

Avoiding Identity Theft: Critical Steps to Take

As on-line and off-line consumers, we are constantly prompted to disclose our personal information to organizations. But with each disclosure comes the risk that one's information will be mismanaged, accessed without authorization or stolen. In fact, it is estimated, that about one in 10 Canadians has been a victim of identity theft. As personal information becomes an increasingly valuable asset, it is important for individuals to take their privacy seriously. By simply following some of the following key steps, you will be in a much better position to protect your information and identity.

- 1. Your On-line Presence** - The importance of choosing strong passwords cannot be overemphasized. When creating passwords, avoid a commonly used nickname, family member or pet's name, or your on-line screen name. Instead, use a phrase or a series of letters and/or numbers (at least 8) that you can easily remember but that would be hard for others, including password sniffers, to guess. - Look for privacy policies on the websites you visit, particularly if you will be entering your information on the site. You need to understand with whom your information will be shared, and how it will be secured before providing it. - Be extremely cautious when providing credit card or other sensitive information on-line. Only provide such information on a secure site. Always check for a lock symbol at the bottom of your browser page and the letters "https" in front of the organization's Web site address to confirm information is encrypted when transmitted to the organization's server. - If you are especially concerned about protecting your privacy on-line, there are an increasing number of programs being offered, such as Anonymizer, that enable consumers to make transactions on-line through third parties and keep their personal information private.
- 2. Understand and Manage E-Mail Risks** E-mail has become a preferred method of communicating, but what comes in or leaves your e-mail server may introduce information risks. Here are some things you can do to minimize these risks: - E-mail is like an open postcard - it's possible for someone who is not the intended recipient to access your e-mail using a simple e-mail sniffer. Never send highly sensitive information like credit card details or medical information through an unencrypted e-mail. - As soon as you see spam (bulk, unsolicited e-mail messages), delete them immediately. Don't click on any embedded links, don't buy anything, don't even reply by asking to unsubscribe. Keep in mind that any response or activity keeps spammers coming back. - No matter how exciting or dreadful the news, always be skeptical of e-mails requesting password updates or your financial information. - Never open an e-mail attachment unless you are expecting it from someone you trust. - Make sure to install and regularly update antivirus and anti-spam software. Also, an up-to-date firewall will reduce the risk of an intrusion. - Protect your e-mail address as best as possible by setting up one e-mail for your trusted personal and business contacts, and a separate one for other on-line usage.
- 3. Be Diligent when using a Fax Machine** In order to reduce the risks associated with faxing out personal information (such as dialling a wrong number, having your fax picked up by the wrong individual, or having your fax sit in an insecure location), try to adopt the following measures: - Only fax personal information that needs to be sent out immediately, and call to confirm its receipt. - If you wouldn't feel comfortable discussing the information over the telephone, chances are it's best not to fax it either. - If its sensitive information, check to see if the recipient has a password feature on their fax machine, ensuring that only authorized recipients are able to access what you've sent over.
- 4. Limit the Personal information you Provide** To place a limit on where your personal information ends up, you can do the following: - When signing up for a reward points program or completing a sales agreement, understand how your information will be used. Carefully check to see if your contact information will be sent to a marketing list or "affiliated" companies. You may need to check a box in order to prevent the transfer of your information. - Remember that you never need to provide information to an organization if its not essential to the provision of products or services to you. For example, a retail store cashier or a warranty card may collect information for marketing purposes - you don't need to provide it.
- 5. Safeguard your Identity** There are a number of additional proactive steps consumers can take to ensure their personal data is protected: - Never carry more personal information with you than is necessary. In particular, leave your SIN card and passport at home. - Choose complex PIN numbers, memorize them well, change them often and do not write them down in a place that is easily accessible. Make sure to always shield yourself when keying in a PIN at a store or bank machine. - Obtain an annual credit report from a credit reporting agency to ensure there are no suspicious activities. - Consistently check your bank, credit and debit card statements to ensure all account activity is legitimate. - Invest in a good quality cross-cut shredder. Shred documents containing personal information you no longer need. - Always remove your mail promptly from your mailbox so as to prevent identity thieves from finding and recording any personal information. With identity theft on the rise, safeguarding personal information is not just an organizational responsibility. In our day to day interactions, we as consumers must make a firm commitment to taking steps to protect our personal identity.

About the Author

Fazila Nurani is a privacy consultant, attorney and lead trainer with PrivaTech Consulting (<http://www.privatech.com>). She advises organizations on privacy best practices. Visit our homepage to download a report on the five key steps that consumers must take to avoid an invasion of their privacy.

Source: <http://americanahost.com>