Protecting your business

A guide to help you identify and prevent fraud.

IS YOUR BUSINESS SAFE FROM ONLINE FRAUD?

As online payment solutions evolve and become more sophisticated, so do fraudsters and their schemes. That's why it's more important than ever for business owners and their employees to understand the potential sources of fraud and take steps to help prevent it.

This guide contains the following tips and information to help keep your business safe:

Over 68%[1] of businesses report being the target of a business email compromise scam. And over half of all fraud activity involves weaknesses in internal controls, including online safety[2].

CWB
Canadian Western Bank

THREE COMMON BUSINESS SCAMS AND HOW TO PROTECT AGAINST THEM

1. BUSINESS EMAIL COMPROMISE

What is it?	Red flags	Prevention tips
A fraudster sends an email impersonating someone you have a business relationship with, such as the CEO of a supplier. The fraudster relies upon the trust that exists to gain access to funds or information.	• A request for a wire transfer or electronic funds transfer that includes a sense of urgency or secrecy. • Receiving new payment instructions for an existing payment. • An email with transaction instructions that contain unusual language, timing, or amounts than what was previously discussed. • Mail from an account that resembles a known email account, but the email address has been slightly altered. • Payment instructions to a known recipient that are different from what you previously used.	• Always confirm payment instructions in person or by phone using the phone numbers you have on record and not provided in an email. **Do not act on an email request alone, call to confirm!** • Take precautions when sharing information either online or through unsolicited phone calls that could be used by fraudsters to commit business email compromise. • Ensure you set individual user limits for your payments that are appropriate for each user. • Review and implement the security features available for CWB's products and services, such as segregation of duties that requires both an initiator and approver for your wire payments.

2. PHISHING/SMISHING/VISHING

What is it?	Red flags	Prevention tips
An authentic looking email (phishing), text message (smishing) or phone call (vishing) that appears to come from a legitimate company.	• Messages and calls that ask you to: – Validate your account – Confirm suspicious activity – Prevent your account from being suspended • Email or text messages that include a link or document that directs you to a fake website where you're asked to provide your login credentials or other confidential information.	• CWB will never send you a threatening email or demand information like your password, account number, or personal information. • Check the "from" address by hovering over the sender's name so you can see the actual email address. Many phishing attempts will look legitimate, but the email domain doesn't match the supposed sender. • Fraudsters will make unsolicited calls (Vishing) to try and obtain personal information to strengthen a phishing expedition. • Hover over links so the real URL becomes visible. If the hyperlinked address doesn't match the displayed link, it's probably a phishing attempt. Never open attachments or click on links in emails from unknown senders. • Always enter www.cwbank.com address into your browser. Do not use links embedded in emails, pop-up windows or search engines.

3. MALWARE/RANSOMWARE

What is it?	Red flags	Prevention tips
Malware is when a fraudster uses malicious software installed without your knowledge to disrupt computer operations, gather sensitive information, or access computer systems. Ransomware is a type of malware that infects computers, encrypting files and data until the victim pays a ransom.	• A suspicious looking email with a link to update software. Most software will alert you through the software itself versus an email. • Pop-ups or alerts for software you don't own on your computer or that your computer has been infected with a virus.	• Install reputable and up-to-date anti-virus and anti-malware protection software. • Ensure you're using the latest version of your operating system. • Use an external drive or cloud-based storage not linked to your computer to back-up your files frequently. • Avoid suspicious links or email attachments.

How these schemes play out

STAGE 1

Compromising victim information and email accounts

STAGE 2

Transmitting fraudulent transaction instructions

STAGE 3

Executing unauthorized transactions

STAYING SAFE ONLINE

Use the checklists below to help protect your financial transactions and reduce the risk of online fraud. We've compiled this information based on recommendations from the Government of Canada's Get Cyber Safe campaign. For more steps you can take, visit their website at https://getcybersafe.gc.ca

SECURE YOUR ACCOUNTS

- **Passphrases, passwords, and PINs**

  - ☐ Consider using passphrases. They're longer yet easier to remember than a password of random, mixed characters.
  - ☐ Passwords should be complex and unique for every account and device. Include at least eight characters with a combination of upper- and lower-case letters, and at least one number and one character other than a number or letter.
  - ☐ Never share your password.
  - ☐ Use a password manager if you have trouble remembering passwords.

