BMO SmartFolio online security

How we protect you

Online security guarantee

We guarantee a 100% reimbursement for any unauthorized transactions made in your BMO SmartFolio account that result in a direct loss.*

To ensure reimbursement under this guarantee, you should:

- Sign out and close your Internet browser at the end of each session.
- Keep your password confidential.
- Review your online account activity and statements.
- Call us within 5 days if:
  - you suspect your password or your BMO SmartFolio account number has become known to someone else without your permission,
  - there has been suspicious activity in your account that you did not authorize, or
  - you suspect your computer system has been compromised by a virus or spyware.

Keeping your information safe

We'll never contact you to ask for your user ID, password, SIN or other personal information.

- If you're unsure a call is from a BMO SmartFolio representative, call us at 1-844-895-3721.
- Safeguard yourself from Internet security problems by being cautious when entering your personal information on websites.

Time-out settings

Session time-out is a security feature designed to help prevent an unauthorized user from accessing your accounts while you're away from your computer or mobile device. You'll automatically be signed out if your account is inactive for a period of time.

Periodic security reviews

To help you protect your information, BMO Nesbitt Burns periodically reviews the security of our computer systems to ensure they are not compromised. At BMO Nesbitt Burns, information security is extremely important and our employees are fully aware of their responsibilities to keep customer information secure and confidential. Whether you choose to deal with us online or over the phone, we follow rigorous security procedures and use state of the art technologies to protect your information and transactions against unauthorized access, disclosure, alteration and misuse.

While we do our best to ensure security and confidentiality, there are steps you can take as well to enhance your security when using the Internet and when using BMO SmartFolio.

How you can protect yourself

Password management

- Change your passwords periodically.
- Select passwords that are not overly simplistic.
- Use a password that is different than your other online accounts such as email, social media, etc.
- Shield your account number and passwords from any onlookers.
- Avoid sharing your user ID and account information.

Two-step Verification

Two-step verification (TSV) is a security feature that helps safeguard your account by asking you to confirm your identity with a one-time use verification code we send to your phone. Normal rates may apply from your telecommunications or data service provider for TSV communications you receive or send. For your security we may temporarily block access to your account or User ID until we can confirm your identity.

Safeguard your computers and mobile devices

In addition to using a firewall and anti-virus software, protect your computer's privacy by installing security updates, clearing your browser's cache and protecting your device with a password. Keep in mind that anti-virus programs often cannot detect spyware on your device. You may need a special spyware removal program.

Cache

We highly recommend that you clear your browser's cache or close your browser (which will also clear the browser's cache) after each account session to protect your personal information. A cache is designed to improve your device's performance and reduce network traffic. When you view a web page, the web page is stored in both your browser's memory cache and your device's disk cache.

Practice safe surfing

Take steps to protect yourself against "phishing"— a type of online fraud that asks you for private information. Think twice before clicking on links embedded in emails asking you to log into your account. Other signs that a site may be suspicious include misspelled or slightly altered website addresses. Check the URL in your browser to make sure the website is authentic.

Check for security

Legitimate organizations that allow you to make online transactions generally take steps to safeguard your security. Look for the security certificate on each site to make sure it's valid. You can confirm this by double-clicking on the locked padlock icon. By informing yourself about ways to stay safe online, you do more than protect the confidentiality of your data. You also arm yourself with the knowledge you need to benefit from online investing. If you notify us of an unauthorized transaction, we'll work closely with you to complete a prompt and thorough investigation. We'll need your assistance in taking all necessary measures to protect you from additional losses. This includes your permission to use a third party to investigate and review the virus present on your computer.

How to use cookies and tracking

Cookies are a commonly used web technology and many browsers automatically accept them. They're designed to give a website owner information about how their website is used, such as the pages, links, buttons and other areas the user is visiting.

BMO SmartFolio uses cookies in a number of locations. Pixel tags (also known as clear gifs) and cookies may also be used in promotional email messages and online advertising. These tools allow us to measure the effectiveness of our advertising and promotional campaigns. We also use analytics to make continuous improvements to the site.

You can set your Internet browser to notify you before a cookie is set, which gives you the choice of whether you'd like to accept it or not. Refer to your browser's online help for information on disabling and setting cookie preferences.

How to avoid phishing attacks

How to protect yourself from phishing

Avoid sending account numbers or personal information by regular email, as it is not a secure method of contact.

No legitimate company will ever ask you to supply personal information via email. Nor will they send you an unsolicited email asking you to open an attachment.

What is an email phishing scam?

Phishing is an attempt by someone to obtain your confidential information through email by impersonating a group or individual you normally trust.

A phishing email can:

- Mimic the look and feel of a genuine company.
- Contain poorly written English or gibberish text.
- Be sent through unsolicited emails containing attachments.
- Include a web address with the @ symbol or a numeric address (e.g., 123.456.1.2) that points to a site that is not related to bmo.com.
- Include a "reply-to" field with a different address than the "from" field.

How phishing scams work

1. You receive an unsolicited email with one of the following subject lines:

- You're required to update your personal information
- You won a contest!
- ACTION REQUIRED: Your card or account is suspended
- Good news: Your product application is approved. Your account has expired.

