Protecting Yourself from Cybercrime

What you need to know

BMO

Introduction

In an increasingly digital age, protecting our customers' data is one of BMO's top priorities. Our model for security comprises talent, technology, data and controls – to ensure you can do business with BMO safely, securely and with confidence.

Our framework includes our investment to ensure you have the tools you need to protect your privacy and security at home and when you travel. In this brochure, you'll find everyday banking and computer tips to help you avoid falling victim to identity theft or fraud.

Table of Contents

> We've brought together experts in cybersecurity, fraud, physical security and crisis management onto one team to strengthen our ability to detect threats and continuously improve our response strategies. Cybersecurity is a very important aspect of our business – this work helps ensure that your data is secure.
>
> Darryl White
> Chief Executive Officer, BMO Financial Group

How BMO keeps you safe

Setting a new benchmark for security

Today, with BMO's powerful digital capabilities, we can deliver the fast, convenient online banking experiences you and the rest of our customers expect from us.

In January 2019, BMO established the Financial Crimes Unit (FCU) to combine our cyber, fraud, physical security and crisis management teams into one internal organization. Together our teams create a fully integrated security task force that strengthens our security capabilities to protect bank and customer data.

We have invested in our technological infrastructure by incorporating advanced analytics and capabilities including AI and machine learning so we can detect, prevent, respond to and recover from security threats against the bank and our customers, enabling a safe environment where you can save, access and transfer your money with confidence.

BMO's security features:

- Our Fusion Centre, a state-of-the-art security hub, manages security threats 24/7/365
- Our "Follow the Sun" operating model enables our Fusion Centre teams to work with global security teams across North America, Europe and Asia

BMO uses sophisticated, secure internal controls to keep your data safe. These include firewalls and email strengthening programming as well as industry-leading security software. We have intensive awareness and education programming to ensure our employees are implementing high security standards.

BMO's security software for our customers

By teaming up with trusted technology partners, we can recommend software, services and apps to help protect you online. The following programs are available on bmo.com/security. Learn more about the programs and download them today.

IBM®* Trusteer Rapport®* software protects you against fraud and identity theft by flagging phishing sites. It's free to download, easy to set up and will ensure you're accessing bmo.com, not an imposter's site.

OnGuard®* is a service that protects your personal information and protects your identity online. OnGuard®* will scan public and underground websites and alert you when it finds your personal information.

Verified.Me™ is an app that helps you quickly and securely confirm your identity using your smartphone.

BMO will send online verification codes to you if we see activity on your account that isn't typical for you, to confirm it's really you.

Sign up for BMO Alerts to receive a text or email notification if we detect suspect suspicious activity on your accounts.

Message Center is a free, simple way to encrypt your emails and confidential information when working with a BMO Representative. Simply visit bmo.com/security to access our Message Center set up guide.

Our commitment to you

BMO offers a 100% Electronic Banking Guarantee for Personal Banking Customers. This means we will reimburse you 100% for any losses to your personal bank accounts resulting from unauthorized transactions through BMO Online and Mobile Banking.

To ensure reimbursement under this guarantee, there are a few necessary steps you must adhere to, as outlined in the Electronic Banking Services Agreement. We also recommend safeguarding your computer. Learn more at bmo.com/security.

TIP!

It's a good idea to review our Electronic Banking Services Agreement, which you can get at any BMO branch or online at bmo.com/agreements.

To ensure your protection with this guarantee, follow the steps outlined in the Agreement, including:

- Keep your password confidential at all times
- Store your password in a safe place, separate from your debit and credit card numbers
- If you wish to enable Touch ID or facial recognition sign-in for BMO Mobile Banking on your mobile device, you must have only your own fingerprints or facial image stored on your device so you're the only one who can access your personal banking information
- Notify us within 24 hours if your debit card, credit card or smartphone that you use for mobile banking is lost or stolen or if your password confidentiality has been compromised

Keeping your identity secure

One of your most valuable assets today is your identity. If fraudsters get access to your personal information, they can access your accounts, set up credit cards in your name, make purchases on your behalf, and much more. We need to work together to keep this information protected.

