Identity Theft

A Crime of Opportunity

www.ipc.on.ca

Identity Theft
A Crime of Opportunity

Introduction

Identity theft is a rapidly growing crime that continues to claim thousands of victims each year, with serious consequences. In most cases, victims of identity theft have absolutely no idea they have become victims until it is too late. As part of its responsibility to serve the public, the Office of the Information and Privacy Commissioner of Ontario (IPC) strives to promote education and provide tools and resources to assist the public in protecting their personal information. This booklet offers tips on how to prevent identity theft as well as steps that victims can take to help recover from the crime.

What is identity theft?

Identity theft involves acquiring key pieces of someone's identifying information in order to impersonate them and commit various crimes in that person's name. Besides basic information like name, address and telephone number, identity thieves look for social insurance numbers, driver's license numbers, credit card and/or bank account numbers, as well as bank cards, telephone calling cards, birth certificates or passports. This information enables the identity thief to commit numerous forms of fraud: to go on spending sprees under the victim's name, to take over the victim's financial accounts, open new accounts, divert the victim's mail to the thief's address, apply for loans, credit cards, social benefits, rent apartments, establish services with utility companies, and more.

Why should I care?

According to the Canadian Identity Theft Support Centre, in 2008 the cost of identity theft in Canada was a staggering $7.2 billion dollars and affected approximately 2.25 million people (representing 9.1 per cent of the population)[1].

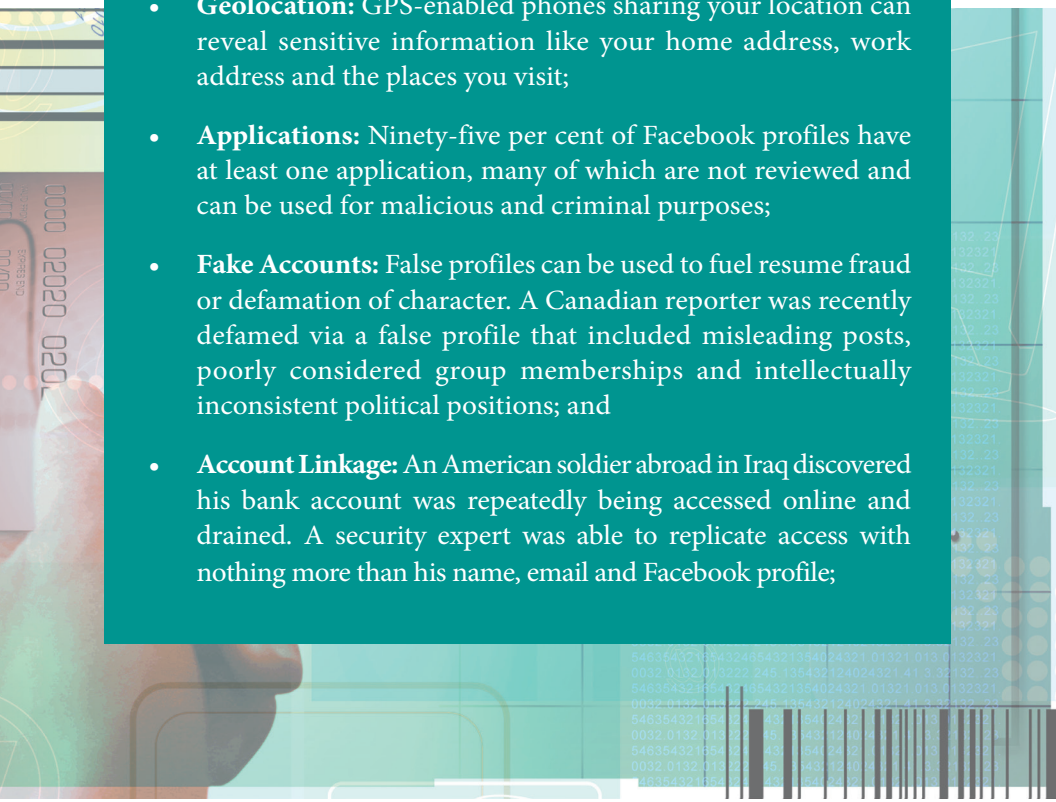
How can my identity get stolen?

