CIBC COMMERCIAL BANKING

TYPES OF FRAUD THAT CAN AFFECT YOUR BUSINESS

Fraud prevention

Client Email Compromise (CEC)

CEC is when a fraudster gains access to a user's email account and gains 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 is 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, Visa / Mastercard, requesting banking information
- A government health agency such as Health Canada, the World Health Organization or a local hospital requesting personal information
- The CRA, or law enforcement agency demanding immediate payment in the form of cryptocurrencies like Bitcoin, gift cards, or any money sending service such as a CIBC Global Money Transfer or a wire transfer
- A utility company or service provider asking for funds due to a late payment or unexpected charge

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 which makes a copy of critical files on a victim's connected computers / servers on the network. The files are then sent to the fraudster, and then virus encrypts all of the original files on the network. Once the virus encrypts the information, the fraudster will contact the victim asking for a ransom in exchange for decrypting the files and committing not to using or disclosing the information stolen. Fraudsters may also sell the data they obtained during a ransomware attack to other fraudsters so it can be used in the future.

Report fraud and scam

Have you encountered any of these signs of fraud?

Report any suspicious activity immediately to your Relationship Manager or to the CIBC Business Client Centre fraud line: 1-800-500-6316

or Visit CIBC.com Privacy & Security Policy

Preventative measures & 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 for various types of fraud, knowing that many of them 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 when there changes to employee payroll instructions, and changes to vendor / supplier payments. Be sure to use a known unchanged 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 Social Insurance Number (SIN) or banking information
- Never share your PINs or passwords with anyone.
- Change passwords often, and ensure to use strong passwords that they have a combination of upper case letters, numbers and special characters
- Be cautious of using password managers
- Establish role-based access controls and dual approval on payments
- Use multi-factor authentication when possible
- Implement system logging controls
- Implement timely bank account reconciliation and resolution of discrepancies. Contact the CIBC Business Contact Centre immediately for any transaction (Wires, EFT, cheque) that you believe are unusual / unknown transaction
- Safeguard cheque stock and eliminate "windowed" envelopes for mailing cheques
- Having a back-up of 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 anti-virus or anti-malware software.
- Be suspicious of unfamiliar screens or request from websites / 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 information 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 multi-faceted and highly customizable. For more information about cyber insurance, visit the Insurance Bureau of Canada.

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