

IF YOU THINK YOUR IDENTITY HAS BEEN STOLEN

- Start taking notes about what has occurred and steps you've taken.
- Contact the fraud/security department of your creditors for any accounts that have been opened or tampered with. This includes utility companies, credit card companies, banks and other lenders.
- Ensure a "fraud alert" be placed on all your files immediately.
- Contact the two main Canadian credit bureaus:
- Equifax: 1-866-828-5961 and Trans Union: 1-800-663-9980.

TIPS FOR COMPUTER USE

- Never use a public wifi network to conduct for financial transactions and always clear your browser history.
- Change your wifi router password from the factory setting.
- Ensure that you use a robust firewall with the latest "definitions" for the anti-virus software and keep it updated.
- Never open emails from sources you don't know and appear suspicious. Delete them from your inbox.
- Look for websites that begin with https://
- Look for an icon of a lock or an unbroken key.



For more information on crime prevention, scan the following QR code on your smart phone or visit our website at www.torontopolice.on.ca/crimeprevention/



To report a crime anonymously, call Crime Stoppers at: 1-800-222-8477(TIPS) or online at: www.crimestoppers.com

For more crime prevention tips visit: tps.on.ca/crimeprevention

In An Emergency: Call 9-1-1

To report a crime to the Toronto Police that is not an emergency call: 416-808-2222

SP 928-E (2018/10)

IDENTITY THEFT



THE FASTEST GROWING CRIME IN NORTH AMERICA

Identity theft can happen to anyone. This rapidly growing crime effects more people every day in Toronto and around the world.

Yet, surprisingly most people think it will not happen to them. Reasons for this increase include the proliferation of card skimming devices and the hacking of computers.



Reduce The Risk!

Reduce The Opportunity!

tps.on.ca

WHAT IS IDENTITY THEFT?

Someone takes possession of your credit card information, drivers licence, birth certificate, social insurance number, bank account or other personal information for the purpose of taking advantage of your credit rating. Once an identity has been “stolen”, the thieves begin to deplete your finances, leaving you to deal with the financial, legal and psychological costs.

HOW DO THESE THIEVES OBTAIN YOUR IDENTITY?

- Shoulder surfing at automatic teller machines – thieves pick off Personal Identification Numbers (PIN), credit card numbers and/or passwords.
- Dumpster diving, recycling containers and see through garbage bags - thieves rifle through trash looking for loan applications, credit card documents, financial documents and other personal information.
- Theft of personal property such as wallets, purses and private information contained in motor vehicles.
- Hacking of Computers - hackers gain access to computers targeting financial information or expose you to spyware.
- “Phishing” occurs when a fraudster sends you an email disguised as being sent from a bank, company or organization such as Revenue Canada for the purpose of enticing you to click on a link to “update” your financial information.
- Buying Information from dishonest employees working for financial institutions or companies that process financial information. This includes workers at retail stores or medical offices. Stolen records are passed on or sold through chat rooms or instant messaging sessions. Some companies have had their security breached compromising your personal information.
- Mail Boxes - removing your mail or having it redirected to another address or box. Thieves look for new credit cards, pre-approved credit offers, insurance statements, tax information, investment documents and benefit documents.
- Searching Public Sources such as newspapers (obituaries), phone books, online notices and records open to the public.

SIGNS THAT YOUR PERSONAL INFO HAS BEEN COMPROMISED!

- A collection agency informs you they are collecting on an account in your name you never applied for in person.
- You no longer receive all your mail including credit card statements.
- You receive letters and/or telephone calls informing you that you’ve been approved for credit products you never applied for in person.

GUARD YOUR PERSONAL INFORMATION AND DOCUMENTS!

- If any key documents i.e. driver’s licence, social insurance card, birth certificate, passport, bank or credit card are lost or stolen – notify the issuer IMMEDIATELY. Do not delay as the thief will attempt to use the information before it is reported stolen or lost.
- Shred sensitive personal documents before disposing of them.
- Shield the entry of your PIN and never give it to anyone else. Choose a PIN that is not easy to figure out. Do not use your birthdate, phone number or a sequence of numbers and never write down your PINs and carry it in your wallet or in your cell phone. Store these somewhere safe.
- Secure your mail box, lock it if possible. Check your credit card statement when it arrives/investigate if it’s late. Arrange to have a person you trust pick up your mail if you are travelling or go to the Post Office and ask for them to hold mail service.
- Carry only “documents” you absolutely need. This includes your birth certificate, passport and social insurance number card.
- Photocopy your “credit cards” back and front. This will help you if you need to alert the company should they be lost or stolen.

GUARD YOUR PERSONAL INFORMATION ON THE COMPUTER!

- Protect your computer with a start-up password only you know. Never use weak or obvious passwords such as 123456, your birthdate or the word “password”. Do not use automatic login features that save your user name and password.
- Phishing – be on guard for phishing scams by means of phone or internet in which thieves falsely claim to be representatives of legitimate enterprises. This includes:
 - thieves claiming to represent Microsoft or “Windows” and want your computer’s password to fix an alleged problem, or
 - emails that appear to be from a financial institution, Revenue Canada, eBay etc. notifying you of a security breach.
- NEVER click on links they provide to update your information.
- Phishers – simply redirect as many internet users as possible from legitimate commercial websites and lead them to malicious sites that look legitimate. This is done by an “imbedded link” which claims to bring you to a secure site. When users enter their login name and password, criminals can capture this information.