CIBC

CIBC COMMERCIAL BANKING

TYPES OF FRAUD THAT CAN AFFECT YOUR BUSINESS

Fraud prevention

Client Email Compromise (CEC)

CEC occurs when a fraudster gains access to a user's email account and obtains knowledge of the user's interactions with the bank and other contacts. The fraudster proceeds to impersonate the client by either using the client's email account or by setting up an account resembling that of the client. Their access is then used to send requests to the user's financial institution(s) or other contacts, requesting banking access changes and sending payment instructions in an attempt to exfiltrate funds.

Business Email Compromise (BEC)

BEC occurs when a fraudster impersonates someone known and trusted by their victim, such as a vendor or company executive. The fraudster then uses that relationship in order to deceive the victim into providing key information that the fraudster later uses for the purposes of misdirecting funds. The scam ultimately concludes with a seemingly urgent request for funds that, without proper verification, are sent to the fraudulent destination.

Criminals may contact a company via phone, email or text and impersonate government, businesses or essential services such as:

- Financial institutions requesting banking information (i.e., Visa or Mastercard)
- A government health agency such as Health and Human Services, the World Health Organization or a local hospital requesting personal information
- A law enforcement agency demanding immediate payment in the form of cryptocurrencies like bitcoin, gift cards, or any money-sending service, such as a wire transfer
- A utility company or service provider asking for funds due to a late payment or unexpected charges

Ransomware

Ransomware is commonly delivered to victims through malicious websites and emails. Social media channels can also be a point of entry for bad actors. Ransomware is essentially a computer virus that makes a copy of critical files on a victim's connected computers or servers. The files are then sent to the fraudster, and a virus encrypts all of the original files on the network. Once the virus encrypts the information, the fraudster will contact the victim demanding a ransom in exchange for decrypting the files and committing to keeping the stolen information confidential. Even if the victim pays, fraudsters may choose to sell the data to other fraudsters to be used in the future.

Report fraud and scams

Have you encountered any of these signs of fraud?

Report any suspicious activity immediately to your relationship manager or to the Customer Service: 1-877-448-6500

or visit CIBC.com Privacy & Security Policy

Preventative measures and best practices

Fraud prevention is about being proactive. Having a fraud prevention and cybersecurity plan in place can help your organization better prepare against financial fraud. Today, criminals are targeting organizations with various types of fraud, knowing that many of those organizations are increasingly vulnerable. Staying informed is the first line of defense against becoming a fraud victim. The following preventative measures and best practices will limit fraud risk exposure against common fraud attempts.

- Verbally confirm any payment instructions, especially changes to employee payroll instructions and vendor or supplier payments. Be sure to use a known phone number and avoid using contact information contained within the request itself.
- Typically, you will not be asked to provide banking or personal information. Be cautious with whom you share your personal information, such as your Social Security Number or banking information.
- Never share your PINs or passwords with anyone.
- Change passwords often, and be sure to use strong passwords that have a combination of uppercase letters, numbers and special characters.
- Be cautious of using password managers.
- Establish role-based access controls and dual approval on payments.
- Use multifactor authentication when possible.
- Implement system logging controls.
- Implement timely bank account reconciliation and resolution of discrepancies.
- Keep checks in a safe place and eliminate "windowed" envelopes for mailing them.
- Having backup files physically disconnected from the network is key to recovery for most victims of a ransomware attack.
- Keep your software, including your operating systems and applications, up to date. Use antivirus or anti-malware software.
- Be suspicious of unfamiliar screens or requests from websites and applications that you regularly use.
- Implement measures for detecting compromises and develop a cybersecurity incident response plan.
- Think before you click! Do not open email attachments or click on links from senders you do not know.

These tips are provided for informational purposes only. Please consult with professional fraud prevention experts for further advice tailored to your organization.

Cyber insurance

Once you've taken the necessary preventative actions and applied best practices to protect your business from cyberattacks, cyber insurance can also be considered as an additional protective measure. There are many variations and types of cyber insurance coverage, which can be multifaceted and highly customizable. For more information about cyber insurance, visit the Federal Insurance Office.

Speak to your insurance broker about the types of cyber insurance and coverages that are specific and appropriate for your business.