

Protecting Your Accounts

Safety tips for paper documents, card security, and electronic transactions



At BMO, your security is our priority. We work hard to bring you the fast, convenient banking experiences you've come to expect, but you also have an important role to play. Protecting your identity, along with your personal or business banking information, is a joint effort.

Follow these tips to help you bank safely, securely and with confidence.



Paper documents

Many people still use paper documents like cheques or paper statements to keep track of their transactions. Consider the following best practices when using paper documents.

Fill out cheques clearly

Write cheques with ink that can't be erased. Fill out cheques completely to leave no space for fraudsters to add numbers or words.

Store safely

Keep cheques and documents with banking data in a safe place.

Shred what you don't need

Destroy any documents you don't need, including any cheques with errors or blank cheque books you no longer use.

Don't leave cheques blank

Never make cheques payable to "cash" or leave the payee space blank.



Card security

Debit and credit cards make it easy to access and move your money. But it's important to take precautions to keep your cards and their details secure to help stay safe from fraud.

Don't share your card or PIN

Beware of fraudsters impersonating banks to try to obtain customer debit cards and PINs. BMO will never contact you asking for your bank card or PIN, or send a courier to pick up your card and/or PIN.

Keep them secure

Store your cards in a safe place. Never leave them lying around or share them with anyone.

Destroy old cards

Cut up and throw away expired or cancelled cards.

Activate new cards fast

Sign and activate cards as soon as you receive them.



Electronic transactions

In this digital age, we can now do our banking through mobile devices, online or by telephone. While it's fast, easy and offers many conveniences, it can open the door to fraudsters. Keep these security tips in mind when making electronic transactions.

Avoid using public computers

Public computers, including in libraries and internet cafes, can carry malicious software that can record your information.

Update operating system software

Fraudsters often target older versions of software to launch malicious programs.

Practise safe browsing

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."

Frequently delete your cookies

Fraudsters can use cookies to access your private information.

Remember

BMO will never contact you via unsolicited email, text or phone call asking for your bank card or PIN, sensitive information, passwords, or verification codes (one-time passcodes). BMO will never contact you asking for your bank card or PIN, or send a courier to pick up your card and/or PIN.

If you get a call, voicemail, email or text from someone claiming to be from BMO and you think it's suspicious, do not share any personal information and contact us immediately using the information on the back of your card.



At BMO, your security is our priority. Learn more about fraud prevention by visiting bmo.com/security.