CYBERSECURITY GUIDE

Practical steps to stay safer online

A free public resource from North Bay IT Services

The four words to remember

STOP. VERIFY. PROTECT. REPORT. Most successful scams and cyberattacks depend on getting you to act before you think. Slow down, verify independently, protect your accounts and devices, and report problems quickly.

What this guide covers

- Strong passwords, passphrases, password managers and multi-factor authentication (MFA).
- Phishing, text-message scams, QR-code scams, phone scams, impersonation and social engineering.
- Safer computers, phones, Wi-Fi, web browsing, online banking, shopping and social media.
- Backups, ransomware protection and the first steps to take after an account or device is compromised.
- Where Canadians can report fraud and cyber incidents, including the Canadian Anti-Fraud Centre and the Canadian Centre for Cyber Security.

A useful rule

Unexpected + urgent + asks for money, personal information, a password, a verification code, or remote access = stop and verify using a phone number, website or app you found yourself.

Who is this for?

Individuals, families, employees, volunteers and small organizations. You do not need to be a technical expert to make a meaningful improvement in your security.

This guide provides general cybersecurity awareness information. It is not legal, financial, insurance, or incident-response advice. Links and contact information were reviewed on August 31, 2026.

10 HABITS THAT PREVENT MOST PROBLEMS

1

Use a unique passphrase for every important account

Aim for at least four unrelated words and 15+ characters where supported. Never reuse your email or banking password.

2

Turn on MFA

Use multi-factor authentication for email, banking, social media, cloud storage and other important accounts.

3

Use a password manager

A reputable password manager can create and remember unique passwords so you do not have to.

4

Install updates promptly

Turn on automatic updates for your phone, computer, browser, apps and security software.

5

Verify before you click, pay or share

Open the official app or website yourself, or call a known number. Do not rely on the contact information in an unexpected message.

6

Never share verification codes

A one-time code proves that you are the person signing in. Anyone asking you to read it back may be trying to take over your account.

7

Back up important data

Keep at least one backup that is separate from your computer. Test that you can restore important files.

8

Lock and encrypt your devices

Use a PIN, password, fingerprint or face unlock and enable built-in device encryption when available.

9

Limit what you share publicly

Personal details posted online can be used to make scams and password-recovery attacks more convincing.

10

Report problems early

Fast action can reduce losses, protect accounts and help authorities connect related incidents.

PASSWORDS, PASSPHRASES & MFA

Use passphrases instead of short passwords

- The Canadian Centre for Cyber Security recommends passphrases of at least 4 words and 15 characters, or passwords of at least 12 characters when passphrases are not supported.
- Make every important account unique. Password reuse allows one stolen password to unlock several accounts.
- Avoid names, birthdays, addresses, favourite teams, common phrases, song lyrics and predictable patterns.

Example format - do not copy this exact phrase

orbit-lantern-maple-river is easier to remember and harder to guess than a short password. Use your own unrelated words and do not reuse the example.

Use a password manager

- Stores unique passwords in an encrypted vault.
- Can generate long random passwords for sites that do not support passphrases.
- Reduces the temptation to reuse passwords.
- Protect the password manager itself with a strong master passphrase and MFA.

Turn on multi-factor authentication

What MFA does

- Requires more than just your password to sign in.
- A stolen password alone may no longer be enough for an attacker.
- Enable MFA first on email, banking and your main Apple/Google/Microsoft account.

Prefer stronger methods

- Passkeys or hardware security keys are highly resistant to phishing.
- Authenticator-app prompts/codes are generally stronger than SMS.
- Any MFA is better than password-only security when stronger options are not available.

Never approve an MFA prompt you did not initiate

If you receive an unexpected sign-in approval or one-time passcode, deny it. Then change your password and review recent sign-ins. Never read a verification code to a caller or send it by text/email.

