How to make your account more secure

We want to keep your account protected, but we need your help in ensuring your security. If there is a security breach within BMO InvestorLine we guarantee a 100% reimbursement.[1] But if an unauthorized person was to access your account with the correct credentials and losses did occur, there is a chance you may not be covered.[2] When accessing your BMO investment accounts on any public or personal device, there are a few ways you can help secure your information and avoid losses.

General Guidelines

1. Avoid using public computers or WiFi

A general rule of thumb is to avoid accessing your information in a public place such as a coffee shop or a library. On public networks, attackers can easily tap into private information like credit card details, account numbers etc. This is because of weak security features and a higher chance of attackers seeing which webpages you access. It is essential that you protect your financial information.[3]

2. Always update your computer and mobile devices

Using an up-to-date anti-virus and firewall protect your computer from malware and Trojan attacks. These security updates also help in filtering the security weaknesses on your system. Don't forget to keep your browser and operating system updated on all your devices as they contain important security features.[4]

3. Never open suspicious emails

Phishing is the method used by spammers to send deceiving emails which then ask to input personal or financial information. As a security precaution, BMO will never request your user ID and/or password over email. Be wary of spam email and phishing attacks that may be disguised as an email from a reliable source. If you see a suspicious email that looks like it came from BMO, let us know at online.fraud@bmo.com and we will take the necessary steps required.

4. Download Trusteer Rapport for free

An easy way to protect yourself from online fraud is by downloading Trusteer Rapport. This software provides essential protection that finds, blocks and removes financial malware, and helps prevent phishing attacks. You can easily download it by clicking here.

Account Verification

Set up two-step verification[5]

BMO InvestorLine uses a two-step verification process that gives you additional security to your account. The two-step process sends a randomly generated 4-digit verification code through voice or text message to your phone when we need to confirm your identity. The code can be entered for secure sign in.

To set up two-step verification, click here for more information.

Passwords

1. Always create a unique password

Using a unique password with a combination of letters and numbers is best. Be sure to avoid creating passwords with personal details like birthdays, addresses or family member names as those can be easily guessed.

2. Change your password frequently

Since your account has sensitive information, it can be dangerous in the wrong hands. By changing your password regularly, ideally every 30-60 days, it makes it difficult for an attacker to log in to your account if they were to acquire your password. When there are any changes to your contact or password information, BMO will send an email notifying you of the change. If you notice the email, but haven't made a change, let us know immediately.

Continued

3. Never share your passwords

Your password is personal. It is important to keep it safe and not share it with anyone, including family members. Emailing passwords is a huge risk as it can be easily intercepted and read by unwanted eyes. Even after deleting an email, traces of it are stored on your computer. For your security, BMO will never ask or send sensitive information like passwords over email.

Browser Security

1. Clear your browser history regularly

Cache is the temporary files your computer stores. When you access a web page again, the computer uses cache to pull up the website instead of loading everything again. Clearing your cache and browsing history after your online session prevents the next user from seeing what you have been doing and gaining access to sensitive or personal information.

2. End your browser session

Signing out of your session ensures that your browser does not hold on to that information, which can be later viewed by unwanted eyes. Don't forget to close your browser after every online session minimizing the risk of your personal details being displayed publicly. Also, each time you log in, check your "last login" time to make sure there is no discrepancy. If you notice anything different, contact us immediately!

3. Check the security

Before inputting personal information on an online form, look at the address bar to make sure it displays **https**. This encrypts your input and makes your browsing more secure. Also, look for the closed padlock icon beside the address bar. It appears when the site is verifiably authentic and represents an SSL (Secure Sockets Layer) certificate.

If you notice any suspicious activity in your account, immediately contact us at 1-888-776-6886.

[1] Reimbursement is dependent on approval. If an active role is not taken in protecting your account, you may not be eligible for reimbursement.

[2] Our Online Security Guarantee will cover any losses that occur. Reimbursement is dependent upon approval.

[3] Accessing your account information on a public network may limit you from receiving your 100% reimbursement.

[4] Having outdated security features on your computer, operating system or browser may limit you from receiving your 100% reimbursement.

[5] Two-step verification is an enhanced form of security to verify your identity by using two methods of confirmations.

BMO Wealth Management
BMO InvestorLine

07/18-1400