Protecting Your Personal Information When Your Email Has Been Compromised

Today's fraudsters are becoming more sophisticated all the time, and it is more important than ever to protect your personal information when corresponding online and via email. But what can you do if you think your email may have been compromised?

Notify RBC of Fraud Attempts

"Phishing" emails are unsolicited emails requesting confidential information, such as your account number or password, PIN or social insurance number. They often appear legitimate and are designed to trick you.

If you receive a phishing email that appears to come from RBC, 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 advisor immediately or call us at 1-800-769-2511.

Remember that RBC will never, under any circumstances, send you an unsolicited email that includes a link or phone number asking you to update or verify your account details or other personal information.

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 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 isn't 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.

More Tips for Safe Computing

Here are some more simple and effective steps you can take to reduce the risk of theft or misuse of your personal and financial information.

- Be careful of using free and unsecured wireless internet with your mobile devices in public locations (especially to access your online banking).
- Don't click on any links or open any files in emails from people you don't recognize or aren't expecting (this can expose your computer to a password key logger or spyware).

RBC Wealth Management

Additional Resources

- RBC – Privacy & Security: www.rbc.com/privacysecurity
- Office of the Privacy Commissioner of Canada: www.priv.gc.ca
- Government of Canada – Canadian Anti-Fraud Centre www.antifraudcentre-centreantifraude.ca
- Equifax 1-877-323-2598 or www.equifax.ca
- TransUnion 1-877-525-3823 or www.transunion.ca

- Always keep your personal computer, tablet and smartphone up to date with the latest software version.
- Maintain a suite of security software products, including a reputable personal firewall, anti-virus, anti-spam and anti-spyware – all necessary to provide online protection for your computer and your information.
- Don't recycle passwords and don't use the same passwords for online banking as you would for other services, such as social networking sites.
- Make sure your home wi-fi connection is secured with a password.
- Always use encryption or a secure email program when sending confidential personal or financial information by email.
- Never store confidential information about yourself or others in your email folders (e.g. Inbox, Sent Items, Drafts, Deleted folders).
- Protect your personal information – 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're dealing with.
- Keep your personal information safe – always shred receipts, statements, other documents and mail (such as credit offers) containing personal information, and clear your mailbox after every delivery.
- Never share your passwords – not even with family, friends or employees of RBC.
- Always use strong passwords, which are difficult to guess and include a mix of letters, numbers and characters – and change your passwords frequently.
- Always log off properly and close your browser to prevent others from being able to view your information later.

To learn more, please visit www.rbc.com/privacysecurity, or contact us today.

15_90083_154 (10/2015)