2. You're then asked to open an attachment or to reply to an email address.

3. If you click the attachment, you're taken to a malicious site that requests your personal information (e.g., bank card numbers/user ID, account numbers, PINs, credit card numbers, SIN, and/or passwords).

Watch our presentation "Don't Take the Bait" to protect yourself from this type of fraud.

http://www.bmo.com/media/dont-take-the-bait/en/index.htm

Browser and desktop support

To assist you in protecting your personal and financial information, BMO SmartFolio supports the following browsers:

Windows

- Internet Explorer 11.0+
- Firefox 41+

- Chrome 46+

Mac OS X

- Safari 8+

iOS

- Safari 8+

Screen reader support

BMO SmartFolio supports the following screen readers:

Desktop

- NVDA
- JAWS

Mobile

- Voiceover for iOS

What we do

Some of the security measures we have in place to help protect you when you use BMO SmartFolio include:

- Strong encryption technology to help ensure that data passing between your device and our web server is secure. Therefore you must have a browser that supports this level of encryption (in technical jargon: 128 bit encryption).
- Digital certificates issued by trusted third-party companies to let you know that our website is secure and genuine.
- Automatic sign out after a period of inactivity.
- Firewalls to protect your information within BMO SmartFolio.
- Two-step verification to confirm your identity when you sign in.

What we don't do

- We never send you messages asking you to provide us with personal or account information via email, i.e. phishing. If you do receive an email that appears to be from BMO SmartFolio asking you for personal information, please contact us immediately.

What you can do

- Ensure you have installed the latest spyware detection and firewall software on your device(s).
- Do not share your user ID and password with anyone.
- Keep in mind that email messages are not encrypted and therefore are subject to being intercepted and read by others. So please do not send us any personal information by email.
- Do not use public computers to sign in to your BMO SmartFolio account. Always use your own secure connection.
- Enroll in two-step verification as soon as you are prompted to.

For more information about BMO Financial Group Security, go to http://www.bmo.com/home/about/banking/privacy-security/how-we-protect-you

*Terms and conditions apply.

Security guarantee terms and conditions

1. Security guarantee

Subject to Sections 2 and 3 below, BMO Nesbitt Burns will indemnify you for monetary losses resulting directly from any unauthorized transactions in your BMO SmartFolio account. This does not include any monetary losses resulting directly from any unauthorized transactions in your BMO Bank of Montreal bank account. We may amend the terms and conditions of, or revoke, this security guarantee at any time without prior notice. For the purpose of this security guarantee, an "unauthorized transaction" refers to a transaction that was carried out in your BMO SmartFolio account through the online portal without your permission, authorization or knowledge where it can be shown that you have been a victim of fraud, theft or have been coerced by trickery, force or intimidation. For greater certainty, an "unauthorized transaction" does not include any transaction carried out in your account by any person acting under any authority to trade in your account or to otherwise act on your behalf.

2. Your responsibilities

BMO Nesbitt Burns will not indemnify you and will refuse all requests for compensation pursuant to this security guarantee unless you:

(a) notify us immediately upon discovering an unauthorized transaction but in any event, no later than 5 business days after the date you receive your monthly account statement following the date of the unauthorized transaction;

(b) notify us immediately if you know or suspect that your BMO SmartFolio account number or your user ID and/or your password has become known to someone else or if there has been any suspicious activity in your account; and

(c) cooperate fully and provide all information and take all actions

that we reasonably request when investigating an alleged unauthorized transaction.

(d) grant BMO Nesbitt Burns your permission to employ a third party to investigate and review the virus present on your computer.

(e) abide by the terms and conditions of the BMO SmartFolio Investment Management Agreement, as well as the agreements governing your personal or business banking or brokerage account(s) or other financial service or product offered by us.

3. Limitations

BMO Nesbitt Burns will not indemnify you and will refuse all requests for compensation pursuant to this security guarantee if we have reason to believe that:

(a) you failed to maintain a current version of antivirus and firewall software;

(b) you engaged in, alone or in concert with others, any fraudulent, criminal or dishonest acts relating to the unauthorized transaction;

(c) you shared your BMO SmartFolio user ID, account number or password with any other person including, without limitation, an online account aggregation service provider, or were otherwise negligent or careless in keeping your BMO SmartFolio user ID, account number or password confidential;

(d) you accessed our online portal using a computer that would reasonably be believed to contain software that had the ability to reveal to a third party, or to otherwise compromise, your BMO SmartFolio user ID, account number or your password; or

(e) you failed to take reasonable precautions to prevent an unauthorized transaction (for example, you failed to sign out and close your Internet browser at the end of your BMO SmartFolio session).

Limitation of Liability: BMO Nesbitt Burns will not under any circumstances, indemnify you or provide you with any compensation other than as detailed in Section 1 above or be otherwise liable to you for any indirect, consequential, special, aggravated, punitive or exemplary damages whatsoever, in who or in part (including but not limited to any business interruption, loss of profit, loss of opportunity, market loss, or any other commercial or economic loss) resulting from an unauthorized transaction in your account, even if we have been advised of the possibility of such damages.