Digital Security – Keeping Your Personal and Account Information Safe

At BMO, we take your security seriously. We are committed to respecting and protecting the privacy and confidentiality of the personal information you entrust to us. It is also important that you know how to keep your information secure. This article provides a few simple ways you can protect yourself, as well as some key reminders for detecting fraud. More information about enhancing your security is available on the BMO Security Centre at www.bmo.com/home/about/banking/privacy-security/. Please be reminded that these are suggestions and we recommend that you speak to a technology professional about your digital security.

Public Wi-Fi

Public Wi-Fi hotspots offer minimal security and may leave you vulnerable to cyber threats because you can't control what security measures are being taken. As such, accessing your financial accounts while connected to public Wi-Fi is not recommended.

Passwords

To make sure that your password remains secure, it's good to get into the habit of changing your passwords regularly – for your computer, Wi-Fi, and all online accounts and websites.

Securing your computer

To help protect your account information, make sure that your computer is free of viruses and malware, and that your network connection is secure. It is recommended that you have antivirus software installed on your computer as it can help you avoid becoming infected from malware such as viruses, worms, Trojans and adware, all of which can be harmful to the security of your computer and, as a result, your information.

Securing your network and browser

Network security

When you secure your network, you decrease the chance of hackers gaining access to your network and, consequently, your personal information. To help protect the integrity of your network, you can use a software or hardware-based firewall[1].

Browser security

With fraudulent websites becoming harder to spot, it's important to be able to verify the web pages you're visiting, especially for Online Banking or when viewing your investment accounts online. To start, we recommend downloading Trusteer Rapport® software. It's free to download on your desktop, easy to set up, and it will ensure that you're accessing bmo.com, not an imposter site.

Permanently delete files

When you delete a file on your computer, it does not mean that it's gone forever. The information still exists on your hard drive until it is overwritten by new data. As a result, identity thieves can retrieve personal information from your hard drive after you sell or donate your computer, even if you deleted the file. To prevent this type of information theft from occurring, it is important to follow a proper electronic file disposal procedure to make your files unrecoverable.

Emailing personal information

Email is an easy and convenient way to communicate with your BMO financial professional. However, it can involve sending attachments or providing personal information. To help ensure that information being sent over email is secure, BMO employees use, and clients can access, BMO's PROTECT Message Center ("PROTECT"). PROTECT is a free service and is easy-to-use. It encrypts/scrambles your confidential information and stores it in a secure format for 90 days, enabling you to send and receive emails with confidence knowing that the information inside is protected. To enroll, speak to your BMO financial professional.

[1]A firewall is a program or device that inspects the information passing between your computer and its network connection. It blocks malware from gaining access to your computer, and also prevents the spread of any malicious software that finds its way onto your computer from spreading to your network

Continued

Detecting fraud

Knowing how to detect fraud is a key aspect of keeping your personal and account information safe and secure. Phishing schemes are becoming increasingly sophisticated, so it's important to know what to watch for.

As a reminder, BMO will never:

1. Call or email you to ask for your debit/credit card PIN or Online Banking password.
2. Send you an email and request that you provide your banking details by clicking on a link in the email. Our preference is to direct you to our website.
3. Ask you to email or text personal or banking information.

If you do receive such a request, please forward it as an email attachment to online.fraud@bmo.com, and then delete the message[2].

Spotting fraudulent emails

The following are some tips that can help you recognize fraudulent emails. Be cautious if:

- The email is sent from a new source or person with whom you have not previously communicated via email;
- The email is coming from an unsolicited source, contains attachments, or states that it is a follow-up to an action you did not take;
- The web address provided in the body of the email is clearly not leading to a BMO site. For example, be cautious if the web address contains the "@" symbol or is completely numeric (eg.123.456.1.2.);
- The email contains major spelling or grammatical errors. Legitimate emails do not contain these types of mistakes;
- The email contains threatening language or invokes a sense of urgency (e.g., "The account has been suspended" or "Click here immediately to reactivate your account"); or
- The email lacks details about who is sending the email (e.g., no street address or company name).

BMO Privacy Code – Canada

The BMO Privacy Code – Canada, which applies to the operations of BMO Financial Group in Canada, outlines what personal information we will collect about you, how we will use it, and who may see it. You can review the code on the BMO site (www.bmo.com) under **Personal >> About BMO >> Privacy Security >> Our Privacy Code**.

! To learn more about BMO's recommendations for keeping your personal and account information safe, visit the **BMO Security Centre** by clicking **Security** at the very bottom of the bmo.com homepage.

[2] Standard messaging and data charges may apply.

BMO Wealth Management

ID1702 (02/17)