



CANADIAN ANTI-FRAUD CENTRE CENTRE ANTIFRAUDE DU CANADA

Cyber Month Week 2: Keeping
Fraudsters Out of Your Accounts

2026-10-12

FRAUD: RECOGNIZE, REJECT, REPORT IT LA FRAUDE: IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

During Week 2 of #CyberMonth2026, the CAFC wants to help you protect your accounts in a rapidly changing digital environment. Our online accounts hold more than we may realize. Email, social media, banking, shopping and other accounts can contain personal information, financial information, saved payment details and access to other services. If a fraudster gains access to one account, they may be able to use it to access others, impersonate you or target your contacts.

Fraudsters don't always need to "hack" an account to get in. In many cases, they obtain the information they need through phishing, social engineering, stolen credentials or information exposed in a data breach. They may also manipulate legitimate security and account-recovery processes to convince you to help them gain access without realizing it.

Understanding how account takeovers happen is an important step in protecting yourself.

Phishing: stealing your information

Phishing messages are designed to look like they come from a legitimate business, organization or person. A fraudster may impersonate your financial institution, a government agency, a delivery company, an online service or another organization you recognize.

The message may claim there is a problem with your account or ask you to verify information. A link may take you to a fraudulent website designed to collect your username, password, financial information or other personal information.

Once fraudsters have this information, they may use it to access your accounts or commit other fraud.

Credential stuffing: one stolen password can put other accounts at risk

Your credentials are the information you use to sign in to an account, such as your username or email address and password.

Credential stuffing happens when stolen login information from one website is tried on other websites and services. This is often done automatically across many accounts. For example, if you use the same email address and password for several accounts and those credentials are exposed in a data breach, a fraudster may try the same combination on your email, social media, shopping or other accounts. If you reused the password, they may get in.

This is why every account should have a strong and unique password or passphrase. A password manager can also help you create and safely keep track of different passwords.



Royal Canadian Mounted Police
Gendarmerie royale du Canada



Competition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

Manipulating authentication

Multi-factor authentication (MFA) adds another layer of protection by requiring additional proof that you are the person trying to access an account. This may include a one-time passcode, authentication app, fingerprint or other verification method. Fraudsters may try to manipulate this security process.

For example, a fraudster who already has your email address or phone number may attempt to log in to one of your accounts. This can trigger a legitimate one-time passcode to be sent to you. The fraudster may then contact you pretending to be the company, a security representative or even someone you know and ask you to provide the code.

The code itself is legitimate but the person asking for it is not!

Once you provide the code, the fraudster may be able to complete the login, change your password and take control of your account. They can then use the compromised account to access information; impersonate you or target people you know.

Warning signs

Be cautious if:

- You receive a one-time passcode or password-reset notification that you did not request.
- Someone unexpectedly asks for your password, PIN, verification code or MFA code.
- You receive an email or text telling you there is an urgent problem with your account and directing you to a link.
- Someone claiming to be from a financial institution, government agency or security team asks for information to "protect" or "secure" your account.
- You receive notifications about login attempts, password changes or account activity you don't recognize.
- You are unexpectedly locked out of an account or your password no longer works.
- Messages, posts or transactions appear on your account that you did not make.
- Friends or family receive unusual messages from your account.

How to protect yourself

- Use a different password or passphrase for every account. Reusing passwords can allow one compromised account to put several others at risk.
- Enable multi-factor authentication (MFA) whenever it is available. It provides an additional layer of protection if your password is compromised.
- Never share one-time passwords, verification codes or MFA codes with someone who unexpectedly contacts you.
- Consider using a password manager to create and store strong, unique passwords.
- Don't click links in unexpected messages asking you to sign in or verify an account. Go to the organization's official website or app yourself.
- If someone contacts you about a problem with your account, end the interaction and contact the organization independently using contact information you trust.
- Regularly review your online and financial accounts for activity you don't recognize.
- If you receive a login or verification code you didn't request, don't approve the request or provide the code to anyone.
- Be cautious about the personal information you share online. It can be used to answer security questions or make an impersonation attempt more convincing.

- If you learn that your login information was exposed in a breach, change the affected password and any other account where you used the same or a similar password.

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police. Also visit the [Report Cybercrime and Fraud](#) website to report online or by phone at 1-888-495-8501.