# **Protecting yourself in the digital age:**
## Security tips from BMO's Financial Crimes Unit

BMO

**BMO's Financial Crimes Unit** – Setting a new benchmark for financial security
Learn more at bmo.com/security

# Table of contents


**Introduction** 3

**BMO's Financial Crimes Unit** 3

**Tips to keep you safe:**

- Scam awareness 4
- Online shopping 5
- Phishing 6
- Social media 6
- Cyber hygiene checklist 7

**Frequently Asked Questions** 8

**Contact information** 11

# Introduction

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

Our framework also includes sharing tools with customers, clients and our communities to help you protect your privacy and security. In this short guide, you'll find simple tips to help you protect your accounts and avoid falling victim to identity theft or fraud.


## BMO's Financial Crimes Unit

***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 additional security features:

- Fusion Centre, a state-of-the-art security hub, manages security threats 24/7/365
- "Follow the Sun" operating model enables our teams to work with global security teams across North America, Europe and Asia
- Layered internal controls to keep customer data safe
- Frequent training ensures employees stay current on security best practices

Tips to keep you safe

## Scam awareness

A scam is a dishonest or fraudulent scheme that attempts to take money or something of value from its targets. Pretending to be a legitimate source, scammers may try to obtain your personal information to commit fraud. They may encourage you to click a link or download an attachment that could install malware (malicious software) on your device.

# How to avoid scams and protect yourself

✓ Avoid any 'urgent' requests or offers that are 'too good to be true.'

✓ Review emails and URLs carefully. Emails and websites can look like they are from trusted companies, but if you review the email and URL carefully, you'll notice a small difference like one extra letter, a period, or a .net instead of .com.

✓ Say no to unsolicited calls or emails. If you're unfamiliar with the caller or sender, proceed with caution or avoid altogether.

✓ Be wary of anyone requesting gift cards, money orders, cheques or wires *as payment*. If anyone is requesting these types of payments, the chance of fraud may be higher.

**Note:** BMO will never contact you via unsolicited email, text, or phone call asking for sensitive information, passwords or PINs. If you get a call, voicemail, email or text from someone claiming to be from BMO and you think it's suspicious, contact us immediately using the information on the back of your card.

# Online shopping

While online retail continues to grow, fraudsters continue to find new ways to take advantage of online shoppers. There are steps you can take to protect yourself, including:

✓ Limit your online shopping to well known and reliable retailers. Seeing a locked padlock icon and "http**s**" in the URL is a good first step. If you're on a site that doesn't have these two things in the address bar, your data is at greater risk of being shared with a malicious entity.

✓ Question unbelievably good deals. If the price seems too good to be true, it most likely is. Additionally, look for these warning signs: the site asks you to pay upfront in order to unlock the deal or receive a discount coupon; you can't pay with a secure method like your debit card, credit card or payment apps; and the site has a vague or nonexistent return/refund policy.

✓ Avoid public Wi-Fi. Public Wi-Fi is every fraudster's best friend. Shopping online while connected to a public network can be risky because there's no guarantee on who's running it and who can access it (and your information!).

✓ Use mobile payment apps. Mobile payment apps are considered more secure for online shopping than directly entering your card details at checkout.

✓ Be sure to check your bank statements regularly. If you notice a transaction that you didn't make on your bank statement, you should contact your bank immediately.

# Phishing

Phishing is one of the most used and effective ways cybercriminals approach 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 on your device. Here are some tips to help you avoid phishing attacks:

- Read emails carefully. Impersonal or generic greetings, spelling mistakes and grammatical errors are all signs of a potential phishing email.
- 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 respond to emails, texts or phone calls from companies or people you don't know.
- 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.

# Social media

Identity theft can occur where you might not expect it — among "friends" or "followers" on social media. While these communities might feel like safe spaces to share the details of your life, you may be sharing more than you think. Here are tips to help protect your information on social media:

- Avoid sharing too much personal information such as your birthday, vacation plans, etc. Could this information provide clues to your passwords or security questions? Posting real-time vacation information could leave you vulnerable to break-ins when you are away.
- Stay away from quizzes that ask for "fun" information; the information you provide may be used to gain access to your accounts. Remember: when you provide your information to obtain something "free" online, you are likely sharing it with third parties.
- Exercise caution with people you don't know; be cautious when accepting new friends and followers on social media. Don't divulge personal information before getting to know someone in the real world.
- Review your privacy settings on all your devices and across each social media account to ensure you're only sharing updates with your intended audience.

# Cyber hygiene checklist

Here are some basic steps you can take to ensure your information stays protected:

**Patching (system updates)** – Improve your device's security and/or enhance functionality by installing updates to your firmware or software as soon as they become available. Use a reputable anti-virus software for an additional layer of protection and regularly create back-ups of your data, especially information you deem critical.

**Passwords** – Create strong and complex passwords for your accounts. Complex passwords are longer than 8 characters and include letters, numbers and symbols. Do not share your passwords with anyone, change them regularly, use different passwords for different accounts – and always change default passwords provided by a manufacturer.

**Permissions** – Restrict access to your personal data by limiting access (increase privacy settings) on your apps, web browsers, cameras and microphones. It is important to disable permissions to file-sharing websites if they are unknown or unused by you.

**Protecting your identity** – Avoid giving out personal information. Don't give out any information you don't need to, especially non-publicly available information. Additionally, limit what you post on social media. Scammers can target social media to discover personal information and use it against you (e.g. password reset questions).

