The Vault

A cyber safety playbook

Contents

Report cyber fraud to RBC

If you believe you are the victim of a malware attack, or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

Protecting yourself and your family in the digital world

Educate. Communicate. Prepare.

Ever bought a new smartphone, only to hear about a new model a month later?

Then you know how quickly technology can change. The rapid progress of technology is great for consumers – but it's also great for cyber criminals who benefit from tech advancements that give them new ways to access our information. The good news is, there are simple steps you can take to proactively protect yourself.

While RBC is committed to keeping your financial information safe and secure, this guide of best practices will help you protect yourself online and arm you with the knowledge you need to improve your cyber security skills.

Resources

RBC:
Be Cyber Aware

Government of Canada:
Stay Safe and Secure Online
An introduction to the Cyber Threat Environment

Other:
Protecting your Wealth from Hackers
What to do if your Business/Employees are Hacked

Don’t pass on password protection

It’s time to refresh those stale passwords

We get it. Remembering new and unique passwords for every online account can be a pain. But so is getting hacked. Having different passwords for each of your online accounts is crucial to protecting them from cyber criminals. A password manager can help by saving your passwords to a vault and suggesting new ones for each site.

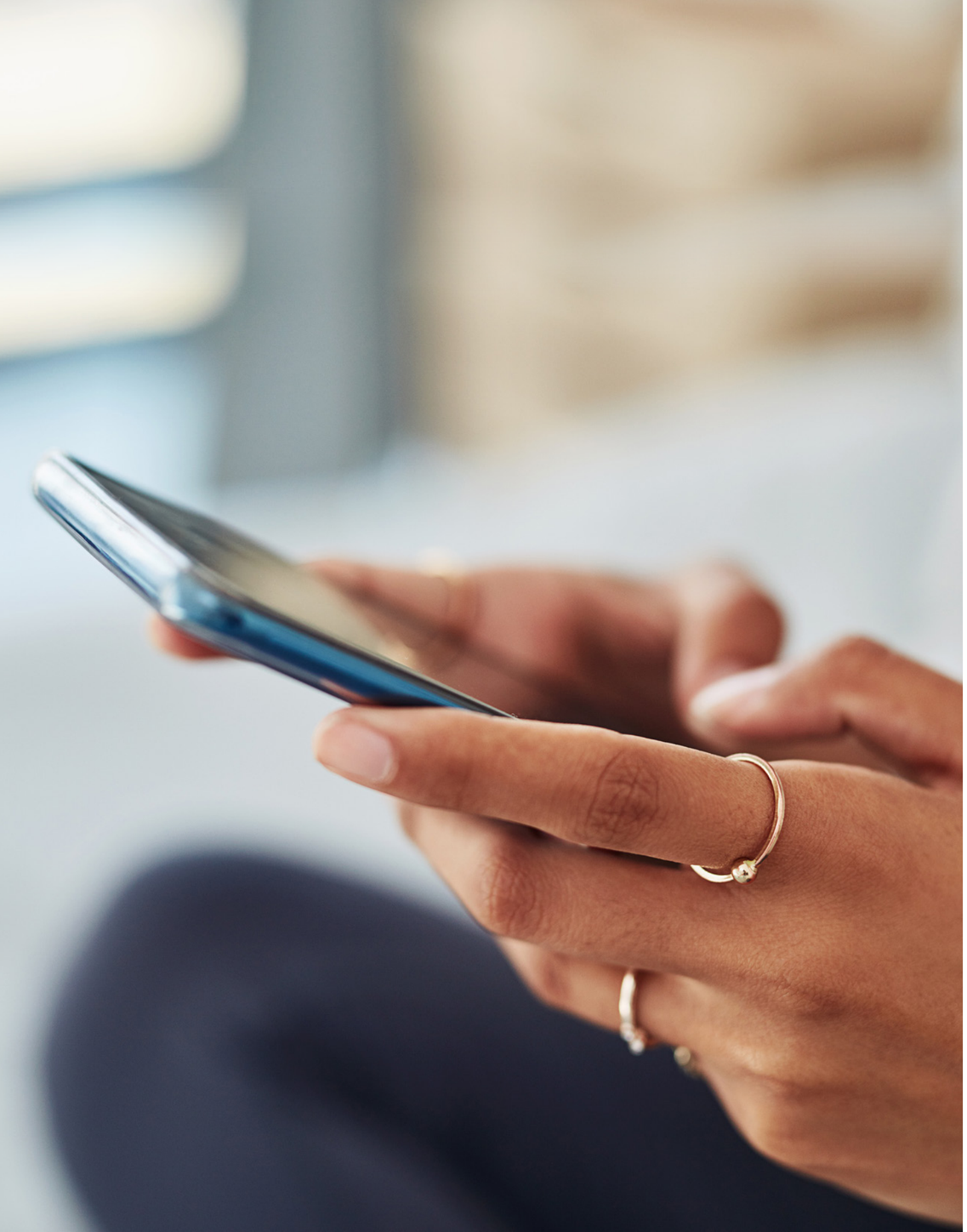
5 steps to stronger passwords

1. **Use a different password/passphrase for each account,** especially when sensitive or financial information is involved.
2. **Complexity is nice, but length is key.** Always use the maximum password length allowed. Aim for at least 16 characters, if possible.
3. **Avoid common words like “password” or “user”,** or anything that can be easily guessed like your birthday, or obvious sequences like “1234” or “ABCD.”
4. **Be creative.** Some of the strongest passwords aren't words, but a collection of words or "passphrases," which are made up of randomly chosen words. They can be both easy to remember and hard for someone else to guess. Here are some examples: "Delay Elephant Buy” or “Europe Profit Now”.
5. **Consider a password manager.** Password managers generate strong, random passwords and remember them, so you don’t have to. Your encrypted password database can then be accessed with one master password/passphrase. It’s the only one you’ll need to remember.