- **Multi-factor authentication (MFA)**

  - ☐ MFA adds an extra step to the login process and an added layer of security to your accounts and devices. Use MFA wherever possible to increase your security.

- **Social media**

  - ☐ Social media is an easy way for fraudsters to learn about you. Make sure you protect your profile using passphrases, complex passwords, and MFA.
  - ☐ Review your privacy settings often to control who can see your posts and what information is on your profile.

SECURE YOUR DEVICES

- **Laptops and computers**

  - [ ] Install anti-virus security software and ensure it scans your computer at least once a week.
  - [ ] Keep the software updated to protect your computer and turn on automatic updates wherever possible.
  - [ ] Customize security settings for your web browser to increase security and frequently clear your cache and browser history.
  - [ ] Only download files from a source you trust.
  - [ ] Never leave your laptop in a vehicle or unattended in public.

- **Phones and tablets**

  - [ ] Keep your mobile operating system updated and turn on automatic updates wherever possible.
  - [ ] Text messages are vulnerable to malware so don't use text messages to send sensitive or confidential information.
  - [ ] Never click on links or attachments from unknown or untrusted sources.
  - [ ] Beware of apps from untrusted sources.
  - [ ] Before downloading an app, make sure to review the permissions.

SECURE YOUR CONNECTIONS

- **Private networks**

  - [ ] Make sure your Wi-Fi is secure by changing the default settings on Wi-Fi routers, using a passphrase or complex password.
  - [ ] Whenever possible, use a Virtual Private Network to encrypt data and keep all your connected devices secure.

- **Bluetooth**

  - [ ] One Bluetooth device can provide access to all your connected devices. Turn Bluetooth off when you're not using it so that fraudsters cannot detect your device and attempt to pair with it.
  - [ ] Don't connect with unknown, untrusted, or suspicious sources.

- **Firewalls**

  - [ ] Ensure your devices have the firewall turned on. Firewalls act as a guard between your device and any other device that is trying to access it through the internet. They help ensure that you control who can access your device.
  - [ ] Only install firewall protection from a credible source.

- **Public Wi-Fi**

  - [ ] Never use public Wi-Fi to access your bank account or make an online purchase.
  - [ ] Turn Wi-Fi off when not using it. Public Wi-Fi comes with increased online fraud risks.
  - [ ] Make sure you only visit websites that use the HTTPS protocol for secure communication. If HTTPS is not displayed in the website address by the browser, then look for a padlock icon at the start of the website address.

REPORTING FRAUD TO CWB

If you discover an unauthorized transaction or suspect your business has been a victim of an online fraud scheme, please **contact your banking centre or relationship manager immediately.**

For full details regarding your responsibility for any financial loss due to online fraud, including your responsibilities for ensuring the safety and security of your transactions, please refer to your account agreement.

This guide is for information purposes only and is not intended to provide legal, banking, or personalized information systems security advice and should not be relied on by the reader. We encourage you to seek qualified professional advice.

NEED MORE INFORMATION?

We're in this together. If you would like more information about how CWB Financial Group can help you protect your business against fraud, please contact your relationship manager or any CWB banking centre.

[1]Association of Finance Professionals 2022 Fraud Payments and Control Survey Available at: https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud [Accessed October 17, 2022]

[2]Association of Certified Fraud Examiners 2022 Report to the Nations Available at: https://legacy.acfe.com/report-to-the-nations/2022 [Accessed October 17, 2022]

CWB
Canadian Western Bank