
SCAM
cybercrime
VICTIMS WITHOUT BORDERS
FRAUD
phishing
ONTARIO ASSOCIATION OF CHIEFS OF POLICE
OACP

DO YOU KNOW WHAT FRAUD LOOKS LIKE?

WE DO.

Allstate.
You're in good hands.

Whether it's an exaggerated claim, identity theft, or staged collision, fraud comes in many forms. But one thing is certain - insurance fraud costs us all. Fortunately, Allstate's Claim professionals are equipped with early fraud detection measures. Complex cases are handled by employees in our Special Investigations Unit - dedicated to investigating, prosecuting, and deterring fraud.

We can all be active in protecting ourselves and stopping fraud when we see it.

Learn more:
www.ibc.ca/en/Insurance_Crime

Report it: 1-877-IBC-TIPS

122000 (01/12)

MESSAGE FROM
the Ontario Association of Chiefs of Police

In today's technology-driven world, it is no surprise to Ontario's police leaders that technology is increasingly being used by criminals and criminal organizations as a tool for perpetrating crime; crimes which know no borders.

That's why the Ontario Association of Chiefs of Police (OACP) is pleased to work with our corporate and community partners to promote the annual Crime Prevention Campaign. Our focus for 2012 is on safeguarding Ontarians against electronic and online fraud – a growing area of criminal activity which feeds on opportunity. Ontario's police leaders believe that educating and empowering our citizens on how to better protect themselves against online and electronic fraud is the best crime prevention tool available.

We've all heard about scams using technology – those annoying emails from a foreign 'prince' asking for your help to transfer a fortune, emails announcing that you have won a lottery prize, or electronic attacks on your banking information through ATM machines and debit card scanners. Besides the technology used, these crimes all have this in common – unwary, uninformed, and otherwise vulnerable citizens.

This informational booklet is designed to provide you with tips and useful information on how you can protect yourself, your family, and your business from on-line and electronic fraud and tech-savvy criminals.

Join us in building a better, stronger, and safer Ontario.

ONTARIO ASSOCIATION OF CHIEFS OF POLICE
OACP

Matthew A. Torigian
CHIEF OF POLICE
WATERLOO REGIONAL POLICE
PRESIDENT – ONTARIO ASSOCIATION CHIEFS OF POLICE

PROPRE CADR UES KPEES YORU IFNORMAITON DISUGISED

Everyday Simply®

Keep private information private by inserting your *Interac*® chip debit card instead of swiping. Only swipe your card if prompted by the terminal. In the unlikely event you do experience fraud, you can count on the *Interac* Zero Liability Policy* for protection.

CYBERCRIME

Cyberspace meets

The term “cyberspace” was first used by Canadian science fiction author William Gibson, and now generally refers to the electronic world created by interconnected networks of information technology and the information on those networks. The Internet is the ‘backbone’ for most of these networks, and is in fact a global ‘commons’ where more than 1.7 billion people are linked together to exchange ideas, services and friendship.

There are various ways to gain access to information in cyberspace, and criminals can exploit vulnerabilities in software and computer hardware by tricking people into opening infected emails or visiting corrupted websites that infect their computers with malicious software. These cybercriminals can take advantage of people who fail to follow basic security practices, such as regularly changing their passwords, updating their antivirus protection on a regular basis, and using only protected wireless networks.

Once they have access to a computer, cybercriminals can steal or distort the information stored on it, corrupt its operations and program it to attack other computers and/or the systems to which they are connected. In many cases, victims suffer a theft of their identity and/or their personal assets.

Criminals now sell information stolen online, such as credit and debit card numbers, login passwords for computer servers, and malicious software designed to infiltrate and damage targeted systems. Even those of us who are diligent in protecting our personal information online are at risk of having our personal data stolen from the third parties we share it with.

online shopping fraud

What is online SHOPPING fraud?

Today you can buy or sell almost anything over the internet…and criminals can use the anonymity of the internet to rip-off unsuspecting buyers and sellers.

For example, scammers may sell a product – often at a very cheap price – just so they can steal your payment card or personal information. They may also take your money and send you a worthless item, or sometimes, nothing at all.