Replacing some letters with spaces, numbers or special characters – for example, @ replaces an “A” or $ replaces an “S” – can help increase the strength of your password.

Double down on safety

Think of it as having more than one lock on your door



When you sign into an online account, you typically have to prove who you are by entering a username and password. This offers one layer of security. But sometimes one layer isn't enough, especially when dealing with financial or sensitive information. That's why many sites have introduced a second layer – or second factor – that helps prove you are who you say you are, like sending you a text with a PIN or requesting a fingerprint. Turning on Multi-Factor Authentication (MFA) can help reduce the chances of someone getting access to your account who isn't you, ensuring the right people get in, and thieves stay out.

Multi-factor authentication

Sometimes MFA is automatically turned on – but sometimes the choice to use it is yours. We highly recommend using MFA when it's an option. See how to activate it for popular platforms:

2-Step Verification in RBC Mobile app

Google

Verification codes with Google Authenticator

Microsoft

Verification codes with Microsoft Authenticator

Two-factor authentication for Apple devices

Smartphones are smart, but they’re not always secure

If you’re like many Canadians, most of your life is on your mobile device – contacts, photos, your social media and email accounts... If someone hacked into your device and stole your personal data or locked you out of it, how would you feel?

8 steps to a safer phone

Check out these 8 simple steps to keep your mobile device secure and out of harm’s way.

1. Disable Wi-Fi when you’re not using it
2. Install a VPN and always use it when connecting to Wi-Fi
3. Install updates when they become available
4. Uninstall unused apps or apps that ask for too much information or access
5. Use biometrics with a longer passcode to unlock your device
6. Periodically erase your network settings to forget about insecure Wi-Fi networks you don't use anymore
7. Turn off Bluetooth when you’re not using it
8. Factory reset your device before returning it for service

Tips for Android devices

- Schedule regular backups
- Disable developer access
  (this is off by default)
- Disable access to third-party app stores
  (Settings > Search for Install Unknown Apps)
- Turn on the "Find my Mobile" tool so you can locate missing devices and protect data
- Set a strong Google password
- Enable multi-factor authentication for the sites you visit

