Take cyber security to the bank

How to protect your money

Opening up a bank account and being in charge of your own money is an exciting part of growing up. But, like most adult things, there are extra responsibilities and risks. If you go online or use an app to check your bank account, you need to take simple steps to keep your money safe from cyber criminals.

Kids and teens work hard for their money.

From carefully saved birthday cash to part-time jobs, you work hard for what you have.

But if you're not safe **online,** **your money** might not be safe, either.

Bank online safely with these tips:

Setting up your first online bank account?

With help from a parent or guardian, follow these cyber secure steps when opening online accounts:

Use a strong password

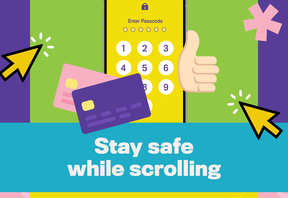
Strong passwords use at least 12 characters, including upper- and lower-case letters, numbers and symbols.

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.

Use a secure network

Don't use public Wi-Fi to check your bank account. Only **use a secure Wi-Fi network (not a free, public one at a mall or restaurant)** or use cellular data on a trusted phone.



Stay safe while scrolling

When using your banking account:

- don't use public Wi-Fi to log in to accounts that hold banking information – access those accounts with a secure Wi-Fi or use cellular data on a trusted phone
- never click on a link to access your account – access it through the official app or website
- disable autosave and 'remember me' features when entering account information

When making online, in-app or in-game purchases:

- only purchase from verified apps and websites you're familiar with
- learn how to spot the signs of spoofing
- always check if the website is encrypted by making sure its URL starts with https and a locked padlock icon

When sending or receiving e-transfers:

- 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 legit source to get you to provide personal info or click a bad link

Ransomware

Malware that locks your files when it's opened until you pay money to unlock them

Spoofed sites

Websites meant to look like real stories or banks, often with a similar design and URL

GET MORE TIPS TO PROTECT YOUR INFORMATION AND MONEY AT

GETCYBERSAFE.CA

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada
Canada.ca