

Internet Fraud – Don't be a Victim!

by John Bryson

Online fraud evolves on a daily basis. You can never be too careful with your personal information.

Always think about why a website would need to know information it is requesting. Only the government should ask for your Social Insurance/Social Security Number to identify you. Who really needs your real birth date? Here are a few more tips to protect your identity and your financial information:

1. Make sure your computer is protected with a firewall, anti-virus/anti-spyware software and that you run the Windows and application software updates regularly. The updates are often to fix “holes” in the software that allow hackers to gain access to your system.
2. Run backups of your system regularly and store them safely – eg on a separate external hard drive, on a USB flash drive or on a **secure** website.
3. Use common sense. The Internet is a wonderful place to do research and while much of the information is from reliable sources, much of it is not.
4. Be wary of “free” or “cheap” online offers. If a website is selling something at a much lower cost than others or than the items are being retailed at, don't be greedy. It may very well be a “phishing” expedition. Phishing is an amalgamation of the two words "password" and "fishing." It is a way of scamming consumers into providing their personal information such as online banking details and passwords.
5. Unsolicited emails and instant messages should also be disregarded – especially if they ask you to click on something or follow a link. If your bank needs to contact you, they will call you and you should always get the person's name and tell them you will have to call them back. Call the number in the phone book for your bank and ask for that person. If it was a legitimate call, the bank personnel will understand your caution and applaud you for it.
6. Choose strong passwords. Microsoft recommends:
 - a. **Length.** Make your passwords long with eight or more characters.
 - b. **Complexity.** Include letters, punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. The greater the variety of characters in your password, the better. However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing "and" to "&" or "to" to "2."

- c. **Variation.** To keep strong passwords effective, change them often. Set an automatic reminder for yourself to change your passwords on your email, banking, and credit card websites about every three months.
 - d. **Variety.** Don't use the same password for everything. Cybercriminals steal passwords on websites that have very little security, and then they use that same password and user name in more secure environments, such as banking websites.
- 7. Provide credit card and bank information **ONLY** on reputable and secure Websites.
 - a. Check for the “lock” icon – the picture of a padlock.
 - b. Click (or double-click) on the padlock icon to see details of the site's security. This is important to know because some fraudulent web sites are built with a bar at the bottom of the web page to imitate the lock icon of your browser! Therefore, it is necessary to test the functionality built into this lock icon. It is very important to **know your browser**. Check your browser's help file or contact the makers of your browser software if you are unsure how to use this.
- 8. Make sure you type financial institution and shopping websites correctly to ensure you don't go to a site that looks like the right one but is actually a mock-up based on a common typo. If there is anything about the webpage that seems a bit off, close your browser and type the site in again. It may have been updated OR it may not be the right site.
- 9. Use encrypted connections for transmitting personal data like credit card and banking info and make sure you log off properly (if you have a wireless network at your home, enable the security or anyone driving by with a laptop could access it as could your neighbours). It is also a good idea to manually delete your browsing history (for example, in Internet Explorer, you would go to the Tools pull-down menu, Choose Options and Delete Browsing History).
- 10. Review your credit card bills and bank statements thoroughly to make sure you have only been charged for transactions you actually performed. Call the bank or credit card company immediately if you do not recognize a charge/debit.
- 11. Be careful when using free WiFi sites like those in hotels, coffee shops, airports. Don't do shopping or banking in these locations and be very careful if accessing your email as well.
- 12. NEVER say yes to “Remember this Password” or “Remember me on this Site” etc. If your computer is ever stolen, the thief will have access to it all.

Follow these common-sense precautions and your chance of becoming a victim will be much reduced.

Practice prevention and enjoy peace of mind.

© 2012 John Bryson
Safe Home Security, East LaHave Nova Scotia
www.safehomesecurityns.com