What information do you need to protect?

You need to protect any piece of information that can be used to identify you. Some examples include your Social Insurance Number (SIN), Personal Identification Numbers (PINs) to access banking or credit cards and verification questions and answers.

The only organizations you should share your SIN with are your employer, the federal government and your financial institution.

TIP!

These organizations will never ask you for personal information, PINs or passwords by email, phone call or website pop-up.

Personal Identification Numbers (PINs) and passwords

PINs and passwords are the gatekeepers to your money and accounts. They identify you as the authorized user of your accounts (debit card, credit card, online banking, telephone banking, etc.) and give you access to your money. It's critical you create strong PINs and passwords and never share them with anyone.

Choosing a strong PIN and password

- Use a different password/PIN for each account
- Make your passwords at least 8 characters long, and include special characters and numbers
- Change your PINs/passwords frequently
- Don't use words from dictionaries, seasons, calendar dates or common phrases
- Don't use dates personal to you that are easily guessed (e.g. birthday, anniversary)

Protecting your PINs and passwords

Protecting your passwords and PINs is one the most effective ways to protect yourself against fraud and identity theft. Here are some tips to keep your passwords safe:

- Don't share your passwords with anyone
- Don't store them in easily accessible places such as your desk, car, wallet, or under your keyboard
- When entering your PIN at an ATM or in a store, shield the key pad with your hand
- Similarly, when entering your password at your computer or on your smartphone, make sure no one is watching you as you enter the information

Protecting your accounts

Paper documents

Many of us still rely on paper documents (such as cheques or paper statements of accounts) to conduct or keep track of our transactions. Here are some tips to help keep your identity safe and avoid fraudulent transactions on your account:

- Store your cheques and any other documents with your banking data in a safe place
- Write your cheques with ink that cannot be erased; write clearly and don't leave room for fraudsters to add numbers or words
- Shred any documents you don't need, including cheques where you've made a mistake
- Never leave a payee space blank on a cheque, and avoid making cheques payable to "cash"
- Always monitor your accounts and transactions (online, bank books, account statements) for any discrepancies. Report any suspicious activity to BMO immediately
- Be cautious about accepting cheques from people you don't know well in exchange for cash. The cheques may not clear, and you will be held responsible for the lost funds

TIP!

Remember to check your bank statements regularly for strange transactions using online banking or the mobile app. If you see anything unfamiliar, report it by giving us a call at 1-844-837-9228, or by visiting your local BMO branch.

Card security and protection

Debit cards and credit cards enable us to access and transfer our money when and how we want, granting us optimal flexibility. It's important to keep your cards and their information safe to prevent becoming a victim of fraud.

Here are some tips to keeping your cards protected:

- Always keep your cards in a safe place; never leave them out in the open and don't share them
- Cancel and destroy any cards that are no longer in use (e.g. expired or cancelled)
- Sign and activate new cards as soon as you receive them
- If you are making a purchase, always ensure the card returned to you is your own card
- Shred or destroy any hard copies (receipts, statements) that have your card information
- Insist on swiping your own card when you are making a purchase. If you are unable, and the clerk must swipe it for you, make sure you can see your card at all times
- When making purchases, ensure the amount is correct before you punch in your card PIN or tap. Double-check by reviewing the receipt immediately
- Hide your PIN when conducting transactions at ATMs or while paying for purchases in a store
- Avoid giving your credit card number out over the phone, unless you initiated the call. Don't give out your credit card number over the phone in a public location

What BMO does to keep you safe:

- Our ATMs are equipped with keypad security shields, recessed screens with protective panels, and anti-skimming sensors to prevent debit card skimming and unauthorized viewing
- If we suspect that your debit or credit card is at risk, we will block access to your funds immediately and alert you through our automated calling program or Customer Contact Centre. BMO will then help you set up access to your debit or credit cards ASAP

Electronic transactions

In this digital age, we can now do our banking through mobile, online or by telephone. While it's fast, easy and offers many conveniences, it can also open the door to fraudsters. Here are tips to help make sure you bank online safely, securely and with confidence:

