to send scam letters and messages. If you receive an e-mail soliciting funds in exchange for access to large sums of money or your bank account, regard the e-mail as a fraud.

"Phishing"

"Phishing" is the term commonly used to refer to e-mails that appear to come from legitimate financial institutions, online retailers and even governments regarding some type of security threat that are written with a sense of urgency.

The e-mails solicit confidential data such as credit card or social insurance numbers and are used for the purpose of perpetuating identity theft. Never respond to these messages. Report them directly to the affected company or institution. For further information about frauds, obtain a copy of the Frauds fact sheet.

Chat Rooms

People frequently meet strangers who represent themselves as someone they are not in chat rooms. This is frequently done with a sexual and/or criminal purpose in mind. Don't trust the identity of anyone you meet in a chat room and be extremely cautious about revealing any personal information.

Cyber Stalking *I* Harassing E-mails

E-mails, like the telephone, can occasionally be harassing in nature. Cyber stalking often takes the form of harassing e-mails which commonly results from failed chat room encounters. If you are receiving harassing e-mails contact your internet service provider. If the e-mails are threatening or otherwise disturbing in nature, contact Police.

SPYWARE

The purpose of spyware is to monitor or control your computer's use without your knowledge or consent Spyware can track your habits, keep statistics on what you do and even result in identity theft. Spyware can also result in some or all of the following:

- Barrage of pop-up ads.
- Hijacked browser.
- Sudden or repeated change in your computer's internet home page.
- New and unexpected toolbars and icons.
- Keys that don't work.
- Random error messages.
- Sluggish/slow performance.

Spyware can be eliminated by getting an anti-spyware program from a vendor you know and trust. Other tips for dealing with spyware:

- Update your operating system and web browser software.
- Download free software only from sites you know and trust.
- Never install any software without knowing exactly what it is.
- Set your browser security setting no lower than medium.
- Keep your browser updated.
- Don't click on any links within pop-up ads.
- Don't click on links in spam that claim to offer antispyware software.
- Install a personal firewall.

MAKING PURCHASES OVER THE INTERNET

The internet has become a popular place to buy and sell goods. Problems can develop as a result of:

- fraudulent/bogus auction sites/purchase of precious metals,
- international boundaries,
- dealing with a site that is not "secure", and
- limited insurance on legitimate auction sites.

In order to protect yourself against fraud, follow these do's and don'ts:

DO

- Look for the name and contact information of the item's owner.
- Find out about delivery charges, warranties, and insurance requirements before you buy.
- Consider obtaining a credit card to be used solely on the internet.

DON'T

- Enter personal data unless a statement indicating that all information is kept confidential is clearly visible and the site is secure.

WIRELESS NETWORKING

Many households and small business are switching to the convenience of wireless networks. Wireless networks work on the same principle as radio waves. As such your network will now be broadcast and accessible outside of the home. Without proper security in place outsiders can "sniff out" and access your internet connection, computer network and files through a process known as "war driving". People who have wireless networks in place or who are considering this technology should research and take the latest security precautions to protect themselves from illegal use and access of their network.

YOUR INTERNET SERVICE PROVIDER

Be aware that your Internet Service Provider (ISP) can track and provide you with a record of the following:

- the internet address of everyone you send an e-mail to as well as when you sent it,
- the contents of unencrypted e-mail,
- the contents and source of every file you download, and
- the address of every website you visit and the length of time you spend there..

AVOIDING THEFT OF YOUR COMPUTER

Personal computers, especially laptop computers, can be readily stolen. In order to reduce your chances of having a computer stolen follow these do's and don'ts:

DO

- Mark your property using a driver's license number (see the Mark Your Property fact sheet).
- Carry your laptop computer with you if you travel.
- Break up computer related boxes and be discreet when recycling/throwing them out.

DON'T

- Leave your computers near an unlocked window or door.
- Work on a computer with the screen to the street.
- Leave a computer visible in your car.