Tips for iOS devices

- Turn on "Find my iPhone" to locate or wipe lost devices
- Turn off iCloud backup unless you are comfortable with your pictures being stored in the cloud
- Use iTunes to make an encrypted backup and to capture your settings
- Set a strong password

Wi-Fi safety. Nothing is free in life

That hotspot could put you in hot water

Public Wi-Fi is less secure than your private network because you don't know who set it up or who else is connecting to it. Plus, an encryption-free connection lets cyber criminals monitor and potentially access any piece of information sent between you and the server.

Here's how to protect yourself when using public Wi-Fi:

- Avoid logging into any accounts that hold private or sensitive information
- Use a secure and encrypted VPN
- Be aware of who is around you and who may be looking over your shoulder
- Keep up your other online security precautions, even if your Wi-Fi connection is secure

Tips to secure your home Wi-Fi network

1	Change the default name of your home Wi-Fi (SSID) and enable a guest network	• SSID with no personal information • Guest network separate from primary devices
2	Make your wireless network password unique and strong	• At least 20 characters long • Include letters, numbers, and symbols
3	Enable network encryption	• Turn on encryption immediately after installation
4	Turn off network name broadcasting	• Disable so only people given the SSID can access your network
5	Keep your router's software up to date	• Firmware can contain flaws that lead to vulnerabilities • Install the most up-to-date software and download latest security patches
6	Make sure you have a good firewall	• Turn on built-in firewall • Install a good firewall solution for those without
7	Use VPNs to access your network	• Internet communication is encrypted when VPN is verified

Oversharing and Geotagging. Tag, you’re it

Never click and tell

You love sharing your vacation photos. Your friends and family enjoy seeing them. However, so do thieves and scammers. Sharing your location while travelling gives criminals the perfect opportunity to target you and your belongings, putting you at risk of identity theft, physical security threats, spear phishing and social engineering.

Make sure you're protecting yourself and what matters to you.

4 steps to protect yourself

1. Set social media accounts to private
2. Disable geotagging
3. Reinforce your security questions
4. Avoid posting sensitive data like phone numbers, addresses and travel locations

Other resources

Click to secure your:

Turn off Geotagging for:

Play hard to get with strangers

The dangers of phishing and malicious emails

How phishing works

- Emails are sent from organizations or personal contacts that ask for financial or personal information.
- They often involve a financial reward, a threat towards you, or claim to be someone in need of your help.
- While you may think you're giving your information to a valid company, you're instead providing it to a fraudster!

Types of phishing

- Spear Phishing
- Smishing
- Vishing
- Business Email Compromise
- Payloads
  - Malware
  - Spyware
  - Ransomware

How to protect yourself

- Check for bad grammar, spelling mistakes, and unusual language.
- Never open attachments you were not expecting.
- Stop and think a moment before replying to any unexpected email.
- Trust your instincts – if something feels wrong, it most likely is.
- If the email appears to come from a person you know, contact them to verify the information.
- Do not give out or post any sensitive information.

Online payments. Is your cheque in someone else's mail?

Don’t be on the hook for a payment gone awry

When you need to send someone money, sending from bank to bank is the most secure. But when that’s not an option, it’s important to take steps to protect your money and your information.

7 steps to protect yourself from theft on peer-to-peer (P2P) payment apps[1]:

1. Create a complex password when setting up your account.
2. Set up multi-factor authentication – i.e. create a PIN that has to be entered before any money can be sent.
3. Link credit cards, not debit cards to minimize your risk.
4. Use a secure network and up-to-date operating system while managing your P2P payment app.
5. Accept notifications so you know when your money has been received.
6. Log out of the app after you've completed your transfer.
7. Triple-check the transaction details. Once the money is sent, it's gone – it's the same as sending cash.

