Cybercrime

Cybercrime are crimes that have been committed with a computer and the Internet. The Calgary Police Service uses the term "cybercrime" to refer to Internet scams with reference to malware, hacking, auction fraud and assorted activity of this nature.

The Canadian Anti-Fraud Centre maintains a list of common and current scams that you should be aware of.

Did you know? Studies have found that 70% of people experiencing cybercrime have never reported it and of those 45% indicated they were unsure of whom to report the crime.

Protecting yourself from cybercrime

With all of the malicious programs out there, it's important that you understand some of the things you can do to keep your computer protected:

- **Use virus protection software**. Anti-virus software recognizes and protects your computer against most known viruses. However, attackers are continually writing new viruses, so it is important to keep your anti-virus software current.
- **Keep your computer software current**. Install software patches and updates so that attackers can't take advantage of known problems or vulnerabilities. You should also consider allowing automatic software updates.
- **Use caution with email attachments and items requiring downloading.**
- **Install a firewall**, which may be able block malicious traffic before it can enter your computer. Some operating systems actually include a firewall, but you need to make sure it is enabled.
- **Set your web browser security level to Medium or High**.
- **Be cautious** when using Peer-to-Peer software.
- **Spyware** is a common source of viruses, but you can minimize the number of infections by using a legitimate program that identifies and removes spyware.
- **Change your passwords** on a regular basis and make them hard to guess by using numbers and special characters. This includes passwords for web sites that may have been cached in your browser.

Reporting cybercrime

If you have been the victim of an online crime, please call the Calgary Police Service non-emergency number at 403-266-1234 to report the crime.

Online sexual exploitation of children must be immediately reported the Calgary Police Service. Call 9-1-1 for any crimes in progress or life exigent circumstances or 403-266-1234 for the Calgary Police Service non-emergency line. You may also report crimes of this nature anonymously to the Canadian Centre for Child Protection.

If you are a victim of online financial crime, please follow these steps:

1. File a complaint with the Calgary Police Service and obtain a police case number.
2. Contact your bank/credit card company if any of your financial information was used. Give your police case number to your bank/credit card company to place on file.
3. Provide the police case number and have fraud alerts placed on your credit reports to either of the two credit bureau companies, Equifax (1 800 465-7166) or TransUnion in Canada.
4. Report the incident to the Canadian Anti-Fraud Centre or 1-888-495-8501.

About malware

Because of the wide use of email, it is a favorite target of hackers - email attachments are common sources of cybercrime. Malware via email comes in a variety of formats so you can never be too careful when opening email.

Email file attachments can contain malware, particularly if they are .exe (executable) files.

Watch out for "disguised" attachment such as a .gif file with an extra ".exe" extension (for example, a file named "happyface.gif.exe" is suspicious.) Opening such a file will almost certainly cause harm to your computer, since the sender felt the need to disguise the file's actual nature. Furthermore, some MS Office files (e.g., with .doc or .xls suffixes) have applications called macros embedded in them. Be cautious when opening files containing macros because the file could have malware embedded. You should also only open compressed files from trusted sources.

Some emails contain malicious links that can lead to viruses and "spyware." Don't follow links in email messages, especially if you don't recognize the sender or were not expecting it.

Types of malware

- **Computer viruses** - these are programs that copy themselves. Viruses can destroy files stored on your computer, corrupt your operating system, and in a worst-case scenario, deny service or shut down an entire network.
- **Trojan horses** - a Trojan Horse masquerades as a benign application and seems to perform a desirable function but damages or compromises the security of the computer. In addition to the expected function, it steals information or harms the system.
- **Spyware** - also called adware, sypware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. It is similar to a Trojan Horse in that users unwittingly install the product when they install something else.
- **Keyloggers** - a keylogger is a computer program that logs each keystroke a user types on a keyboard. Keyloggers can also capture screenshots of user activity, log passwords, record online chat conversations or take different actions in order to find out what a user is doing. Malicious keyloggers often are installed by other parasites like viruses, trojans, backdoors or even spyware.

Important: Avoid conducting banking business or entering personal information on public computers such as computers found in libraries or cybercafes. Public computers could contain keyloggers.