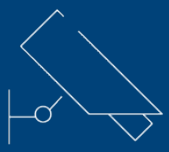
Digital Safety and Scams

Your guide to spotting scams, protecting your accounts, and staying safe

RBC®

Table of Contents



Staying One Step Ahead

From shopping to banking to keeping in touch, our lives are more connected than ever. But that convenience also comes with risk. Scammers are constantly finding new ways to manipulate people into giving up personal information or sending money.

The good news is, you don't need to be a tech expert to stay safe. This guide offers practical tips to help you protect yourself online, including easy-to-follow checklists and a list of resources in case you – or someone you know – needs to report a scam.

Cyber Security Basics: Your Protection Checklist

Strong cyber habits are your first line of defense. These simple steps can help protect your personal information, secure your devices, and reduce your risk of falling victim to online scams.

☐ **Install anti-virus and anti-malware software – and keep it updated**
These tools help catch harmful programs that could steal your information or damage your device.

☐ **Update your devices and apps as soon as patches are available**
Updates often fix known security holes that scammers can exploit.

☐ **Use strong, unique passwords – or passphrases – for all login credentials**
If one password is stolen or compromised, maintaining unique passwords that are different help stop scammers from accessing all of your login credentials.

☐ **Turn on two- or multi-factor authentication**
2FA or MFA adds an extra step for anyone trying to log in to your account, making it much harder for scammers to get in – even with your password. Setting up a trusted device can help prove it's really you during security checks; it can also make for a smoother experience on sign-in and offer simpler security checks when transacting at higher limits.

☐ **Back up your files regularly (ideally both in the cloud and offline)**
This way, if your device is hacked or locked by ransomware, you can recover your important information.

☐ **Avoid downloading apps, software, or files from unknown sources**
Some downloads are hiding viruses or spyware designed to steal your personal data.

☐ **Don't overshare on social media - limit what you post and who can see it**
Scammers use personal details like your birthday or pet's name to guess passwords or trick you.

☐ **Make your social media profiles private and review contacts often**
This keeps strangers (and scammers) from seeing or misusing your personal information.

☐ **Use secure connections and avoid public Wi-Fi for financial transactions**
Public Wi-Fi networks can be unsafe, making it easier for scammers to intercept your data.

☐ **Register for Autodeposit for e-Transfers to reduce fraud risk**
Autodeposit sends money directly to your account, preventing it from being intercepted.

☐ **Use security questions that aren't easy to guess**
Answers to questions like "What's your dog's name?" can often be found online, so choose questions only you would know the answers to.

Spotting Common Scams

Scams come in many forms – and they're getting harder to spot. Knowing the warning signs can help you avoid falling for a fake message, phone call, or website, no matter how convincing it might seem.

Social Engineering Scams

Scammers often try to exploit your natural instincts to help others or respond to urgency – and this is the essence of a social engineering scam. In these scams, fraudsters try to manipulate people into giving up confidential information, such as passwords or banking information, by posing as someone trustworthy.

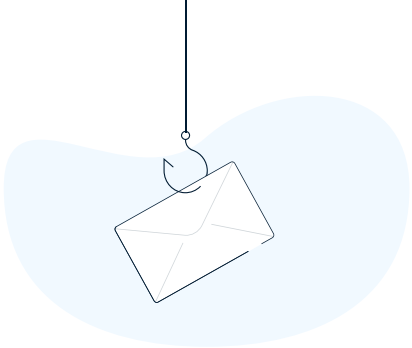
These scams may involve urgent requests from a "friend," "boss," or "customer support." The trick lies in making the story sound believable.

If you receive an urgent message that asks you to perform an out-of-the-ordinary task or send money, always pause, verify the facts, and never feel pressured to respond on the spot.

Social Media Scams

Scammers use social media platforms to contact victims directly, often offering fake giveaways, tax refunds, or business grants. Be skeptical of direct messages from people you don't know and avoid clicking links or sharing personal details.

If you get a direct message from someone you know that seems unusual or out of character, don't reply – it could be a scammer using a hacked account. Try reaching out through another method, like a phone call or text, to confirm whether the message is legitimate.