Social Media and Mobile Devices

It is important to remember that vulnerability to identity theft lies not in the technology itself, but in how the technology is used. Social media encourages the sharing of personally identifiable information such as: birthday, address, phone number, emails, family members, pet names, high school, and work history.

Here are just a few of the ways your information can get stolen via social media and mobile devices[2]:

- **Phishing:** Phishing attempts using personal information can be used to gain trust in order to obtain non-public information through online conversations;
- **Geolocation:** GPS-enabled phones sharing your location can reveal sensitive information like your home address, work address and the places you visit;
- **Applications:** Ninety-five per cent of Facebook profiles have at least one application, many of which are not reviewed and can be used for malicious and criminal purposes;
- **Fake Accounts:** False profiles can be used to fuel resume fraud or defamation of character. A Canadian reporter was recently defamed via a false profile that included misleading posts, poorly considered group memberships and intellectually inconsistent political positions; and
- **Account Linkage:** An American soldier abroad in Iraq discovered his bank account was repeatedly being accessed online and drained. A security expert was able to replicate access with nothing more than his name, email and Facebook profile;



The theft of your identity can leave you with a poor credit rating and a ruined reputation which may take months or even years to correct. Meanwhile, due to your seemingly dreadful credit history, you may be denied jobs, loans, cheque-writing privileges, or the right to rent or buy accommodation. You may even risk false arrest and have your story viewed with suspicion.

Low-tech Methods

- Lurking around automatic teller machines (ATMs) and phone booths in order to capture PIN numbers (by watching through binoculars as the numbers are being entered, or more simply, by casting a watchful gaze over someone's shoulder). Travellers are a particularly favourite target;
- Stealing mail from mailboxes or redirecting mail in an effort to collect credit cards, bank statements, credit card statements, pre-approved credit offers, tax information or other personal data. Privacy Journal has also pointed out, "how automated credit bureaus freely accept an address change without confirming it or notifying the consumer who is the subject of the file. An imposter can easily have a retail store enter a change of address for a consumer whose identity the imposter has misappropriated, and that is what thousands of credit fraud perpetrators are doing …";
- Illegally obtaining personal credit reports;
- Setting up telemarketing schemes to elicit account numbers from unsuspecting consumers;
- Accessing personal information accidentally sent to the wrong fax number, email address or voice mailbox; and
- Scavenging through the garbage (a.k.a. dumpster-diving) in search of credit card or loan applications, employer's files, and identification/authentication data such as login IDs and passwords. Similarly, thieves can search erased disks for any retrievable data.

Prevention

Steps you can take to avoid identity theft

While consumers may not be responsible for the large-scale occurrences of identity theft emanating from poor data management practices, there are, nonetheless, steps that can be taken to attempt to minimize the risk of becoming a victim of identity theft:

1. Minimize the amount of personal information you give out, especially online;
2. Do not give out your Social Insurance Number (SIN), unless absolutely necessary; never disclose it online; never use it as a password;
3. Keep items containing personal information, such as your birth certificate, passport, citizenship card, etc., in a safe place;
4. Minimize the use of personal information when using social media. Understand the privacy and security settings available and take advantage of them;
5. Guard your mail from theft add a lock to your mailbox;
6. Password-protect your mobile device. Always use strong passwords on your tablet and/or smartphone;
7. Ensure your computing devices are kept up to date with the latest security updates and patches.
8. Be cautious when downloading or using third party applications on your devices and/or social media outlets. Third party applications come with their own set of privacy policies and may be able to access and distribute your personal information upon installation;
9. Pay attention to your billing cycles; carefully review bills and statements on a regular basis; monitor your account balances and activities frequently;

10. Obtain and review your full credit report every year; mark the date in your calendar as a reminder;
11. Notify creditors immediately if your cards are lost or stolen;
12. Obtain a separate credit card dedicated to the exclusive use of your online purchases (with the lowest credit limit possible);
13. Shred all personal records and financial statements instead of just throwing them into the wastebasket;
14. Beware of dumpster divers: ask businesses that you deal with (like car rental agencies) to shred your application forms upon completion of their use;
15. Ask companies that print your entire credit card number on the sales receipt to consider truncating the number (so it doesn't appear in its entirety); and
16. Be very wary of responding directly online to any email request for personal information sent by online service providers (phishing), or an alleged superior within your organization (spear-phishing). Instead, contact the institution or sender through another communication channel – call them by phone, using a pre-existing number.