Tips to avoid P2P scammers

- Do not engage with tweets claiming to be giving away money for retweeting and/or liking a tweet[2].
- P2P payment apps, such as Cash App, Venmo or PayPal, will never request money to "verify" your account, so do not accept that type of request under any circumstance[2].

Protecting children online

Growing up online comes with opportunities and risks

Your kids are going to spend time online – it is expected and even essential in this tech era. Just as you take steps to protect them in the physical world, keeping them safe in the digital world takes similar vigilance and care.

6 steps to protect your child online[3]

1. Keep devices where you can see them.
2. Set up parental controls. The SafeSearch Filters feature on Google will block sites with explicit content.
3. Know who your child's online friends are.
4. Encourage your child to ask themselves if the information or photo they want to post is something they would give to a stranger. If the answer is no, don't post it.
5. Show your child how to keep their location private.
6. Report inappropriate posts and keep information secure.

Resources

RBC:
Protecting yourself online

Other:
Protecting kids online

Glossary

Business Email Compromise	A scam where messages appear to come from a legitimate source such as a CEO or a high-ranking executive and may demand immediate action such as the transfer of funds or information.
Dedicated Payment Device	Independently managed devices used for a single purpose, such as kiosks, retail checkout, and bank ATMs.
Encryption	A way of scrambling data so only authorized users can understand the information. It helps protect the data on your network.
Firewall	A network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules.
Geotagging	The process of adding geographical coordinates or locations to various media, allowing anyone to see where you are.
Guest Wi-Fi Network	An access point on your network separate from the one your primary devices connect to. A guest network allows internet access for devices that may be more susceptible to viruses without letting them connect to your home network.
Malware	Short for “malicious software,” malware refers to software developed by cybercriminals to steal information, damage your saved files, or take control of your computer or device.
Multi-Factor Authentication (MFA)	An electronic authentication method that requires a user to present two or more pieces of evidence to gain access to an app or account. It is sometimes referred to as two-factor authentication or 2FA.
Passphrases	Phrases made up of randomly chosen words that are easy for a user to remember yet hard for a hacker to guess (for example, Delay Elephant Buy).
Password Manager	An encrypted database for passwords, which is unlocked using one master password.

Peer-to-Peer (P2P) Payments	Payment systems that allow users to send and receive money from their mobile devices through a linked bank account or credit card.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Remote Access Trojans (RAT)	A program used by intruders to take control of a computer for the purpose of performing malicious activities.
Service Set Identifier (SSID)	The technical term for a Wi-Fi network name.
Smishing	A style of phishing that targets your mobile phone. Smishing uses text messages to lure you into clicking links or downloading attachments that will install malware or try to steal your financial or personal information.
Social Engineering	The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
Spear Phishing	A phishing method that specifically targets an individual. Messages may mimic those from friends or family and contain details about you or the organizations you interact with.
Spyware	Spyware is software designed to enter your computer device, gather data about you, and forward it to a third-party. Spyware can be malicious, or it can be legitimate software that monitors your data for commercial purposes like advertising.
Virtual Private Network (VPN)	A group of computers or networks that work together over the internet to secure and encrypt your communications.
Vishing	Short for “voice phishing,” vishing involves defrauding people over the phone, enticing them to divulge sensitive information.

Sources

1. Real Simple. 2018. *This Is Exactly How to Avoid Hackers When Using Venmo and PayPal*. July 7, 2022. <https://www.realsimple.com/work-life/technology/safety-family/money-sharing-app-safety>

2. Tenable. 2020. *Scams Exploit COVID-19 Giveaways Via Venmo, PayPal and Cash App*. July 7, 2022. <https://www.tenable.com/blog/scams-exploit-covid-19-giveaways-via-venmo-paypal-and-cash-app>

3. Queensland Government. 2017. *10 Things Every Parent Can do to Keep Their Kids Safe Online*. July 7, 2022. <https://www.childrens.health.qld.gov.au/blog-10-things-keep-kids-safe-online/>

128676 (10/2022)