What is online AUCTION fraud?

Frauds at online auctions include **misrepresentation of an item**, **non-delivery of goods and services**, as well as **non-payment for goods delivered**.

The actual auctions can also be rigged. If you are selling a product, the scammer can enter a low bid followed by a very high bid under another name. Just before the auction closes, the scammer withdraws the high bid and the low bid wins. If you are buying a product, the scammer can boost the price using dummy bidders.

You should also be aware of **cheque overpayment scams**. In this type of scam, you are sent a cheque for something you have sold, but the cheque is made out for more than the agreed amount. The scammer hopes you will refund the extra money before noticing that his cheque has bounced.

What to look for...

- Be cautious of items offered for extremely low prices.
- Limited or no feedback rating on sellers.
- Buyers and sellers from overseas.
- Requests to send funds to a third-party company or money service.

Protect Yourself

- Deal with buyers or sellers you know by reputation or experience. If you are not familiar with them, do some research.
- Look for a privacy policy. Be sure you are comfortable with how the company collects, protects and uses your personal information before you submit any details.
- Do not be lured into using payment methods other than the options recommended by the Internet auction site. Be wary of phishing emails that ask for personal or financial information. For more information on phishing, see that section in this booklet.
- Shop only from your home computer. It's much safer than shopping at a terminal in an internet café or library.
- If you plan to buy something, go directly to a store's website by manually typing its address into your web browser. Don't click on links in an email message even if you know who sent it.
- Verify secure connections. Do not enter any financial information on a site if you see a broken key or an open padlock symbol in your browser. This means the transaction is not secure and could be intercepted by a third party.
- Check your bank and credit card statements online, as this allows you to review your payments as they happen rather than waiting until the end of the month to review a paper statement.
- Never give out your social insurance number, date of birth or driver's license number to a seller.
- Before you bid, learn as much as you can about how the online auction works, your obligations as a buyer, and the seller's obligations.
- Remember, if an offer sounds suspicious or too good to be true, it probably is.

Lottery Emails

There has been an ever-growing number of scam lottery emails advising consumers they have hit the jackpot. We ask that you consider the following when you receive a solicitation of this kind.

- You cannot win without first buying a lottery ticket.
- Legitimate lotteries do not notify winners by email.
- They do not randomly select email addresses to award prizes to.
- They do not use free email accounts (Yahoo, Hotmail, etc) to communicate with you.
- They do not tell you to call a mobile phone number.
- They do not tell you to keep your winnings secret.
- They will never ask a winner to pay any fees up front (like taxes or a security deposit) to receive a prize, lottery or sweepstake!
- Remember, if you don't recognize who sent you the email – **delete it!**

OLG is committed to preventing fraud.

Here's why:

At OLG we're building Ontario's trust in our Lottery and Casino games. We conduct our business openly and honestly and provide Ontarians with games that are fair. One way we are doing this is to use a new, revolutionary and powerful analytic tool called Data Analysis and Retrieval Technology (DART) system to detect and prevent potential fraudulent behaviour. We are taking measures to ensure that the right prize goes to the right person, so that Ontarians can enjoy their favourite OLG games with peace of mind. For more information on this or for any questions related to OLG, call us at 1-800-387-0098 or visit us online at www.olg.ca.

Experienced car thieves know they can profit from stealing your car and your identity

Identity theft is a growing target in auto theft.

