

Sergeant Bob's Personal Safety Tips

Retired Police Sergeant Bob Paterson works with The McLennan Group Insurance Inc. to develop practical safety tips for CARP members.

"Don't gamble with your safety. The stakes are too high."

Electronic Crime Review

While senior Canadians are frequently targeted and victimized, Electronic Crime (E-Crime) is increasingly common for all age groups. It costs nothing to provide a level of security that is manageable and tolerable.

E-Crime Basics

E-Crime can be classified as either theft or fraud designed to generally do one of two things:

- Obtain money from your accounts or make purchases using your personal banking information.
- Apply for new identification and credit using your personal information, otherwise known as identity theft.

In an E-Crime, a thief with your PIN, or other electronic codes, can easily access your personal information and credit. Just as you want to keep the key to your family safe secure, you and your financial institutions are trying to keep your PIN and electronic codes guarded.

It takes a smart and patient thief to obtain the information needed to unlock your bank accounts, but the returns can be very high. Detection and apprehension of e-criminals is difficult for police and even if convicted, the sentencing is typically less severe than a traditional criminal act.

What you should do:

- Tip #1:** Make yourself aware of some basic safety tips that will address the most common forms of E-Crime.
- Tip #2:** Be sure to report any real or suspected E-Crimes to your local authorities in a timely manner.

What you shouldn't do:

- Tip #3:** Do not become pre-occupied with every possible form of E-Crime and worry about every financial transaction. E-Crime thieves are adaptive and creative and their methods change frequently. Leave the technical work to the experts who have a vested interest in combating E-Crime on your behalf and review the tips provided in this document to increase your security.



How Does E-Crime Happen?

There are dozens of methods for e-criminals to use: Sleight of hand tricks by a dishonest retailer that electronically skims info from your credit card; theft of your mail, unattended purse or wallet; or more recently the introduction of electronic pick-pocketing which relies on using Radio Frequency Identification Technology (RFID) to obtain your information without ever laying a hand on your wallet. The information needed to pull off an E-crime can also be obtained by telephone, email or by a convincing fraudster at your front door.

Common E-Crime Methods:

The most common forms of E-Crime are:

- Stealing your credit card, PIN or other personal information from your home, workplace, mail or garbage.
- Asking you for your personal information by phishing; the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. As an example: Sometimes email messages, complete with company logos, could be received with a request to confirm information such as your PIN and account number. Another common technique is advising that they "have identified a problem with your account" or that "you are eligible for a valuable credit" and just require some details from you.



Electronic Crime Review Continued...

What to do about phishing?

- ❑ **Tip #4:** Do NOT surrender private account numbers, PIN information, your SIN or date of birth online. The exception is if you initiated the contact using the email address or website taken directly from past official company letterhead.
- ❑ **Tip #5:** Do NOT click on web links contained in an email. Instead source the information and type the web address directly into the browser.
- ❑ **Tip # 6:** When unsure about the validity of an email request look for two things:
 - Look for spelling and grammatical errors in the text.
 - Contact the company in question by sourcing the correct phone number and calling their customer service department to confirm validity.

Electronic Pick-Pocketing:

Credit card Radio Frequency Identification (RFID) has made paying for purchases much more convenient for consumers but this recent technology has also made it possible for a thief to scan some credit card information by simply placing a scanning device close to your wallet or purse as you walk by. But do not be alarmed! While a recent bulletin from the Canadian Bankers Association (CBA) confirms that a thief may be able to scan some data from an unsuspecting cardholder they will have difficulty using this information to make purchases since the data is incomplete. The three-digit number on the rear of the credit card remains unknown to the thief and complete magnetic strip data or electronic chip data is not captured by the scanning device.

Legitimate cardholders should not be overly concerned about electronic pick pocketing as the chance of complete credit card information being illegally scanned is remote.

Credit / Debit Card Security:

Protect your cards as if they were gold; they can be just as valuable to a trained fraudster.

- Don't share your PIN and don't record the PIN anywhere near the card location (on the rear of the card or on a piece of paper in your wallet, etc.). A stolen card, complete with a matching PIN, makes things very easy for a thief.



- When making a purchase don't lose sight or control of the card, and don't let anyone walk away with your card.
 - Watch carefully and be alert to a distraction that could draw your attention away from the transaction, allowing the card to be swiped a second time.
 - Be alert to someone watching you enter PIN information; try to subtly shield your entry from others.
 - Be alert to a modified or tampered automatic banking machine, especially where the card is inserted.
 - When using a credit card number to make reservations or telephone purchases, use a credit card with a low spending limit.
 - Contact your bank prior to making a large or irregular purchase or if travelling abroad. The banks are trying to protect you and will be cooperative.
 - If your credit / debit card is stolen, lost or if you suspect trouble, report it immediately.
- ❑ **Tip #7:** Keep your receipts and monitor your bank statements monthly. Be sure to shred old banking documents prior to discarding them.

Electronic Crime Review Continued...

Mail Theft & Garbage Security:

It's amazing how much personal information can be obtained just by looking through our mail or garbage. And, frighteningly, a wide variety of financial data can be lifted directly from your mailbox or the recycle bin sitting at the curb.

What should you do?

- Install a residential mailbox with a locked storage compartment, or a mail slot directly in the security door making any possible theft more time consuming.
- Rural mailboxes should not display the family name and should be emptied as soon as possible.
- Be aware of unfamiliar people accessing the mailbox after the initial delivery. The person could be removing, rather than delivering your mail. Call the police with a vehicle description and direction of travel if you suspect a rural mail theft, it's very common.
- When away from home, have a trusted friend collect your mail before it accumulates or advise the post office and ask them to hold your mail until you return.
- If an expected cheque or other valuable mail item doesn't arrive on time, contact the issuing agency immediately.
- Put garbage at the curb in the morning instead of the night before.
- All sensitive papers should be ripped up, shredded or otherwise destroyed prior to disposal.
- Discarded cheques, old or rejected credit cards must be cut into several pieces before they reach the garbage container.

Watch Out For The "Recovery Scam"

Sometimes, after an E-Crime has been committed, fraudsters have approached the initial victim a second time in hopes of recovering more money or additional information. People posing as investigators will make a seemingly sincere offer to research the crime and recover lost money and help recoup for damages. This offer to investigate will not be free. You will be asked for up front money to get the investigation started. The possibility of recovery money and solving the problem can be attractive, especially to an individual who was embarrassed or reluctant to report the original E-Crime.

What should you do?

- Recognize this as a Recovery E-Crime scam, record contact information and report it to the authorities as quickly as possible. Don't be victimized twice

Tip #8: Police and banking officials will never ask you for money to support their investigation.

In Summary

Even if you have not been directly affected by E-Crime, we all pay a price in terms of increased security measures, institutional fees, and interruptions to routine financial transactions.

E-Crimes are complex and constantly evolving so a solid defence is difficult. A few basic, no cost security steps can provide a level of security that is manageable and tolerable. Individuals are reminded to TAKE CHARGE and be vigilant when sharing personal information.

Above all else remember this critical tip: If you are being rushed into making a decision or asked to share personal information, STOP! Do nothing in haste. Pressure to make a fast decision is the strongest indicator that something is wrong. Instead, do some basic research, confirm the facts and ask for help prior to making a decision about sharing personal information.



www.carpinsurance.ca