BMO

Protecting yourself from scams

Learn about the most common scams

What is a scam? How can you protect yourself?

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 malicious software (also known as malware) on your device. We've created a list of some of the most common scams out there in this quick-reference guide to help protect you, our valued customer.

For more information and the latest security information, please visit BMO.com/security or BMOHarris.com/security

Common scams

Business email compromise scams
Business email compromise occurs when a fraudster sends a message that appears to come from a known business source. The email makes a request for you to share financial information or process a payment and seems legitimate – the fraudster is counting on you to provide the payment or information to commit financial crime.

Business scams
Beware of false billing for a directory placement, sales of "required" health and safety products, and office supply scams. Fraudsters will hound you to pay the amount they claim you owe or trick you into believing they will report your business to a collection agency.

Cryptocurrency investment scams
Fraudsters are using market interest in cryptocurrency to lure investors into scams. Some crypto investment scams are variations on traditional scams, such as investment or romance scams. Here are scams unique to cryptocurrency:

- You are directed to a specific trading platform to convert your funds into crypto assets, and then are encouraged to transfer these assets to an investment website to fund an "account," but the website and account are fake.
- You are instructed to download software to supposedly facilitate asset conversion and transfer, but the software provides fraudsters with remote access to your computer.

- Using false statements and the illusion of rapid gains, fraudsters encourage you to make additional deposits. Ultimately, requests to withdraw your assets will fail, fraudsters will stop replying to your communications and you could lose all your funds.
- Read our full article on emerging cryptocurrency scams on BMO.com/security or BMOHarris.com/security.

Door-to-door scams
Door-to-door salespeople may use high-pressure tactics to convince you to buy a product or sign up for a service you don't want or need. In some cases, you never receive the product or service, or it's of inferior quality.

Emergency scams
This scam starts with a phone call to a grandparent from someone claiming to be their grandchild saying they're in trouble and need money immediately. Taking advantage of our emotions and need to protect loved ones, fraudsters attempt to rob victims of their money.

Employment scams
A fraudster may employ you to help with banking transactions. They may send you a cheque and ask you to deposit it into your bank account and then ask you to transfer the money to another account (fraudster's account) in exchange for a percentage of the original deposit value. When the original cheque doesn't clear, you're on the hook.

Google Voice verification scam
Google Voice allows you to make and receive free calls and texts in Canada, the US and internationally. Fraudsters are finding phone numbers online and then tricking individuals into providing them their Google Voice verification code to setup accounts to commit fraud. Never give your code to anyone regardless of how convincing their story may be.

Health and medical scams
The three most common health scams are miracle cures, weight loss programs, and fake online pharmacies. They often appear as sponsored posts on social media or website pop-ups. If you do receive the product, there is no guarantee it will work or be safe to consume.

Identity theft scams
Criminals are always on the lookout to collect or reproduce your personal information to commit fraud. Offline, they may go through trash bins or steal mail. Online, they may use spyware and viruses, as well as hacking and phishing. Thieves can ruin your credit and disrupt your life when they make purchases using your accounts, obtain passports, receive government benefits, apply for loans, and more.

Investment scams
Traditional investments are not immune to scams. Investment scams are any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all their money. You run the added risk of having your identity stolen, accumulating losses for unauthorized withdrawals on your credit cards and incurring high interest payments on investments that do not exist.

Money mule scams
A money mule is someone who moves stolen money from one bank account to another. Criminals may try to recruit you through social media or by email, mail or phone to move money they've made from criminal activity. When scammers use money mules, they make it harder for authorities to track them down, so they can commit more crimes without getting caught.

One time password (OTP) scams
Fraudsters collect your OTP through social engineering, gain access to your online banking account and proceed to send electronic funds transfers. In some cases, scammers keep customers on the phone to verify the fraudulent transactions via two-way SMS.

Overpayment scams
If you're considering selling your old devices or last season's designer clothes online, watch out for "accidental" overpayments that exceed the agreed-upon price. These scams involve tricking you into refunding money to a fraudster who has overpaid you with a bad cheque, stolen card and/or email money transfer or wire payment. You lose out on the payment itself and the money you returned as overpayment.

Phishing and smishing scams
Phishing attacks aim to attain personal and financial information, such as credit card details or passwords for online accounts; or to steal your identity, your money or both. They are used through email but can also be sent through phone (vishing), text message (smishing), social media messages and pop-up ads.