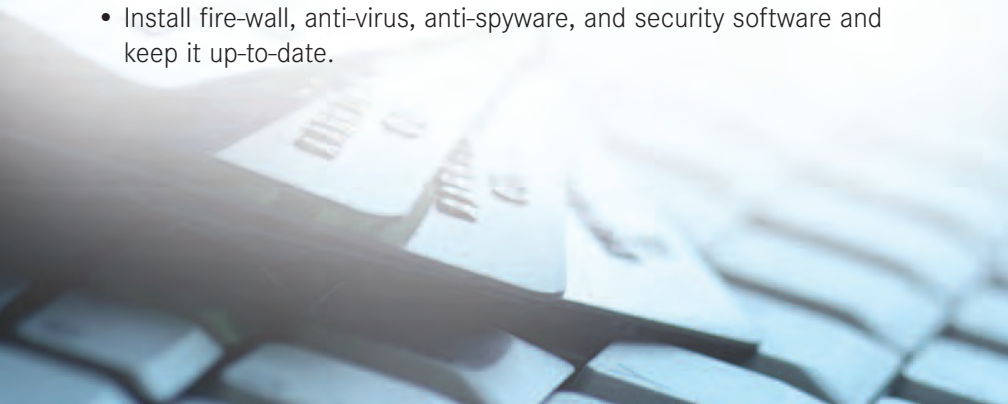
There is a way to fight back: **globali.com®** the next generation of vehicle registration and recovery has added identity protection and restoration services. Vehicle owners, car dealers and law enforcement are now united through a powerful and user-friendly website.

Register your vehicle now and learn more about identity theft protection at globali.com

www.globali.com

Protect **Yourself Online!**

- **NEVER** share your passwords and select a complex password of letters, numbers and symbols.
- Beware of Internet promotions that ask for personal information. Identity thieves may use phoney offers to get you to give them your information.
- After completing any sort of financial transaction online, make sure you sign out of the website and clear your Internet file/cache.
- Before giving your credit card number or other financial information to a business, make sure that their website is protected and secured. Look for a lock symbol located somewhere on the browser or make sure the URL begins with "https://".
- Chain letters and phoney investment schemes try to win your confidence with false promises of incredible returns – they're only after your personal and/or credit information. There are many types of investment frauds and scams. Many are convincing and look very real. To learn more about investing and making good investment decisions, visit www.GetSmarterAboutMoney.ca.
- Teach children to keep their identities confidential in chat rooms, bulletin boards or newsgroups.
- Today the vast majority of young people in Canada use social networking websites such as Facebook. Identity thieves can take simple information such as your birthday or your pet's name, as clues to common passwords and steal your identity.
- Install fire-wall, anti-virus, anti-spyware, and security software and keep it up-to-date.



"I KNOW MY FAMILY IS SAFE BECAUSE MY HOUSE TOLD ME THEY WERE SAFE."

INTRODUCING AN ENTIRELY NEW WAY TO PROTECT YOUR HOME AND FAMILY.

SMART HOME MONITORING FROM ROGERS.

- With remote access you can control your system and receive instant alerts on your smartphone or computer, so you know what's happening at home from anywhere.
- The only system that runs simultaneously on both cable and wireless networks. If one is ever cut or damaged, the other keeps working.
- Your home is monitored 24/7 by certified security experts with 20+ years of industry experience.

ALWAYS CONNECTED.
ALWAYS CLOSE.™

ANOTHER FIRST. ONLY FROM ROGERS™

CALL 1 877 497-6590 or **CLICK** rogers.com/smart

TIPS FOR **PROTECTING YOUR HOME** YEAR-ROUND

There is no better peace of mind than knowing that your home and loved ones are protected. Whether you're at work, in the car or off on a family holiday, there are many ways to maintain peace of mind and keep your home safe.

HERE ARE FOUR USEFUL TIPS COMBINING TECHNOLOGY WITH TRIED-AND-TRUE SAFEGUARDS:

Keep in touch (conveniently)

Asking a trusted neighbour or friend to keep an eye on your home while you're away is a great idea. Smartphones, tablets and laptops provide access to social media almost anywhere at any time. This is a great way to keep in touch with your house sitter, allowing you to get instant updates and also giving you the option to check in at your convenience.

Monitor your home from anywhere

Your smart phone, tablet or laptop can give you access to home security, monitoring and automation services such as Rogers Smart Home Monitoring. These new systems allow you to stay connected to your home from any smartphone or internet connection. For example, you can adjust the thermostat or turn the lights on from your smartphone. You can also receive real-time alerts about activity in your home, including notifications on water leaks, presence of smoke and entry into your home. Systems with remote video allow you to look in on your home anytime you want and get video alerts to your smartphone.

