

Personal Information Protection and Identity Theft Prevention Tips (Canadian edition)

Top 30 Best Practices for Privacy Protection

An Informatica Security Research White Paper

Author:

Claudiu Popa,
President & Principal Risk Advisor,
Informatica Corporation

30

PERSONAL INFORMATION PROTECTION AND IDENTITY THEFT PREVENTION TIPS



DO:

1. Understand the value of your own personally-identifiable information. To anticipate and prevent corporate identity theft, be aware of the information required to impersonate a company (incorporation number, business number, bank account numbers, corporate credit cards, etc). Always think about controlling the risk: it's better to be safe than sorry: Once confidential information is compromised, it can only rarely be recovered.
2. Know your rights. Canadian law requires individual consent for collecting, sharing and managing your personal information. It also gives you the right to access that information, correct it and file complaints with the Privacy Commissioner of your province if you feel you need to.
3. Understand that not all attacks on your privacy and security use technology. The most effective ones are simply humans asking for information. This is politely called social engineering.
4. Pay closer attention when interacting with large organizations that collect and traditionally manage large amounts of personal and client data. Banks and financial institutions, telecommunications firms, government offices and healthcare facilities.
5. Remember that both privacy and security are entirely dependent on the weakest link. Just because an organization has a policy in place doesn't mean anyone follows it or its staff is even aware of it.
6. Pay particular attention when interacting with smaller organizations that do not visibly disclose their privacy practices and appear to leave personal records lying around on desks and in garbage bins.
7. Ask about their systems and their incident management procedures even if you don't feel you're an expert. Explain that you are concerned about identity theft and personal privacy. The responses to questions about privacy and security are often interesting. If you're told that there has never been any security or a privacy issue, it's a good indication that they just don't monitor these activities and may compromise your data without even knowing it. Be sure to retain their privacy officer's contact information.
8. Destroy personally identifiable records, printouts, bank statements, credit card receipts, offers and cheques before discarding them. Follow these best practices at work and at home; corporate identity theft is just as popular as personal identity theft. Always take your credit card receipts with you, never discard them in public.
9. Check your credit history report at least once a year with any of the major Canadian credit bureaus responsible for providing this kind of service for free. Do it all at once or spread out the reports throughout the year.
10. Remember: mail theft is a crime, discarded garbage is not. Use a lockable mailbox to prevent the theft.
11. Avoid using the same password twice. A good password is easy for you to remember but nearly impossible for anyone else to guess. Use a password management program if you need to keep track of numerous passwords or require a random password generator. Avoid easily identifiable PINs (i.e. date of birth).
12. Ensure that your computer is not only free of viruses but also spyware and key logging software designed to steal passwords to banking, gambling, auction and other restricted sites. Once lost, it's difficult to find out about these breaches until it's too late.
13. Take note of your surroundings to ensure that no one is about to steal your belongings or is shoulder surfing as you're using your computer, entering codes into a bank machine, etc. Use a privacy screen and anti-theft device with your laptop.
14. Recognize the signs that you are (or your company is) a victim of identity theft: you've been informed, approved or declined by a creditor regarding an application for credit you know nothing about; a collection agency is collecting on an overdue account you have nothing to do with, you're missing pieces of mail such as financial statements; you notice unauthorized transactions on your bank, credit card or phone statement. Challenge any such transactions in a timely manner.
15. Keep a list of all your credit cards, credit accounts and bank accounts in a secure place so you can quickly call the issuers to inform them about missing or stolen cards. Include account numbers, expiration dates and telephone numbers of customer service and fraud departments.



DON'T:

