



IDENTITY THEFT

Protect your Personal Information

What is Identity Theft?

Identity theft is someone wrongfully obtaining and using your personal identifying information to commit fraud or theft or for other purposes.

Did you know?

In Canada, in 2006, \$16.2 million was lost to identity theft, almost double from 2005.
-Project Phonebusters (RCMP & OPP)

It takes 12 months, on average, for a victim of identity theft to notice the crime.
- U.S. Federal Trade Commission

In the USA, in 2005, the leading target age groups of Identity Theft victims were 18-29 and 30-39.

- U.S. Federal Trade Commission, Jan 2006

Don't Become a Victim

There are many ways someone can access your personal information:

■ **Mail Theft** – Superboxes and apartment boxes are more of a target than individual mail boxes for mail theft. This may include redirection of mail as well as theft of mail.

- **Vigilance:** be vigilant, and report suspicious activities around mailboxes.
- **Attention:** pay attention if you do not receive mail that you had expected.
- **Regular:** don't let mail build up in your mailbox.

■ Intercepting Garbage

- **Shred Documents:** containing personal information before discarding.
- **Guard Client Information:** businesses must be especially careful for their clients.

■ **Theft of Wallets and Purses** – Your identification is more valuable than the cash.

- **Essential ID:** do not carry unnecessary identification (passports, birth certificate, Social Insurance card).
- **Report Immediately:** any stolen credit and debit cards, driver's license or other ID.

■ **ATM Fraud** – Tampering with automated teller machines (ATMs) and point of sale terminals (POS) enables thieves to read your debit or credit card number and personal identification number (PIN).

- **Known ATMs:** use familiar ATMs.
- **Security Cameras:** ATMs with security cameras are less likely to attract criminals; seek out these machines when possible.
- **Beware Helpful Strangers:** be suspicious if your card is "eaten" by the machine and someone approaches you to say the same thing happened to them, then advises you to enter your PIN again.
- **Avoid After Hours:** limit your after-hours ATM use especially if alone.
- **Watch for "shoulder surfers":** people who watch you enter your PIN.
- **Watch Monthly Statements:** keep an eye on your monthly statement, as well as your balance, & report problems to your bank.

■ Computers

- **Safe Surfing:** provide personal information on secure & trusted web sites &/or certified to be using high encryption.
- **Practice Safe Computing:** do not open suspicious e-mail or share your personal access codes (PAC) for online transactions.
- **Use a Firewall:** Internet Security software to prevent hackers from unauthorized intrusion to you computer & data.



Identity Theft Prevention Tips

- Never throw away **bank records** or other documents in a readable form, shred them instead.
- Never give your **credit card number** over the telephone unless you make the call.
- Never share your **PIN, PAC or other Passwords** with anyone.
- Never ignore your **bank account activity**; reconcile your bank account often and notify your bank of discrepancies immediately. Watch your account activity online.

How is personal information used?

- **Purchases & Withdrawals:** performing transactions with your account(s).
- **Establishing New Accounts:** in your name (and not paying the bills).
- **Changing Mailing Addresses:** so you will not notice a thief's activities.
- **Renting Property:** to be used for illegal activity such as a marijuana grow op.
- **Government Social Programs:** EI, pension, social assistance.
- **Illegal Entry to Canada:** use false identification to avoid prosecution, access government services in your name or allow unwanted visitors to Canada.

How will you know if your identity has been stolen?

- **Credit Card Applications:** you learn of a credit application that you did not make.
- **Missing Mail:** regular statements from banks or credit cards do not come by mail.
- **Unauthorized Payments:** a payment is charged to you that you did not authorize.
- **Defaulted Loans:** a collection agency informs you that you have defaulted on a payment for a purchase you did not make.

“Phishing” & “Spoofing” refers to directing people to web sites either online or by e-mail that look official, but are in fact bogus sites designed to access personal information. For example, if your bank's web site is www.mybank.ca, beware of www.mybank.com; www.my_bank.ca; etc – they may be fake!

“Back doors” or **“Trojans”** are programs that may be loaded onto your computer, usually by e-mail, that enable other computers to access your personal information. The threat can be eliminated by using Internet security programs, such as firewalls & anti-virus software.

What can you do if you think you are a victim?

1. **Bank & Credit Cards** - notify your bank or credit card company IMMEDIATELY.
2. **Equifax** 1-800-465-7166 and Trans Union (877) 525-3823 and request a “fraud alert” be placed on your credit record.
3. **Identity Theft Statement** - go to www.phonebusters.com and complete it
4. **Police** - contact your local police.
5. **Phonebusters** – call at 1-888-495-8501.
6. **Keep a Record** - the dates and times of what you do and who you speak with.

FOR MORE INFORMATION PLEASE VISIT THESE RESOURCES:

- **BC Crime Prevention Association** www.bccpa.org
- **PhoneBusters** 1-888-495-8501 www.phonebusters.com
- **Safe Canada Identity Theft Resources** www.safecanada.ca/identitytheft_e.asp
- **Fight Identity Theft** www.fightidentitytheft.com