If you think a password was stolen

- Use a trusted device to change the password immediately.
- Change reused passwords on every other account that used the same or a similar password.
- Sign out of other sessions/devices if the service provides that option.
- Review recovery email addresses, phone numbers, forwarding rules and MFA methods for unauthorized changes.

PHISHING & SOCIAL ENGINEERING

Phishing is an attempt to trick you into clicking, downloading, signing in, sending money or revealing information. It can arrive by email, text message, social media, QR code, phone call or even a video/voice impersonation.

Common red flags

- Urgency or fear: “Act now,” “Your account will be closed,” “There is a warrant,” or “Your computer is infected.”
- Unexpected money requests, refunds, prizes, investments, delivery fees, gift cards, cryptocurrency or e-transfers.
- A request for your password, PIN, security answers, one-time code, banking details or Social Insurance Number.
- A request to install remote-control software or let someone access your computer or phone.
- A sender, website or phone number that is slightly different from the real organization.
- An unexpected attachment, QR code, shared document or login page.
- A request to keep the conversation secret or not contact your bank, employer, family or police.

A message can look real and still be fake

Spoofing

- Caller ID can be faked.
- Email display names and sender addresses can be imitated.
- A familiar logo or professional-looking website does not prove legitimacy.

AI & deepfakes

- Voices, photos and videos can be generated or altered.
- A message that appears to come from someone you know may still need independent verification.
- Use a known phone number or a family verification phrase for urgent requests.

The safest response

Do not use the link or phone number in the suspicious message. Close it. Open the organization’s official app, type its known website yourself, or call the number on your card, statement or official website.

Think before scanning a QR code

- Treat a QR code like a web link. It can send you to a fake login or payment page.
- Be especially cautious with unexpected QR codes in emails, texts, parking/payment notices, posters and invoices.
- After scanning, check the website address before entering any information.

COMMON SCAMS & MONEY REQUESTS

Rules that should stop the transaction

- Do not move money to a “safe account” because an unexpected caller tells you to.
- Do not buy gift cards, cryptocurrency, prepaid cards or send cash to satisfy a government, police, bank, utility or technical-support demand.
- Do not give a caller remote access to your computer or phone.
- Do not share passwords or one-time verification codes - even with someone claiming to be your bank, the police, a government agency or technical support.
- Do not pay an upfront fee to recover money you previously lost to fraud.

Scams worth recognizing

Impersonation scams

- Bank/fraud investigator: claims your account is compromised and tells you to transfer money.
- Government/law enforcement: threatens arrest, deportation, taxes or fines.
- Tech support: claims your device is infected and asks for remote access.
- Family/emergency: claims a relative is in trouble and needs money immediately.

Online & relationship scams

- Investment/crypto: promises exceptional returns or a “special opportunity.”
- Romance/relationship: builds trust and eventually asks for money or financial help.
- Marketplace/service: fake buyers, sellers, invoices, shipping notices or payment confirmations.
- Recovery fraud: offers to recover earlier losses for a fee.

Verify money requests another way

For a business payment or change in banking instructions, verify using a previously known contact method. For a family emergency, call the person or another family member directly before sending money.

Unexpected call claiming to be the CAFC or Cyber Centre?

Government agencies themselves are impersonated. The Canadian Centre for Cyber Security states that it does not make unsolicited telephone calls to individual Canadians. The Canadian Anti-Fraud Centre also warns that fraudsters impersonate the CAFC. Hang up and use official contact information you looked up yourself.

PROTECT YOUR DEVICES & NETWORK

Computers, phones and tablets

- Turn on automatic operating-system, browser and app updates. Security updates fix known vulnerabilities.
- Use the built-in security protections on your device. On Windows, keep Microsoft Defender/Windows Security and the firewall enabled unless another trusted security product replaces them.
- Install apps and programs from official app stores or the software publisher's real website.
- Use a screen lock and a strong device PIN/passcode. Enable fingerprint or face unlock where appropriate.
- Turn on full-device encryption where supported. Modern iPhones/iPads and many Android, Windows and Mac systems support built-in encryption.
- Remove software, browser extensions and apps you no longer use, especially unsupported software.

