The fastest growing crime in North America that targets consumers.

Identity theft can happen to anyone. This rapidly growing crime effects more people every day. Yet, surprisingly most people think it won't or cannot happen to them. The recent increase of this crime is largely due to the development of new technologies such as "card skimming" devices and to criminal involvement in computer hacking. .

What exactly is Identity Theft?

Someone may have taken possession of your credit card information, drivers licence, birth certificate, social insurance number, bank account or other personal information. Once an identity has been "stolen" in this manner the thieves can go on a shopping spree, leaving you to deal with the financial, legal and psychological costs. Frauds, forgeries, applying for loans, mortgages, or credit cards, taking over financial accounts **all in your *name***.

How do these thieves obtain your identity?

Shoulder surfing: at Automatic Teller Machines (ATM) – thieves want to pick off Personal Identification Numbers (PIN), credit card numbers or passwords.

Dumpster diving, re-cycling boxes 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: items such as wallets, purses and vehicles contain private information. Computers contain information about web sites that you have visited, your e-mails and possibly your financial information.

Skimming or Tampering: occurs at automatic bank machines and point of sale terminals. Skimmers enable thieves to read your credit or debit card numbers and personal identification number (PIN) by way of a data storage device. These are often capable of gathering information that can be used to reproduce cards for their personal use at your expense.

Buying Information: 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 are looking 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 and records open to the public.

Guard your personal information and documents.

- If any key documents ie. birth certificate, driver's licence, passport, bank card, or credit card are lost or stolen – **IMMEDIATLEY** notify the issuer and the police. **Do not delay** the thief will attempt to use the information as quickly as possible before it is reported stolen or lost.
- **Shred or destroy** sensitive personal documents before tossing them into the garbage or recycling.
- **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 phone or SIN number.
- **Secure your mail box,** lock it if possible. Know when your bills, financial statements and credit cards are due. Call the company if they do not arrive on schedule. Arrange to have a person you trust pick up your mail. Go to the Post Office and with proper identification ask for their hold mail service.
- **Match records** (financial) to catch irregularities.
- **Photocopy your Credit Cards**, this will help you if you need to alert the company should they be lost or stolen.
- **Carry only Documents** you absolutely need. Rarely do you need your birth certificate, passport or Social Insurance Number card.
- **Protect your Computer** with a start –up password only you know. Do not use automatic login features that save your user name and password.

Guard your personal information and documents.

Phising – essentially this is an old con game updated to take advantage of new technology.
Phising means using mail, phone or internet promotions in which thieves falsely claim to be representatives of legitimate enterprises. They provide you with upsetting or exciting information which demands an urgent response in an attempt to scam the user into disclosing private information.
Example – receiving a bogus e-mail from a company that appears to look legitimate asking for account or PIN numbers.

Pharmers – simply redirect as many internet users as possible from legitimate commercial web sites and lead them to malicious sites that are made to look legitimate.
This is done by a "imbedded link" which claims to bring you to a secure site. When users enter their login name and password, criminals are able to capture this information.

Tips for Computer Use

- Never use a public computer for financial transactions.
- Install virus protection software and update it regularly.
- Be careful what e-mails you open
- Look for web sites that begin with http://
- Look for an icon of a lock or an unbroken key.

CRIME PREVENTION

TORONTO POLICE SERVICE

EMERGENCY

9-1-1

POLICE NON – EMERGENCY

(416) 808-2222

For more information regarding IDENTITY THEFT contact the Crime Prevention Officer at your local Police Division

Working Together to Prevent Crime…

SP - E, 2005/08

IDENTITY THEFT