Victim Support

If you have already become a victim:

1. Immediately report the crime to the police; keep a copy of the police/occurrence report;
2. Armed with the police occurrence report, advise all businesses with whom you have a relationship of the possible loss, theft, or misuse of your identity. Ask for stronger security measures — have a fraud alert placed on your accounts; start with the credit bureaus;
3. Cancel all your existing cards and accounts, and open new ones;
4. Document all the steps you have taken and your expenses to clear your name and re-establish your credit;
5. Have your credit reports annotated or possibly "frozen;"
6. Contact the post office if you suspect that someone is diverting your mail through false change of address forms;
7. Consider telling your employer, as an added precaution;
8. Keep a log of all your contacts and make copies of all documents. You may also wish to contact a privacy or consumer advocacy group; and
9. In some cases, it may be advisable to seek the assistance of a lawyer.

What organizations can do

Organizations have an equal, if not larger role to play than consumers when it comes to preventing identity theft. We make the following recommendations (especially applicable to financial and public sector organizations):

- When information systems are being designed or upgraded, consider how user-privacy could best be protected;
- Absent legislation, adopt a privacy policy for your organization and train all employees on responsible information handling practices;
- Exercise considerable caution when collecting, using, and disclosing SINs. Do not ask for these numbers if not required by law. Avoid the use of SINs as client/employee/student identification numbers;
- Consider storing the textual portion of a record (i.e., clinical encounter data in a health record) separately without any personal identifiers; retain identifying information (such as name, SIN, address, date of birth) in a separate database, preferably in encrypted form. Organizations can also separate the flow of personal data from other transactional data in their information systems;
- If you are a credit bureau, provide your customers with a free credit report annually, upon request, and notify customers whenever their credit reports have been accessed;
- Require proof of identity and check it carefully when a customer applies for credit or a change of address. Credit bureaus should not accept client address changes from creditors without first verifying them with the consumer involved;
- Make use of artificial intelligence programs to identify patterns of fraudulent use and notify consumers of any suspected fraudulent activity. Creditors have a responsibility to report fraudulent accounts to the police and ensure that they are deleted from a bona fide client's record;
- Do not use customers' personal information for "secondary purposes" such as adding it to mailing lists or selling/leasing it to third parties, without the explicit consent of the individual concerned;

- Store and dispose of personal information accurately and securely, especially credit and loan application forms;
- Avoid using date of birth or mother's maiden name as passwords for financial accounts. This type of information is often quite easy for others to acquire; and
- Do not put scanned copies of anyone's signatures on your organization's website.

Summary

The theft of your identity can pose a serious threat to your privacy and has the potential to make your life very difficult. As a result, the problem of identity theft must be fought on several fronts. Moreover, as technology makes it easier to gather your personal information, it becomes evermore important to ensure privacy is the default setting.

Resources

Canadian Identity Theft Support Centre
http://idtheftsupportcentre.org

Canadian Anti-Fraud Centre
http://www.antifraudcentre-centreantifraude.ca

Ontario Provincial Police
http://www.opp.ca

Identity Theft 911 (IDT911)
http://idt911.com

Notes

1. *Canadian Identity Theft Support Centre: http://idtheftsupportcentre.org/id-theft/*
2. *Entrepreneurs' Organization: http://bit.ly/bHMKtK*

About the IPC

The role of the Information and Privacy Commissioner is set out in three statutes: the F*reedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

For more information:
Information and Privacy Commissioner
Ontario, Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 CANADA

Tel: 416-326-3333 or 1-800-387-0073
Fax: 416-325-9195 TTY: 416-325-7539
info@ipc.on.ca www.ipc.on.ca

Cette publication est également disponible en français

Updated: July 2014