Safer Wi-Fi at home

- Change the router's default administrator password.
- Use WPA2 or WPA3 security and a strong Wi-Fi passphrase.
- Keep router firmware updated; replace very old routers that no longer receive security updates.
- Create a guest Wi-Fi network for visitors and, when practical, smart-home/IoT devices.
- Do not expose router administration or remote desktop services directly to the internet unless you know how to secure them.

Public Wi-Fi

Lower risk	Higher risk
• Reading news or other public information. • Using websites and apps that are fully updated. • Using your cellular connection when you need to do something sensitive.	• Banking, password changes or entering sensitive information on unknown/open Wi-Fi. • Ignoring browser certificate warnings. • Leaving file sharing, hotspot sharing or device discovery enabled unnecessarily.

Browser warning

HTTPS and the padlock mean the connection is encrypted; they do not prove the website is honest. Always check the actual domain name.

BANKING, SHOPPING, EMAIL & PRIVACY

Online banking and payments

- Open your bank's official app or type the known website yourself instead of following an unexpected link.
- Enable account alerts for logins, transfers and card transactions when your financial institution offers them.
- Review bank and credit-card statements regularly and report unfamiliar transactions quickly.
- For online purchases, use reputable sellers and payment methods that provide fraud protections. Be cautious when a seller insists on irreversible payment methods.
- Never send money because a caller tells you it must be moved to protect it from fraud.

Email is the key to your other accounts

- Protect your primary email with a unique passphrase and MFA.
- Review forwarding rules and recovery methods after any suspicious login. Attackers may create hidden forwarding rules to keep receiving your messages.
- Be cautious with shared-document invitations, password-reset messages and invoice attachments you did not expect.

Social media and privacy

- Limit public information such as your birthday, address, travel plans, workplace details, family relationships and answers to common security questions.
- Review privacy settings periodically. Platforms add and change settings over time.
- Do not accept connection requests solely because a profile has mutual friends or familiar photos.
- Assume anything posted publicly may be copied and used to make future scams more convincing.

When a website asks for too much

Ask whether the information is actually necessary. A shopping site usually does not need your Social Insurance Number. When possible, check out as a guest and avoid storing payment details on unfamiliar sites.

BACKUPS, RANSOMWARE & LOST DEVICES

Backups are your recovery plan

A backup protects you from hardware failure, accidental deletion, theft and some ransomware incidents. The goal is to have another copy of important data that an attacker or failed device cannot easily destroy.

- Keep important photos, documents and business files backed up to a trusted cloud service, an external drive, or both.
- Keep at least one backup separate from the computer when it is not actively backing up.
- Use automatic backups when possible, but occasionally confirm they are completing successfully.
- Practice restoring a file so you know the backup can actually be used.

> **Simple 3-2-1 idea**
> Keep 3 copies of important data, on 2 different types of storage, with 1 copy kept separate/offline or in a protected cloud service. You do not need a complicated system - you need a backup you can restore.

If you see a ransomware message

- Disconnect the affected device from Wi-Fi and wired networks if you can do so safely.
- Do not connect backup drives to the affected computer.
- Do not start deleting files, reinstalling the system or running random “fix” tools before deciding what evidence/data you need.
- Contact qualified IT/security support. Organizations should follow their incident-response plan and consider reporting significant cyber incidents to the Cyber Centre.

If a phone, tablet or laptop is lost or stolen

- Use Apple Find My, Google Find Hub/Find My Device, Microsoft Find My Device, or your organization’s management system if previously enabled.
- Change important passwords if the device was unlocked, shared, or you believe account sessions may be accessible.
- Contact your mobile carrier promptly if a phone/SIM is missing.
- For a work device, notify the organization immediately rather than trying to handle it yourself.

