Bank on cyber security

How to easily secure your financial data

Online banking is a convenient way to manage your finances and investments – but instant access for you could mean easier access for cyber criminals, too. By implementing simple cyber security steps and behaviours, you can help keep your online accounts safe and your finances secure.

Canadians work hard for their money.

But they don't always know how to protect it online.

60% of Canadians worry about financial loss because of cyber crime[1]

but

only **22%** of Canadians feel prepared to face cyber threats towards their finances[1]

And when accounts are unprotected, it can add up.

$531,000,000

was lost to financial scams in 2022[2]

Keep your risk of financial scams low with these tips:

Secure your online banking profile

Use a strong password

Strong passwords use at least 12 characters, including upper- and lower-case letters, numbers and symbols.

79% of Canadians use complex passwords with letters, numbers and symbols[3]

Set up multi-factor authentication (MFA)

MFA adds an extra layer of security, like a text verification code, to keep unauthorized users out of your account.

69% of Canadians use multi-factor authentication (MFA)[3]

Use a secure network

Only use a secure Wi-Fi network or your cellular data to access your banking information, not a public Wi-Fi network.

If you **have** to connect to public Wi-Fi, always use a virtual private network (VPN) to keep your information safe!

88% of Canadians have taken precautions to protect their online accounts, devices and networks[3]

Stay safe while scrolling

26% of Canadians have been the victim of computer viruses, malware or spyware[3]

Accessing your account

- Don't log in to sensitive accounts on public Wi-Fi
- Use a virtual private network (VPN) if using an external network
- Never click on a link to access your account
- Disable autosave and 'remember me' features when inputting account information

Shopping online

- Only purchase from verified sites you're familiar with
- Learn how to spot the signs of spoofing
- Always verify the website is encrypted by checking that its URL starts with https and a locked padlock icon

Transferring money

- Only accept e-transfers from people you know
- Never include personal information in your e-transfer passwords
- Don't send e-transfer passwords through a message, email or transfer notification

Be on the lookout for

Phishing

Messages disguised as a legitimate source to get you to provide personal info or click a malicious link

Ransomware

Malware that, when opened, locks access to your files until you pay a ransom

Spoofed sites

Websites meant to look like reputable retailers, often with a similar design and URL

GET MORE TIPS TO SECURE YOUR ACCOUNTS AND DEVICES AT

GETCYBERSAFE.CA

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Sources

1. Get Cyber Safe Awareness Tracking Survey, EKOS, 2022
2. Canadian Anti-Fraud Centre, 2022
3. Get Cyber Safe Awareness Tracking Survey, EKOS, 2020

Catalogue number: D96-100/2023E-PDF | ISSN: 978-0-660-46850-5
Catalogue number: XXXX | ISBN: XX-XXX-XXXX-X