Make sure you're not an easy target

Make sure that your home looks lived in. For example, if you are away in the winter months, arrange to have your driveway and sidewalks shovelled. You may also want to consider having a neighbour park a vehicle in your driveway.

Evaluate options for home security systems

Traditional security systems will alert the security system provider of a break-in using conventional telephone lines – if the phone line gets cut the system may not work and you may not be able to make or receive phone calls during an alarm. Now there are more options available to Ontarians when it comes to home security, including systems such as Smart Home Monitoring from Rogers that is powered by both a cable and wireless connection and does not require a phone line. This means that if the cable line is cut, the system will stay up and running on the wireless network. In addition, if you have a home phone line, it will still be usable during an alarm.

How do I Know if MY IDENTITY has been Stolen?

Some of the signs your identity might have been stolen:

1. Bills and statements don't arrive when they are supposed to – they may have been stolen from the mailbox or someone has changed the mailing address.
2. You receive calls from collection agencies or creditors for an account you don't have or that is up-to-date. Someone may have opened a new account in your name, or added charges to an account without your knowledge or permission.
3. Financial account statements show withdrawals or transfers you didn't make.
4. A creditor calls to say you've been approved or denied credit that you haven't applied for. Or, you get credit card statements for accounts you don't have.
5. You apply for credit and are turned down, for reasons that do not match your understanding of your financial position.

What to do:

- Call your financial institutions and the police
- Put a fraud alert on your credit report
- Contact Canada Post if your mail is missing
- Keep records of steps taken to clear your name and re-establish your credit
- To replace ID cards like health, driver's licence, SIN call 1-800-O-Canada

TitlePLUS® TITLE INSURANCE

titleplus.ca

Buying a house or condo?

Refinancing your mortgage?

Think you might be a victim of fraud?

Have a legal problem with your home?

Consult with your lawyer who is your trusted advisor in real estate matters.*

* The TitlePLUS® title insurance policy is underwritten by Lawyers' Professional Indemnity Company (LAWPRO®). TitlePLUS policies issued with respect to properties in Québec and OwnerEXPRESS® policies do not include legal services coverage.

What is Phishing?

Phishing is typically an email scam which tries to deceive people into thinking a legitimate organization is requesting private information. Also called "brand spoofing," phishing is the creation of email messages and web pages that are replicas of existing, legitimate sites and businesses. These websites and emails are used to trick users into submitting personal, financial, or password data.

What to look for...

- A phishing message is intended to get a quick reaction from you, using upsetting or exciting information demanding an urgent response, or employ a false pretense or statement. Phishing messages are normally not personalized.
- Typically, phishing messages will ask you to **update**, **validate**, or **confirm** your account information, etc., to avoid negative consequences. They might even ask you to make a phone call.
- **The information being sought can include:** Social Insurance Numbers, full name, date of birth, full address, mother's maiden name, username and password of online services, driver's license number, personal identification numbers (PIN), credit card information (numbers, expiry dates and the last three digits printed on the signature panel) and bank account numbers.
- Often, the message or associated website includes official-looking logos and other identifying information taken directly from legitimate websites. Government, financial institutions and online payment services are common targets of brand spoofing. In some cases, the offending site can modify your browser address bar to make it look legitimate, including the web address of the real site and a secure https:// prefix.

How to protect yourself...

- **Be suspicious of any email or text message containing urgent requests for personal or financial information** *(financial institutions and credit card companies normally will not use email to confirm an existing client's information).*
- Contact the organization by using a telephone number from a credible source such as a phone book or a bill.
- Never email personal or financial information.
- Avoid embedded links in an email claiming to bring you to a secure site.
- Get in the habit of looking at a website's address line and verify if it displays something different from the address mentioned in the email.
- Regularly update your computer protection with anti-virus software, spyware filters, email filters and firewall programs.
- A number of legitimate companies and financial institutions that have been targeted by phishing schemes have published contact information for reporting possible phishing emails as well as online notices about how their customers can recognize and protect themselves from phishing.
- Regularly check you bank, credit and debit card statements to ensure that all transactions are legitimate.

