SLOWING DOWN CYBER CRIME

Internet criminals want to make money quickly and easily. The more difficult you make their job, the more likely they are to leave you alone and move on to an easier target.

We asked experts at J.B. Maclean Consulting (http://www.jbm.net/), who specialize in intelligence solutions, and they advised us of the following:

Choose strong passwords and protect them.

- Choose a password that cannot be easily guessed. Strong ones have at least eight characters and use a combination of letters, numbers and symbols (i.e. # $ %). Avoid using your last name, and words that can be found in a dictionary.

- Keep passwords in a safe place and don't use the same password for every online service. Change them regularly, at least every 90 days.

Install security software.

Security software includes firewall and antivirus programs. A firewall controls who and what can communicate with your computer. Antivirus software protects computers from viruses, worms, Trojan horses, spyware and other malicious programs.

Protect your personal information

- Watch for fake emails. Emails will tell you to provide information immediately or else something bad will happen. Don't take the bait.

- Don't respond to email messages asking for your name, address, phone number and email address. Legitimate companies will not use email to ask for this. When in doubt, phone the company.

- When visiting Web sites, type their address (URL) directly into the Web browser rather than following a link within an email. Web sites requiring sensitive information should have an "S" after the letters "http" (i.e. https://www.yourbank.com not http://www.yourbank.com)/. The "s" stands for secure.

- Spammers send millions of messages. Responding to these messages or downloading images ensures you will be added to their lists to receive more messages.

Online offers that look too good to be true usually are.

Supposedly "free" software and contests that you've surprisingly won without entering are enticing hooks, but may contain advertising software ("adware") that tracks your behaviour and displays unwanted ads. If an offer looks unbelievable, ask someone else's opinion, read the fine print, or even better, ignore it.

Review bank and credit card statements regularly.

The impact of online crimes can be greatly reduced if you can catch it shortly after your data is stolen. Check statements for anything out of the ordinary.

Fortunately, many banks may call to ask you to confirm unusual purchasing behaviour (i.e. you live in Alberta and all of the sudden start buying refrigerators in Budapest). Don't take these calls lightly - this is your hint something bad could have happened and you should consider updating your computer, your software or your passwords.

Keeping things current will make it more difficult for hackers to gain access, and might discourage a less-determined attacker to look for a more vulnerable computer elsewhere.