Online Scams (Fake Websites, Apps, and News)

Fraudsters have become skilled at creating fake shopping websites and apps that closely resemble the real thing. These sites may ask for your credit card or personal information without actually delivering a product, or they may spread false news stories on social media to manipulate you into clicking links or making fraudulent investments.

How to tell if a site is fake? Look out for poor design, broken links, vague policies, or a lack of contact information. On apps, check the publisher name, read user reviews, and avoid apps that ask for too many permissions. For news sites, watch for sensational headlines, unusual URLs, and stories that appear only on questionable sources or social media.

Email Scams (Phishing)

With phishing emails, scammers impersonate familiar brands and companies (i.e., shipping services, the government, or your bank) and use tactics to trick you into sharing your personal information or to click on malicious links. Phishing emails often appear to come from a legitimate company or organization, using scare tactics ("Your account is frozen!") to prompt you to click a link or enter personal information.

Even professional-looking emails can be fake. No matter who the email appears to come from, don't click suspicious links and never provide passwords or account details via email. Not sure if an email is legit? Contact the company directly using a verified number or website.

Phone Scams (Vishing and Smishing)

Phone scams might involve a fraudster posing as a bank, government agency, or even a police officer. In many cases, they'll say you owe money or that your account is at risk, and pressure you to share personal or financial details.

Some scams come via text message and ask you to click a suspicious link (this is called "smishing"), and others are phone calls (this is "vishing").

If you're unsure about the contact, hang up or ignore the message and call the organization back using a number you trust.

Romance Scams

Romance scams usually start on dating sites or social media. The scammer will build a relationship, often over weeks or months, gaining the trust of their victims. There will be multiple messages sent back and forth, strong feelings expressed, and many compliments shared. These scams are extremely effective, and play on the victim's emotions, leaving them in a vulnerable state to fall victim to the scam. Eventually, the scammer will ask for money – often citing an emergency, the need to cover travel expenses, or perhaps even a lucrative investment opportunity.

Be cautious of red flags such as excuses for why they can't meet in person, requests to move the conversation off the platform, and urgent pleas for financial assistance, or too-good-to be true investment opportunities often involving cryptocurrencies.

Bank Impersonation Scams

These scams often begin with a call, text, or email pretending to be from your bank. They may claim your account was compromised and – in order to verify the activity – they ask for your password, PIN, or even the two-factor authentication (2FA) code sent to your phone.

These interactions can feel very legitimate and have been successful in tricking even the most cyber savvy targets. Keep in mind, however, that no bank will ask for this information via text or phone. Never share codes or passwords with someone who contacts you first. If you're ever unsure, hang up, and call the bank directly using the number on your card or official website.

Often times, these scammers will have victims sign in to their Online Banking, and send an e-Transfer to a newly added payee under the victims own name. The scammers will indicate that this transfer is needed to secure the funds in the account, while the investigation is ongoing.

Keep in mind, RBC will never ask you to perform any financial transaction on our behalf, especially in order to resolve a fraud/scam situation.

AI-Powered Scams

Artificial intelligence has made scams harder to spot.

Criminals use AI to boost the frequency, reach, and appearance of their scams, enabling them to:

- Write polished phishing messages.
- Clone voices for phone scams.
- Create fake job or video calls with deepfakes.
- Set up convincing fake websites.

While AI makes scams trickier to detect, the best way to protect yourself is to be cautious with unfamiliar communications – especially those that ask you to act quickly or send money.

Investment and Crypto Scams

Investment and cryptocurrency scams often target individuals through both solicited and unsolicited means. Scammers will lure you to invest in opportunities (often tied to cryptocurrencies) with a promise of high rates of return in a short amount of time, with little to no risk.

Scammers create fake websites, ads and might also pose as trusted companies and high-profile individuals – sometimes using deepfake technology to convincingly impersonate someone. They also play the long-game, soliciting via social media platforms, messaging apps, and even dating websites often taking time to build trust. They may share “screen captures” or live “trend graph” showcasing the progress of the investment. Watch out for red flags such as directions to send e-Transfers to crypto companies, wires, or deposit into Bitcoin ATMs, where the funds are then obtained by the scammer.