**Parents (guardians), children and seniors** – Protect your friends and family by educating them on the tips above and letting them know they can contact you if they are in doubt or trouble regarding cyber-related issues. Seniors are among the most targeted by fraudsters; keep an open dialogue with the seniors in your life about cyber security and their online activity.

**Tips for kids:**

✓ Ensure your kids only download apps from reliable sources, like Google Play or the App Store and review an app's privacy settings before downloading.

✓ Most browsers offer safe-searching features to help you block websites with questionable content. Consider adding parental control software, which lets you filter website categories, block personal information from being shared, and schedule times children can browse the Internet.

✓ Teach your kids how to avoid questionable content they find online. In general, kids should avoid interacting with pop-up ads, websites asking for personal information, and downloads from people or sites they don't know.

# Frequently Asked Questions

## Do you suggest the use of password managers?

There is no one answer to this question as security experts normally have different opinions on it, depending on the context and application. However, here is a list of pros and cons when it comes to password managers:

**Pros:**

One password for all – The most desirable feature is that instead of having to remember tens or even hundreds of passwords for your online accounts, you simply need to remember just one.

Generate powerful passwords – One of the benefits of a password manager is it can create automatically-generated complex passwords for you.

**Cons:**

Single point of failure – If you happen to forget your password, then you may be locked out of the different accounts or services managed by your password manager. Alternatively, if someone is able to access your master password, they could access your accounts.

Password manager programs are a target for hackers – Hackers need to crack just one password to access your entire catalog of private login info.

## How do you know your device has been hacked?

Here are some signs that may indicate your device has been compromised:

### Noticeable decrease in battery life

A device that has been compromised may start to display a significantly decreased battery lifespan as the malware may be using up additional resources.

### Freezing/sluggish performance

Poor or slow performance could be caused by malware using your resources or clashing with other applications on your system.

### High data usage

Excessive data use can be caused by malware using your internet connection to send information back to its server.

### Mysterious pop-ups

Constant and unexpected pop-up alerts could indicate that your device has been infected with a form of malware that forces devices to view certain pages that drive revenue for the attackers through clicks. This type of malware is known as adware.

### Unusual activity linked to the device

If a threat actor is successful in accessing your device (especially your phone), they may also have access to its accounts. Watch for unusual activity on your accounts, including resetting passwords, sending emails, and receiving verification emails for new accounts you didn't sign up for.

## What should I do if I think my device has been compromised?

Here are some actions to take if you think your device has been compromised:

- Download a verified security application that can scan your device for malware and clear it from your computer or phone.
- Reset your passwords and relevant account information.
- Go through your list of applications and delete those that you don't recognize or fully trust.
- Update your operating system and the applications to the latest versions. This will ensure all known vulnerabilities are patched and cannot be used against your device.

## How do I adjust my privacy settings to better protect myself?

**Watch how location data is being used** – This information can identify your location – and track you throughout your day – so be sure to check and adjust geolocation settings for each application you use.

**Don't give apps access to your phone** – Applications may request access to your contacts, calendar, cameras, photos and microphone. Turn off these options from the device settings if they aren't needed.

**Limit access to your accounts** – Applications may request access to your other accounts like Facebook, Twitter or Google. When you are no longer using an application, you should delete it and unlink it from your accounts and device through the settings.

## How do I safely use social media apps while protecting my privacy?

### Understand what information is being collected

Before you sign up for an online service or download a social media app, learn about what personal information is collected and the privacy controls offered. If you're not comfortable with how a service handles personal information, don't sign up for it.

### Adjust privacy settings

Before posting information or images on social networking sites, make sure you review and adjust the default privacy settings. Set your preferences so that information is shared only with those you intend to share it with.

### Turn off location tracking

Turn off or limit your location tracking if it is automatically enabled. Many apps or services will ask you to turn on location tracking; consider whether the information is essential to the service before making a decision.

## What mobile apps are safe to use on my device?

### Know your source and download applications from reputable markets

Apps within Google Play and the Apple App store are screened for legitimacy, quality, safety, and many other factors. Apps outside of these markets are more likely to be infected with malicious programming. Ensure your app source is safe and legitimate.

### Understand the vendor or developer of the application

Reputable app developers are easy to research and many applications link to their vendor's web page, allowing you to learn more about the provider.

### Inspect permissions

Applications should not have too many permissions; the permissions they do have should be appropriate to the app.

### Read reviews

Pay attention to the number of times an app is downloaded and its rating. Reading the app's reviews can also help you understand the app's pros and cons.

**Important reminders!**

✓ Sign up for alerts with your bank. BMO Alerts make it easy to keep track of your account activity and monitor for suspicious transactions. You can sign up through Online Banking or the BMO App.

✓ Keep your contact information up to date. That way, BMO employees can contact you immediately if they detect unusual activity on your account.

✓ Be sure to use multi-factor authentication (MFA) where possible. MFA uses more than one piece of information to confirm a customer's identity. A combination of factors can be used, for example, something the customer knows (like a password), with something they have (like a hardware token), or something they are (like a fingerprint, facial pattern or voice, also known as biometrics).

# Contact information

Visit bmo.com/security to learn more about BMO's Financial Crimes Unit and additional ways to stay safe online.

**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)

**Think you might be a victim of identity theft or cyber crime?**
Visit the Canadian Anti-Fraud Centre to submit a report, get a personalized step by step recovery plan, and find other helpful resources.

**BMO's Financial Crimes Unit** – Setting a new benchmark for financial security
Learn more at bmo.com/security