IF SOMETHING GOES WRONG

Act quickly, but do not panic

1	**Stop contact** Stop replying to the scammer. Do not send more money, codes, documents or information.
2	**Protect money** If banking, cards or payments are involved, call your financial institution using the number on your card or official website. Ask about freezing transactions/cards where appropriate.
3	**Secure accounts** From a trusted device, change compromised passwords starting with your primary email and financial accounts. Sign out other sessions and enable/reset MFA.
4	**Disconnect remote access** If you gave someone remote control of a device, disconnect it from Wi-Fi/Ethernet and get professional help before using it for banking or sensitive work.
5	**Preserve evidence** Keep screenshots, emails, texts, phone numbers, usernames, transaction details, dates, receipts and any case/reference numbers.
6	**Check identity exposure** If personal identity information was disclosed, contact affected institutions and consider fraud alerts/monitoring with Canada's credit bureaus.
7	**Report** Report fraud/cybercrime to local police and the Canadian Anti-Fraud Centre. Significant cyber incidents can also be reported to the Canadian Centre for Cyber Security.
8	**Warn affected people** If your email or social account was taken over, tell contacts through another channel so they do not trust fraudulent messages sent from your account.

Emergency

If someone is in immediate danger, a crime is in progress, or there is an imminent threat to life, contact 911 or your local police service.

CANADIAN REPORTING & TRUSTED RESOURCES

Use official contact information you looked up yourself. Do not trust a phone number, email address, website or QR code supplied by a suspicious caller or message.

Canadian Anti-Fraud Centre (CAFC)

Report fraud and cybercrime, whether you are a victim or a witness. Local police investigate criminal incidents; CAFC collects and shares reports to support law enforcement and prevention.

reportcyberandfraud.canada.ca

1-888-495-8501

Mon-Fri, 10:00 a.m.-4:45 p.m. Eastern
Closed holidays

Canadian Centre for Cyber Security

Canada's technical authority on cyber security. Provides guidance and accepts cyber incident reports. The Cyber Centre warns that it does not make unsolicited phone calls to individual Canadians.

cyber.gc.ca

1-833-CYBER-88 (1-833-292-3788)

contact@cyber.gc.ca

Official Canadian resources used in this guide

- Canadian Centre for Cyber Security - Information for individuals
- Cyber Centre - Best practices for passphrases and passwords (ITSAP.30.032)
- Cyber Centre - Social engineering (ITSAP.00.166)
- Cyber Centre - Contact the Cyber Centre
- Canadian Anti-Fraud Centre - Report fraud and cybercrime
- Canadian Anti-Fraud Centre - Phishing

Need help verifying something suspicious?

North Bay IT Services

Phone: (705) 773-3777 | Email: info@northbayitservices.ca | Website: northbayitservices.ca

North Bay IT Services can help you review suspicious messages, secure devices and accounts, and determine sensible next steps after a cybersecurity incident. We cannot guarantee recovery of stolen funds or replace law enforcement, your bank, or official government reporting channels.

QUICK REFERENCE: STOP - VERIFY - REPORT

Print or keep this page near your computer

STOP	VERIFY	REPORT
Do not click, pay, share a code, install software, or give remote access. End the call or close the message.	Use a trusted phone number, official app or website you found yourself. Ask a second person if you are unsure.	Tell your bank or organization quickly. Preserve evidence. Report fraud/cybercrime to police and the CAFC.

Never give these to an unexpected caller or message

- Your password or PIN
- A one-time login / MFA verification code
- Full banking or credit-card credentials
- Remote control of your computer or phone
- Money by gift card, cryptocurrency, wire transfer or a “safe account” transfer

If money is involved

Call your bank or card issuer immediately using the number on your card or official website. Fast reporting can matter.

Canadian Anti-Fraud Centre	reportcyberandfraud.canada.ca | 1-888-495-8501
Canadian Centre for Cyber Security	cyber.gc.ca | 1-833-CYBER-88
North Bay IT Services	northbayitservices.ca | (705) 773-3777

For immediate danger or a crime in progress, call 911 or your local police service.