Purchase of merchandise scams
Online shopping is a favourite pastime for many consumers but some deals you see online may seem too good to be true. Scammers can set up accounts on legitimate sites such as online marketplaces offering products at very low prices. If you do receive a product, it may be of poor quality or a bad imitation.

Romance scams
Keep your guard up and look out for potential scammers who will try to lower your defences by appealing to your emotions using popular, legitimate dating sites as well as social media. Scammers will eventually ask for money – often due to "urgent" circumstances – and once you provide it, they disappear.

Sale of merchandise scams
If you sell items online, you risk being targeted by tricksters who want to take your merchandise, money, or both. Beware of buyers who offer to purchase your item sight unseen. They request a tracking number before providing payment and then don't send payment. Scammers may also try to provide payment using a fake money transfer, a fraudulent check, or a stolen credit card.

Subscription scams
A subscription trap can trick you by offering "free" or "low-cost" trials of products and services. Once you provide your credit card information to cover shipping costs, you are unknowingly locked into what can be an expensive monthly subscription, with delivery and billing difficult or even impossible to stop.

Tax scams
You get a text message or an email claiming to be from the Canada Revenue Agency (CRA) or the U.S. Internal Revenue Service (IRS) saying you're entitled to an extra refund and all you need to do is provide your banking details. Or the scammer may say you owe the CRA or IRS money and you need to pay right away or they will report you to the police. Please know that these organizations will never ask for these details. Providing these details or any other personal information gives scammers access to your accounts and/or may defraud you of your money.

How to avoid scams and protect yourself

There are so many scams targeting innocent individuals and businesses. Luckily, there are some common steps you can take to protect yourself:

- **Avoid giving out personal information.** Don't give out any information online, via phone, or in person that you don't need to, especially non-publicly available information such as social insurance numbers and account numbers.

- **Limit what you post and who you connect with on social media.** Scammers can target social media to discover personal information; this information can be used to manipulate a vulnerability.

- **Slow down.** Avoid any 'urgent' requests and be mindful of responding too quickly. Instead, take a moment to investigate and follow up with the company using information from their website.

- **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, for example, one extra letter, a period, or a *.net* instead of *.com*.

- **Say no to unsolicited calls, emails or visitors to your door.** If you're unfamiliar with the caller, sender, or visitor, proceed with caution or avoid altogether.

- **Never share your bank card information.** Never give out your card, expiry date, CVV(certified verification value) or PINs to anyone, either online, via phone, or to some one who comes directly to your home.

- **Be wary of anyone requesting gift cards, money orders, cheques, or wires.** If any one is requesting these types of payments, the likelihood of fraud may be higher.

- **Independently verify if the request seems out of the ordinary.** Get into the habit of calling phone numbers and checking websites to ensure they are legitimate.

- **Do your research when considering crypto currency and traditional investments.** Validate the investment firm's reputation or the representative's professional background with your own independent research. Beware if the investment representative encourages you to do load specific software.

- **Sign up for alerts with your bank.** BMO Alerts are free and 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.** Ensure your contact info is always current. That way, BMO employees can contact you if they detect unusual activity on your account. Reminder! BMO will never contact you via unsolicited email, text or phone call asking for sensitive information, passwords, PINs or verification codes (one-time passcodes). If you get a call, voicemail, email or text from someone claiming to be from BMO and you think it's suspicious or would like to verify it's BMO, hang up and contact us immediately using the information on the back of your card.

- **Choose passwords that are unique and complex.** Avoid common passwords like "123456" or passwords that include obvious personal info. Your password should be a least eight characters long and combine upper and lowercase letters and special characters (numbers and symbols). Use a favourite song or catch-phrase to help you remember it. Remember to change your passwords regularly.

Setting the standard for bank security

At BMO, your security is important to us. That's why we go above and beyond to protect you. Founded in 2019, BMO's Financial Crimes Unit combines world-class expertise from our cyber security, fraud, physical security, and crisis management teams to detect, prevent, respond to and recover from security threats.

Learn more at **BMO.com/security** or **BMOHarris.com/security**

Contact information

In Canada

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
To report suspicious activity on your account, call us right away at 1-877-225-5266 or visit your local branch.

Report a lost or stolen card
For lost or stolen credit or debit cards, call 1-800-361-3361.

In the United States

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

Report suspicious activity on your account
To report suspicious activity on your account, call us at 1-888-340-2265 or visit your local branch.

Report a lost or stolen card
Visit bmoharris.com/contactus and find the right number to call based on the type of card lost.

BMO

This document was inspired in part by "The Little Black Book of Scams" (accessed in June 2022), which was produced by the Competition Bureau Canada.