If you are aware of a cybercrime or online fraud:

Report it to **info@antifraudcentre.ca** and the associated website or institution – online shopping or auction, charity, or financial institution, etc.

If you have unwittingly provided personal or financial information, follow these steps:

STEP 1

Contact your bank/financial institution or credit card company

STEP 2

Contact your credit bureau and have fraud alerts placed on your credit reports:

Equifax Canada
Toll free: 1.800.465.7166

TransUnion Canada
Toll free: 1.877.525.3823

STEP 3

Contact your local police

STEP 4

Always report phishing. If you have responded to a suspicious email, report it to info@antifraudcentre.ca

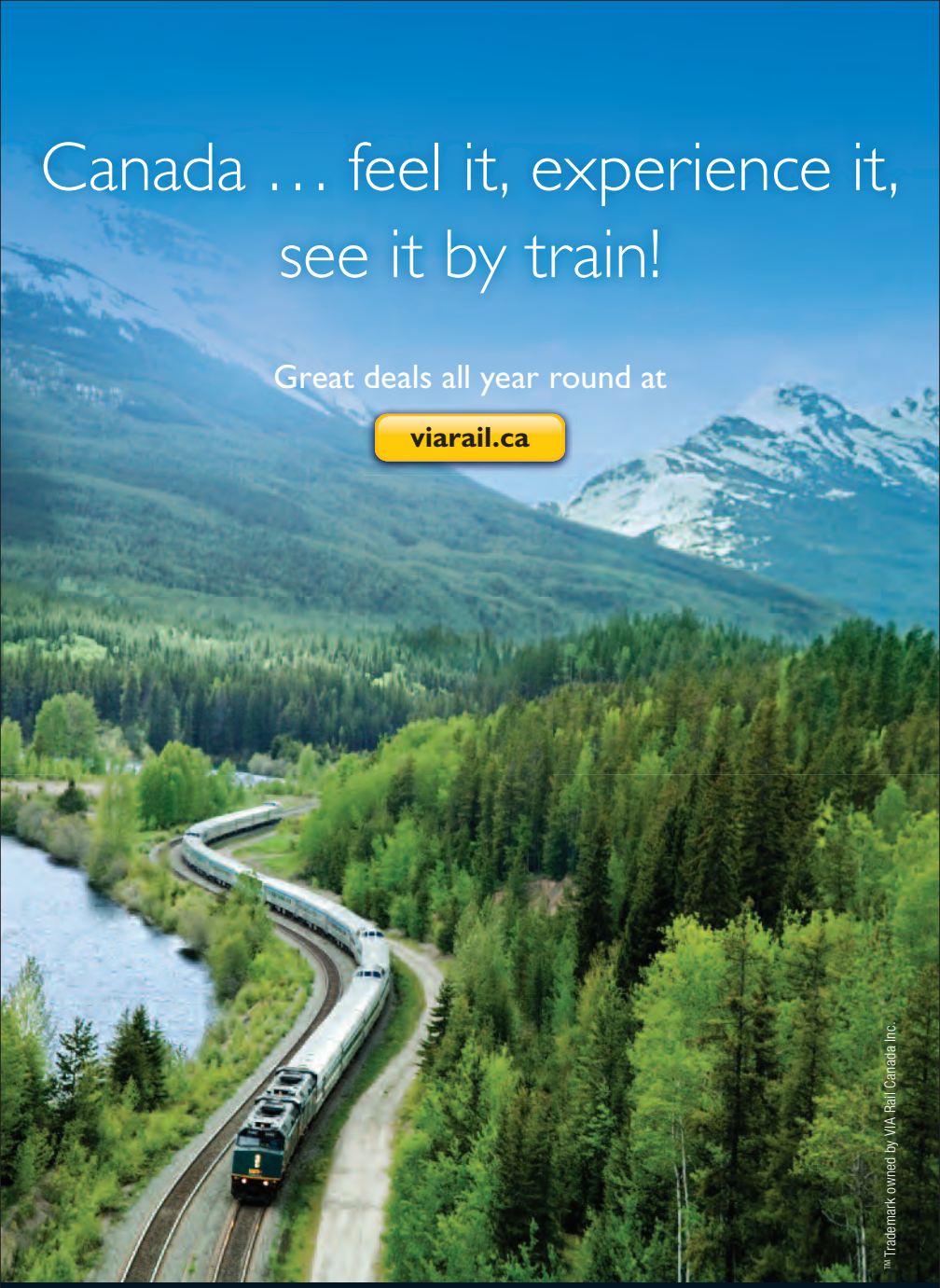
To Learn More…

Canadian Anti Fraud Centre
1.888.495.8501
www.antifraudcentre.ca

Canadian Ministry of Public Safety
http://publicsafety.gc.ca/cybersecurity

Ontario Provincial Police
www.opp.ca

Royal Canadian Mounted Police
www.rcmp.ca


Canada … feel it, experience it, see it by train!
Great deals all year round at
viarail.ca
™Trademark owned by VIA Rail Canada Inc.
A GREEN CHOICE
A MORE HUMAN WAY TO TRAVEL
VIA™
VIA Rail Canada

30 Seconds is all it takes...WITHOUT A KEY.

Protect your vehicle from theft even when at home:

- If you have a garage, use it and lock it
- If you have a rear-wheel drive car, back into driveway
- If you have a front-wheel drive car, park front end first
- Always set the emergency brake
- Never hide a spare key in the vehicle
- Don't leave the ownership or insurance cards in the vehicle when unattended
- Drop business cards or address labels inside doors to assist with vehicle identification

Canpar

EXPERIENCE THAT DELIVERS

CANPAR IS PROUD TO BE ASSOCIATED WITH THE 2012 CRIME PREVENTION CAMPAIGN

www.canpar.com

1-800-387-9335 A TRANSFORCE COMPANY

ACCIDENT SUPPORT SERVICES INTERNATIONAL LTD.

If **YOU** are involved in a collision, COLLISION REPORTING CENTRES *are here to help!*

$1,000 or more combined vehicle damage must be reported to Police.