Make sure you can directly access your investment account and can independently verify performance. Always do thorough research before investing and remember if an investment opportunity sounds too good to be true, it is likely a scam.

Fraud and Scams: What to do if You've Fallen Victim

Have you fallen victim to fraud? If so, you're not alone. Many people hesitate to report scams out of embarrassment, but today's fraudsters are very sophisticated, and their tactics are designed to fool even the most cautious and savvy individuals. Reporting what happened not only helps protect you, but it also helps prevent others from being targeted.

Here's what to do if you've been affected by fraud.

1. Notify your bank

If you've experienced fraud, your bank can help you protect your accounts and prevent further loss. Contacting them right away means any affected cards or accounts can be locked, monitored, and replaced quickly. Your bank also has dedicated fraud specialists who can guide you through the next steps and help secure your information.

RBC Clients

If you're an RBC client and have been a victim of fraud, please contact your branch, local office, or call immediately. For general inquiries or comments regarding Privacy and Security, please also call us.

- 1-800-769-2511 (telephone banking)
- 1-800-769-2555 (online/mobile banking)
- 1-800-769-2512 (credit cards)
- 1-800-769-2535 (RBC Express online banking Client Support Centre)
- RBC Bank (Georgia), N.A.: 1-800-769-2553
- TDD/TYY: 1-800-661-1275

If you live in the U.S., please also contact your local authorities as well as the FTC (Federal Trade Commission) at 1-877-438-4338.

2. Notify credit reporting agencies

If a fraudster has accessed your personal information, contact the credit reporting agencies right away. They can place a fraud alert on your file, which makes it harder for someone to open unauthorized accounts in your name. It's also a good idea to request a copy of your credit report and review it for suspicious activity.

There are two major credit bureaus: Equifax and TransUnion. It's best to contact both, as they operate independently and may not share information.

Canada:

TransUnion
1-877-525-3823
transunion.ca

Equifax
1-877-323-2598
equifax.ca

United States:

