Concerned about the safety of your personal and financial information?

While RBC® employs rigorous security and technological safeguards, you can help too. Here's how!

Top 10 tips to safeguard your assets

1. **Keep your personal information safe.** An identity thief will pick through your garbage or recycling, so be sure to shred receipts, copies of credit applications, insurance forms, etc.
2. **Keep personal information confidential.** Do not give out personal information on the phone, through email or the Internet unless you initiated the contact and know who you're dealing with.
3. **Be aware of billing and statement cycles.** If your bills or statements don't arrive on time, follow up immediately to ensure they have not been fraudulently redirected. Request electronic statements.
4. **Protect your mail.** Bring in your mail daily. Forward or re-route it if you move, change your mailing address or are away.
5. **Protect your PIN and passwords.** Do not reveal your PIN or passwords to anyone, including employees of RBC, family and friends. When conducting a transaction, keep your card within sight and shield the keypad when entering your PIN.
6. **Limit your risk.** Sign all credit cards as soon as you receive them. If they are lost or stolen, report it immediately.
7. **Unusual transactions.** Beware of "too good to be true" or unexpected offers or requests such as, "You've inherited a large sum of money. To claim it, send us a deposit first." Never agree to conduct financial transactions on behalf of strangers.
8. **Review your transactions.** Regularly review your financial statements to ensure that all transactions are authorized, and report any missing or fraudulent ones. Review your credit bureau file annually.
9. **Limit your exposure.** Only carry credit cards you use. Don't carry your birth certificate and social insurance card when you don't need them, instead keep them in a safe place.
10. **Contact the authorities.** If you suspect you are a victim of fraud or theft, contact the authorities immediately.

For more information on fraud or our privacy policy, call 1-800-769-2511 or visit www.rbc.com/privacysecurity/

RBC®

Top 10 tips for safe computing and online privacy

1. **Protect your personal information.** Be aware of schemes that ask for personal or financial information. Do not respond to unsolicited requests for confidential information.

2. **Choose effective passwords.** Choose passwords that are difficult to guess but easy for you to remember. Use multiple passwords, change them frequently and use ones that include a mix of letters and numbers: all essential components of online safety.

3. **Verify a message before you take any other action.** Do not click on a link, call a phone number, wire money or take any requested action, unless you first verify that a request is legitimate. Verify it using information from a source other than from within the message itself.

4. **Limit the online information that you make available about yourself.** Be careful about including personal information online, on social networking sites, in chat rooms and in unencrypted email, as fraudsters may try to get at your information for their own benefit.

5. **Be cautious in your online activity.** Be aware that email scams and malicious websites quickly surface for publicized or recurring events or when any news story breaks. Use caution when accessing new sites.

6. **Be wary of pop-up windows.** Don't click on any action buttons within a suspect pop-up window, including those requesting financial or identification information and those offering to sell you something.

7. **Maintain a suite of security software products.** This should include a reputable personal firewall, anti-virus, anti-spam and anti-spyware, all necessary to provide online protection for your computer and your information. Beware of pop-up warnings that your computer is infected and instructing you to buy or download software to fix the problem.

8. **Keep your computer healthy.** Take advantage of automated updates for your web browser, operating system and for all software that supports your online behaviour, e.g. browser plug-ins such as PDF viewers, or regularly check the applicable websites for required software patches and updates.

9. **Remember to log off.** Ensure you properly log off and close your browser to prevent others from being able to view your information later.

10. **If it looks too good to be true, it probably is!** Be cautious of emails and websites that promise incredible deals and monetary windfalls. You may end up giving your financial information to fraudsters or downloading malicious software by clicking on a tempting link.

To learn more, visit www.rbc.com/privacysecurity/

07744 (02/2010)