Report the collision to the Police at the **Collision Reporting Centre** when there are:

- No injuries
- No Criminal Activity
- No Dangerous Goods

Exchange information at the scene, then conveniently report in the safety of your local Collision Reporting Centre as soon as possible. Our professional and courteous staff will guide you through the process with Police, and if you wish to report to your Insurer, they will assist you for convenient "One Stop Service"!

Our "Damage Reported to Police" Sticker program and photographs of all vehicles brought to our Collision Reporting Centres help to prevent insurance fraud.

Accident Support Services has 23 offices across Ontario to serve you!

For more information and
our locations please visit our website
at www.accsupport.com
or call 1-877-895-9111

PROUD TO SUPPORT THE 2012 CRIME PREVENTION CAMPAIGN

HUMBER
School of Social &
Community Services

MAKING A DIFFERENCE

- depth and breadth of **offerings in** the exciting field of **criminal justice**
- from licensing preparatory courses and professional development workshops to certificate, diploma and degree programs

Launch your career or
Advance your professional skills in your current job, or
Prepare for a career change

Develop the competitive edge sought by employers

Diploma and Degree Programs include
- Criminal Justice
- Protection, Security and Investigation
- Community and Justice Services
- Police Foundations

Want further details?
Visit **www.communityservices.humber.ca** or contact
cheryl.evans@humber.ca

Protect what matters most. Hire a Canadian Security Association member today.

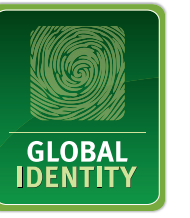
www.canasa.org | 1 (800) 538-9919

CANASA

Canadian Security Association
L'Association canadienne de la sécurité

On behalf of the Ontario Association of Chiefs of Police, I would like to thank the following sponsors and partners for their support in the 2012 Crime Prevention Campaign. If you would like more information on this or any other OACP campaigns, please email oacpadmin@oacp.ca.

Ron Bain
Executive Director, OACP



www.oacp.ca