

# Identity Theft: Protect Yourself

**Consumers must remain vigilant and understand the role they have to play in preventing identity theft. Here are some tips from the Canadian Bankers Association and Phonebusters.**

- Do not give out personal information on the phone, through mail or over the Internet unless you have initiated the contact or know whom you're dealing with.
- Keep the amount of identification that you carry with you to a minimum. For example, you don't need to carry your birth certificate or social insurance card with you if you're just going out shopping. Instead, keep them in a safe place.
- Protect your personal information. Keep items with personal information in a safe place and watch what you throw out or recycle. An identity thief will pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers you get in the mail.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.
- Don't give out your SIN card number or carry it with you. Use other forms of identification when possible.

---

**There are also steps you can take to ensure that your personal information is protected while you're online, including:**

- Use common sense and be aware of potential security leaks. You wouldn't give information to just anyone in the off-line world. Apply the same discretion online.
- Change your passwords regularly, use hard-to-guess passwords (e.g. using a combination of letters and numbers), and never share your password with anyone.
- Look for a company's privacy policy or link to its privacy statement when you visit its website. Pay attention to what information the company gathers, how it's used, and with whom it's shared.
- Always ensure you're in a safe environment. Look for the closed-lock or unbroken-key icons on your browser when entering your credit card number or other sensitive data. If you don't see the unbroken key or closed lock, or if the key is broken or the padlock is open, your transaction is not being securely transmitted across the Internet. When you send messages insecurely, someone outside of the organization you are sending to could intercept your information.
- Clear the cache of your browser after visiting secure sites. This will ensure that nobody else can view any confidential information you may have transmitted.
- Be familiar with the encryption level of your browser and what it means to your privacy. Many businesses require that you use 128-bit encryption to access secure websites. Update your Web browser on a frequent basis to ensure you are using the latest browser technology and the highest encryption level.
- Install and maintain a firewall to guard against unwanted access to your computer and make sure you have the latest anti-virus software installed.
- Be suspicious if you receive e-mail from a business or person requesting personal information. Be particularly suspicious of e-mails that direct you to websites that request your password, Social Insurance Number, or other highly sensitive information. You may wish to call the organization to verify the legitimacy of the request.
- Be careful when downloading files from the Internet and installing programs. Also, take care when reading e-mail with attachments – e-mail is often used to transmit viruses.