Cyber security – strategies for staying safe online

Wealth Management

Today's fraudsters are becoming more sophisticated all the time. That is why it is more important than ever to protect your personal information when corresponding online and via email.

Avoid email fraud

Beware of "phishing" emails asking for personal information, such as credit card, account or social security numbers. Typical phishing emails use an urgent reason for providing information, such as a security breach or contest, to trick you into responding. And they often include links to websites that may appear to be legitimate. These websites may even contain RBC banners and logos in an attempt to fool you.

Do not take the bait — do not click links or reply to the message. Because RBC will never, under any circumstances, send you an unsolicited email asking you to update or verify your account details or other personal information by clicking a link or calling a phone number provided.

If you receive such an email, do not respond. Instead, please notify us by forwarding the email to phishing@rbc.com. If you believe you have provided your account or other personal information in response to a fraudulent email, contact your financial advisor immediately or call us at 1 (800) 769-2511.

From time to time, RBC will engage in promotional campaigns via telephone, mail and email. If you are ever unsure of any of the information you receive from us, do not respond and contact your financial advisor.

10 tips to safeguard your assets

Knowledge is often your best defense against online fraud. Following these 10 steps is a simple and effective way to reduce the risk of theft or misuse of your personal and financial information.

1. Keep your personal information confidential

An identity thief may go to any lengths to obtain your personal information (even picking through your garbage or recycling bins). So be sure to shred receipts, copies of credit applications, insurance forms, credit offers received in the mail, etc. Get into the habit of clearing your mailbox after every delivery. Make sure that your mail is forwarded or re-routed if you move or change your mailing address. Do not give out personal information on the phone, through email or over the Internet unless you have initiated the contact independently and know the person you are dealing with.

2. Be aware of billing and statement cycles

If your bills or statements do not arrive on time, follow up immediately to ensure they have not fraudulently been redirected. Review your statements regularly to ensure all transactions are authorized, and review your credit report annually.

3. Protect your PIN

Do not reveal your PIN to anyone, including employees of RBC, family members and friends. When conducting a transaction at an ATM or retail (point-of-sale) location, keep your client card within your sight and shield the keypad while you enter your PIN.

4. Limit your risk

Review your daily withdrawal limits on your debit card. If you do not need a high daily limit, reduce it. This will help contain fraud by reducing the amount someone can access. Only carry the ID and credit cards that you need; leave the rest (especially your birth certificate, social security card and passport) at home in a secure location.

5. Protect your personal information online

Always keep your personal computer, tablet and smartphone up to date with the latest software version. Be cautious in your online activity, especially when using unsecured/free wireless internet in public locations and when accessing sites with sensitive information, such as online banking. Make sure your home Wi-Fi connection is secured with a password.

6. Be password-smart

Never share your passwords and use ones that are difficult to guess. (Strong passwords use a mix of letters, numbers and characters.) Change passwords frequently. Do not recycle passwords and do not use the same passwords for online banking as you would for other services, such as social networking sites.

7. Verify before you click

Verify a message before you take any other action, such as clicking on a link or initiating a transaction. Do not click on any links or open files in emails from people you do not recognize or are not expecting (this could expose your computer to a password key logger or spyware).

8. Encrypt for greater security

Always use encryption when sending confidential information by email, and never store sensitive data about yourself or others in your email folders. Even encrypted emails can be hacked.

9. Maintain a suite of software security products

Install a well-recognized security program on all of your devices (PC/tablet/phone), and keep it up-to-date. A reputable personal firewall, as well as anti-virus, anti-spam and anti-spyware software, is 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.

10. Always log off

Remember to log off and close your browser to prevent others from being able to view your information later.

Additional precautions

The following tips may be useful if you think that your email may have been compromised, and can be useful as general guidelines when protecting your information online.

Contact your email service provider to change the password for your email account, or set up a new email address and password and discontinue using of the old one.

Get your computer professionally serviced and cleaned of viruses, spyware, malware and other harmful programs.

Check that your secondary email accounts or online banking at other financial institutions have not been compromised.

Request a copy of your credit bureau report and review for anything that is not yours. Remember to review your credit report again once per year.

Consider signing up for credit alert monitoring (fees may apply).

If you suspect you are a victim of fraud or theft, contact the authorities immediately. To learn more, please visit www.rbc.com/privacysecurity.