Crime Prevention Week

November 1st to 7th, 2019

Crime Prevention is Everyone's Responsibility

Online Fraud Prevention – How Cyber Safe Are You?

There are times where it is hard to imagine life before the Internet. From e-mail to social networking to shopping to turning lights on and off in your home, citizens are performing more of their daily activities online and putting more of their personal information online. As the Internet becomes the connection to everything, the speed and sophistication of different forms of online fraud continues to grow.

In 2018 there were 32,968 reported cases of internet related crimes in Canada, impacting 7,727 victims
~ Statistics Canada

Identity Theft: Any false, deceptive, misleading or fraudulent act used to obtain someone else's personal information for criminal purposes. Identity theft techniques can range from unsophisticated, such as dumpster diving and mail theft, to more elaborate schemes, such as phishing, job scams, loan scams, service scams, tax scams, bank investigator scams, and investment scams. Computer spyware and viruses designed to help criminal acquire personal information are an emerging trend.

Credit/Debit Card Crimes: Organized criminals have the technology which allows them to "skim" the data contained on magnetic strips and manufacture phony cards. Cardholder information can also be used for fraudulent purposes.

Phishing Scams: Traditionally associated with misleading and deceptive emails or text messages. Criminals falsely claim to be from a legitimate organization such as a financial institution, business or government agency in an attempt to have you surrender private and personal information

Information Sought After by Cyber Criminals:

- Name
- Date of birth
- Address
- Mother's maiden name
- Driver's license
- Passport information
- Credit card numbers
- Social Insurance Number
- Bank account number
- Any personal information they can benefit from

Cyber criminals take advantage of low cyber security awareness, and technological developments to gain unauthorized access to their victims' personal and financial information.

Criminals can use your stolen or reproduced personal or financial information to

- Access your computer/e-mail
- Access your bank accounts
- Open new bank accounts
- Transfer bank balances
- Apply for loans or credit cards
- Make purchases
- Pay for adult websites
- Gamble online
- Hide their criminal activities
- Obtain passports or receive government benefits
- Get a job
- Rent cars and book vacations

Crime Prevention Week 2019

November 1st to 7th, 2019

Crime Prevention is Everyone's Responsibility

Passwords, the key to protection

- Create passwords eight characters in length using a combination of upper and lower case letters, numbers and at least one character that isn't a letter or number.
- Be creative. Use your pet's name, your favourite numbers, the street you grew up on or other combinations. Then make it even tougher by changing some of the letters to numbers (e.g. use a "3" to replace an "e").
- Never use your name, birthday, driver's license or passport number.
- Commit your passwords to memory and don't store them on your computer or in your mobile phone.
- If a website or browser asks to keep you signed in, unclick that option and take the time to re-enter your password each time.
- Clear your browsing history or cache after online banking and shopping.
- If you get an e-mail that includes a password you've just set up, delete it.
- Make sure sites are secure before you enter your password.
- Avoid using a single dictionary word.
- Don't repeat numbers or letters (i.e. 55555 or bbbbb). Don't use simple sequences (123456 or abcefg) or letters that appear in a row on your keyboard (qwerty).
- Make sure that you change your smartphone's original default password.
- Change your passwords after implementing a fix or following being compromised.
- Use different passwords for different online accounts, especially those dealing with sensitive or financial information (banking online).

Protecting your Money

As online banking activities expand, cyber criminals are finding new ways to bypass the security measures established by financial institutions to protect your personal and financial information.

Choose strong passwords for your online banking and financial accounts and keep them private.

- Look for the lock symbol on the website or "https://" at the beginning of the website address (the "s" means "secure") to be sure the site is encrypted.
- Never allow "auto fill" or "auto-remember" of your password or personal information.
- Ensure your anti-virus protection and web browser are both the latest versions. Use a firewall and make sure it's set to "on".
- When finished online banking transactions, close the browser window, clear the cache (delete your browser history).
- Never use public WiFi or public computers to conduct online banking transactions.
- Legitimate banks and businesses will never ask for personal information in an e-mail or by text message.
- Always enter the website address in the browser yourself – never use a link supplied in an e-mail.
- Review your bank and credit card account activity regularly. Contact with your financial institution right away if you notice anything suspicious.
- When in doubt, call your bank about suspicious messages. Verify by phone and don't reply to a suspicious message or click on a link that's in it.
- Always log out completely.
- When disposing of an old computer or electronicc device, be sure to erase all personal data.

Banking on the Go

Most banks offer online banking apps for easy access to your financial information and allowing you the ability to complete online banking transactions from your phone. Make certain of the following before logging onto a banking app:

- Is your wireless network secure?
- Is your mobile banking application actually from your bank? Be sure it's the real thing and not a copycat.
- Have you installed anti-theft technology on your mobile device, and backed up your data?
- Does your device automatically lock after a period of time? If not, it's a good idea to set this feature and use a strong password for your mobile device.
- Do not store passwords and banking information (branch #, bank address) on your mobile device. If you lose your phone, this information would go with it.
- Are all of your apps and device software current?