TransUnion
1-800-888-4213
transunion.com

Equifax
1-800-685-1111
equifax.com

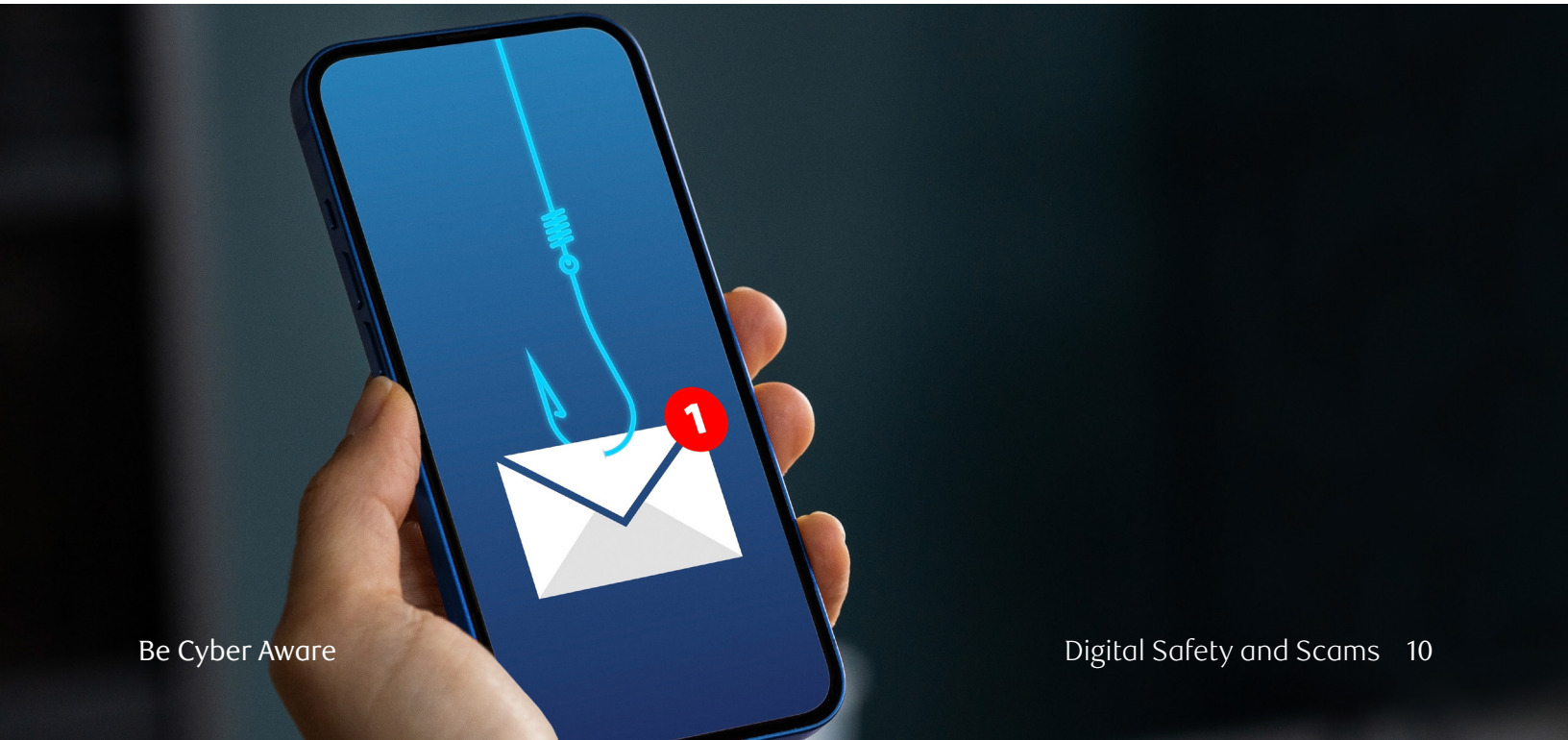
Experian
1-888-397-3742
experian.com

International (British Isles):

Experian
+44-844-481-8000
dialing from outside the UK

0844-481-8000
dialing locally within the UK
experian.co.uk

Equifax
equifax.co.uk
(all contact is online, unless someone is a member of the Equifax service)



3. Take steps to mitigate further impact

Once money or personal information is shared online, it can be difficult to recover. That's why taking quick action is so important. Here are key steps to limit further damage and protect yourself – and others – from additional fraud attempts.

- ☐ **Scan your devices**: If you clicked on a link or attachment, there's a chance the scammer tried to install malware on your device. It's a good idea to run an antivirus scan to check.

- ☐ **Change your passwords**: If you use the same password for multiple accounts, you'll want to change any relevant passwords immediately. This is a great opportunity to create stronger passwords.

- ☐ **Lock down your credit**: If you shared personal information with the scammer, one of the bigger risks is that they could use that data for identity theft purposes. It's therefore recommended to place a fraud alert on your credit report. This will alert creditors and other credit bureaus that you may be a victim of identity theft or fraud. These alerts can help keep someone else from opening an account using your information.

- ☐ **Lock or cancel your credit card**: If you inadvertently provided a scammer with your credit card or debit card information, you can immediately lock your card and then call the bank to cancel it. This will prevent fraudsters from using your card for unauthorized purchases.

4. Monitor your statements

Scan your bank card, credit card, and other account statements to ensure all transactions are legitimate. Reviewing your statements is always recommended, but is particularly important if you were a victim of fraud.

5. Stay vigilant

Scam and fraud victims can be targeted repeatedly, especially after they lose money. Scammers often impersonate government agencies, fraud departments, or lawyers claiming they can get your money back (and ask you to send additional money to do so). If you can't verify that a message is legitimate, don't engage. Instead, contact the organization directly through official channels to confirm.

Staying safe online doesn't have to be complicated. With a few smart habits and a healthy dose of caution, you can protect yourself from the most common scams and digital threats. Share what you've learned with friends and family – because the more informed we all are, the harder it becomes for scammers to succeed.

Notes

Checklist

- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐

For more cybersecurity content visit: rbc.com/cyber

Created: October 2025
Last Updated: December 2025