- Keep your operating system software up to date. Fraudsters often target older versions of software to launch malicious programs; make sure you are using security software products that include firewall, anti-virus, anti-spam and anti-spyware
- When banking online, make sure you're accessing the true BMO website by looking for the "closed lock" icon. The website should also start with "https"
- Avoid using public computers – these include computers in libraries and internet cafes. They could be carrying malicious software that can record your information
- Frequently delete your cookies as fraudsters can use them to access your private information
- Make sure your wireless connection at home is encrypted and password-protected to ensure no one else can use your connection without your permission
- Protect your mobile and tablet devices. Make sure no one is reading information from your device's screen; don't use public Wi-Fi for banking transactions and don't store your passwords on your device
- Ensure your mobile devices are password-protected and locked when not in use. This ensures your information is protected if your device is lost or stolen

What BMO does to keep you safe:

- If you forget to log out of a secure online session, we will automatically log you out after 10 minutes to help ensure that no one else can access your personal financial information
- BMO has device matching and security question verification. This is a security feature where BMO asks additional verification questions when your accounts are accessed by an unknown device, like a new mobile device or new browser

Secure telephone banking

BMO now offers Voice ID, a secure way of confirming customer identity using your voice when you use telephone banking. Voice ID is our primary method of authenticating customers, which makes banking over the phone fast, simple and safe.

When engaging in telephone banking, remember the following tips:

- Be mindful of what you say to the agent
- Ensure no one can overhear your personal information

Avoiding common scams

The following are common scams used to gain access to personal and financial data – and our suggestions on steps you can take to protect yourself.

TIP!

Visit bmo.com/security for regular updates on new scams being leveraged by fraudsters.

Phishing scams: Phishing is one of the most used and effective ways cybercriminals attack individuals everyday through email (phishing), text (smishing), or voicemail (vishing). Pretending to be a legitimate source, they try to obtain personal information from you, or encourage you to click a link or download an attachment that could install malware (malicious software) on your device. Here are some tips to help you avoid phishing attacks:

- Double-check links in emails by hovering over them with your cursor
- Read emails carefully. Impersonal or generic greetings, spelling mistakes and grammatical errors are all signs of a potential scam
- Don't respond to emails, texts or phone calls from companies or people you don't know
- If you receive an email, text or call asking you to urgently reply, click on a link, verify your account or reset your password, check with the company before you respond. Don't feel pressured to respond to an urgent request
- Don't click on attachments from unknown sources
- Don't enter personal or credit information into a form that is linked in an email. If you think the email is legitimate, call the company or visit their website and log in securely before you enter the requested information

Romance scams: Online dating sites are popular forums for scammers looking to trick victims into sending them money. Watch out for individuals who try to move quickly, put off meeting in person, or request money in any way. Avoid becoming a victim by not sharing personal information (including personal photos) and by refusing to send or accept money.

Money mule scams: A money mule is someone who moves stolen money from one bank account to another. They're recruited – often unknowingly – by criminals to move money made from criminal activity, making it harder for authorities to track them down. They may entice you with offers through social media or email, mail or the phone. Look out for job offers that are too good to be true – or people looking for you to open a banking account for them.

Phoney charity scams: Scammers can pose as legitimate charities to convince compassionate victims to give generously to their cause. Ask the organization to send you a pledge form and make sure to look them up online to ensure they are credible.

Social media scams: Watch for fake friend requests and hidden URLs to "free" quizzes. Only engage with people you know. When you provide your information to anything "free" online, know that you are likely sharing it with third parties.

TIP!

Remember, we'll never contact you via unsolicited phone call, email or text to ask you to confirm or provide your password, or for personal information or account details.

Contact information

Report a phishing email

If you think an email is a phishing attempt, forward it as an attachment to **phishing@bmo.com** and then delete the message

Report suspicious activity on your account

If you notice suspicious activity of any kind on any of your BMO accounts, please let us know at **bmo.com/contactus**

Report a lost or stolen card

For lost credit cards, call **1-800-361-3361** or **514 877-0330** (International Call Collect)

For lost debit cards, call **1-877-225-5266** (Canada)

5118600 (06/20) 06/20 - 1153

BMO