

Information Security Newsletter

Brought to you by the Information Security Team

January 2009

If you have questions about information security, please contact the Chief Information Security Officer:

Peter Subar

(416) 382-4945

psubar@its.jnj.com



Top 10 Tips for Identity Theft Prevention

An identity thief takes some piece of your personal information and uses it without your knowledge. The thief may run up debts or even commit crimes in your name. The following tips can help you lower your risk of becoming a victim.

1. Protect your Personal Information

Don't carry your extra credit cards, birth certificate, Social Insurance Number card or passport in your wallet or purse except when necessary. This practice minimizes the amount of personal information a thief can steal in the case of a lost wallet or purse.

2. Fight "phishing" – don't take the bait!

Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, via e-mails and regular mail. Don't give out your personal information – unless you initiated the contact. Don't respond to a request to verify your account number or password. Legitimate companies will not request this kind of information in this way.

3. Keep your identity from getting "trashed".

Never discard credit card receipts or other documents containing personal information in a public trash container – use a shredder. Do not discard pre-approved credit card offers or "convenience checks" that you don't use in the trash without first tearing them into small pieces or shredding them.

4. Control your personal financial information.

Canadian privacy laws require your bank and other companies providing financial services to get your permission before sharing your personal financial information with outside companies. You also have the right to limit the sharing of your personal financial information between your financial institution and their affiliates. Write to your bank and tell them you want to "opt-out".

5. Shield your computer from viruses and spies.

Protect your personal information on your home computer. Use strong passwords with at least eight characters, including a combination of letters, numbers, and symbols, easy for you to remember, but difficult for others to guess. Use firewall and virus protection software that you update regularly. Download free software only from sites you know and trust. Don't install software without knowing what it is. Set Internet Explorer browser security to at least "medium." Don't click on links in pop-up windows or in spam e-mail.

6. Click with caution

When shopping online, check out the Web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. If there is no privacy policy posted, shop elsewhere. Only enter personal information on secure Web pages with “https” in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted, protecting it from hackers!

7. Check your bills and bank statements.

Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Scrutinize your utility and subscription bills closely to ensure the charges are yours and are accurate.

8. Theft is a crime of opportunity – prevent theft!

Install a lockable mailbox at your residence to reduce mail theft. Never leave your purse or wallet unattended at work, church, fitness club, restaurant or shopping cart. Never leave your purse or wallet in open view in your car even if your car is locked. Destroy all cheques immediately after you close a chequing account. If you move, do not have your bank send your new cheques to your home address. Tell the bank you prefer to pick them up instead.

9. Ask questions.

Ask questions whenever you are asked for personal information that seems excessive or inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. You have the right to ask questions. If you're not satisfied with the answers, consider going somewhere else.

10. Credit Monitoring

The best way to protect yourself from identity theft is to monitor your credit history regularly for unauthorized activity.

Order a copy of your credit report from a different credit-reporting agency every four months. Check out the following sites:

<https://www.econsumer.equifax.ca/ca/main?link=OPIEM&lang=en>

http://www.transunion.ca/ca/home_en.page

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of Johnson & Johnson. If you want advice on a particular incident, you should consult an attorney or other expert.