- 1.** Give away information about yourself unless you have verified the identity of the party that is requesting it. Never give out personal information and details (i.e. social insurance number, driver's lic., bank accounts, etc) over the phone.
- 2.** Succumb to phishing attacks. These social engineering tricks impersonate your bank or trusted online company, introduce some urgency (i.e. your account is about to close), ask you for your password and even bank card code. Most will even ask you not to attempt to log in again afterwards, thus giving them time to actually use the stolen information.
- 3.** Legitimate companies do not require the verification of your confidential account details. Do not respond to requests for verification of your (or your company's) details.
- 4.** Hesitate to ask for the written privacy policies in effect at any place of business that uses your information, along with the contact information of the Chief Privacy Officer. This individual is individually responsible for satisfying your requests for information about the organization's data collection practices and remediation activities in case of a breach.
- 5.** Do business with any organization that you don't feel comfortable with. Personal and confidential information is very valuable and if you lose it, it can very rarely be recovered. By law, companies cannot penalize you for not disclosing personal details if they are not required for the specific purpose under discussion. In fact, it is illegal to ask for it and collect it if it is not material to the activity being carried out.
- 6.** Carry unnecessary pieces of identification with you such as numerous credit cards, passports or birth certificates, to limit the amount of information that could be stolen.
- 7.** Open emails from people you don't recognize. Keep your preview pane closed, use anti-spam software and do not allow your emails to automatically make outbound connections through your firewall.
- 8.** Click on links in emails or instant messaging windows. Type or paste them directly into your browser to increase your chance of noticing phishing scams (suspect URLs) and Trojan infections. Only access your important sites from the (SSL-encrypted) login pages that you have previously verified and bookmarked.
- 9.** Stray. When it comes to the Web, stay on the beaten path. Underground sites and sites with questionable content generally have fewer scruples about exposing visitors to malicious code and privacy breaches.
- 10.** Fall for letters from companies that send notices about your expiring domain name. The letter itself may not be from your registrar and by responding, you're actually switching from a trusted company that was managing your Internet domain to an unethical company seeking to profit from your confusion. This can disrupt your company's operations in a serious manner as all your web traffic and emails depend on a domain name.
- 11.** Leave your purse, wallet, laptop, cell phone or PDA unattended or within reach of anyone. The information they contain and their capabilities will often result in a privacy or security breach that is difficult to recover from.
- 12.** Allow any institution to use your social insurance number or credit card number as an identifier on any account.
- 13.** Give out your Social Insurance Number liberally. Although it is tied to your identity, it is not a piece of identification. If offered the choice by an authorized organization, choose to use a different form of ID. According to the Office of the Privacy Commissioner, your SIN can be used to steal your identity. Along with other personal information, someone may be able to use your SIN to apply for a credit card or open a bank account, rent vehicles, equipment, or accommodation in your name, leaving you responsible for the bills, charges, bad checks, and taxes.
- 14.** Delay. If you're sure of being the victim of identity theft, fraud or a privacy breach and you have requested the cancellation of old cards be sure to have a complete list of contact numbers and addresses for all issuers and departments that need to be aware of your new identity credentials. For example, if you have obtained a new Social Insurance Number (make sure you don't request a new one unnecessarily) you'll need to contact all your financial institutions, creditors, pension providers and employers and ask them to update their past and current records on your file.
- 15.** Panic! Make sure that it was not a mistake and that you are indeed the victim of fraud, identity theft, personal information compromise or security breach. If so, report the incident to the police and make note of the complaint number, ask each major credit bureau to add a fraud warning to your credit file to ensure that all credit requests are verified through you first. If necessary, report all stolen cards to the issuers and verify all activities in writing. Notify your bank of stolen cheques, cards or compromised accounts. Notify your postal inspector if you suspect mail theft.

Informatica Corporation provides information security consulting, services and technology. With over 18 years in the business, Informatica is a recognized industry innovator and its certified professionals are trusted business advisors. Services include executive consulting, information risk management, complete training programs, decision support and standards-based risk assessments.

Copyrights and trademarks of Informatica Corporation (www.InformaticaSecurity.com) include: FlexSecure Verify (audits, analysis and assessments), FlexSecure LockDown (managed security), FlexProtect (corporate security support) WorkLife Security Education.

For More Information

Email: info@InformaticaSecurity.com

Web: www.PrivacyandSecurity.ca

Informatica Corporation
1 Yonge Street, Suite 1801
Toronto, ON M5E 1W7, Canada

We welcome media enquiries and requests
To share and/or distribute this document.

References

1. How to Submit a Complaint to the Privacy Commissioner of Ontario
<http://www.ipc.on.ca/index.asp?navid=36>
2. How to Submit a Complaint to the Privacy Commissioner of Canada
http://www.privcom.gc.ca/contactUs/index_e.asp
3. Information About Protecting Your Social Insurance Number
http://www1.servicecanada.gc.ca/asp/gateway.asp?hr=en/cs/sin/0300/0300_in016.shtml&hs=sxn#html
4. What To Do In Case Of Social Security Number Theft or Loss
<http://www.servicecanada.gc.ca/en/sin/lost/lost.shtml>
5. Free Password Management Software
<http://passwordsafe.sourceforge.net/>
6. Free Credit Report Information from Equifax
http://www.equifax.com/EFX_Canada/consumer_information_centre/ownreport_e.html
7. Free Credit Report Information from Experian
<http://www.experian.ca/intl/canada.html>
8. Free Credit Report Information from Trans Union
https://www.tuscores.ca/content/page.jsp?id=tucanada/common/data/en_CA/ps/orderbymail.xml&locale=en_CA
9. Privacy Awareness Education from Informatica
<http://www.privacyeducation.ca/>
10. Corporate Information Privacy Assessments from Informatica
<http://www.privacvassessments.ca/>