Fraud prevention playbook

A guide to the common types of fraud experienced by small businesses and middle market companies

In this playbook, you will find:

Background information on scams

Whether you are an owner, a manager, or an employee, one thing is certain: you work hard for your business. Your cybersecurity systems and fraud prevention measures should work just as hard too.

When everyone takes an active responsibility to recognizing and rejecting fraud, your business will be better protected against cybercriminals.

so·cial en·gi·neer·ing
/ˈsōSHəl ˌenjəˈni(ə)riNG/

The use of psychology to manipulate our human instinct to respond to urgent requests and fear, so that victims are lured into revealing confidential information that may be used to commit financial fraud.

The basis of many scams

Fraudsters, also commonly referred as cyber-criminals, use **social engineering** tactics in order to take advantage of and obtain confidential information on its victims. These tactics are often in the form of suspicious emails, calls and text messages that may impersonate family members, clients, vendors or other employees or service providers. Once they obtain this information, they will use it to commit financial fraud and deplete their victim's funds.

Here are three key characteristics of social engineering techniques:

Using fear as a motivator by sending threatening emails, phone calls or texts to scare you into revealing information or conducting transactions

Urgent and unexpected requests for personal or business information through written communications, such as email or text messages

Offers, prizes or contests that sound too good to be true, often claiming to provide a reward in exchange for login credentials or other personal or business information

Types of scams that may target your business

1. Business Email Compromise (BEC) scams

In BEC scams, **fraudsters exploit employees of companies who have the authority to conduct business transactions** by pretending to be a known vendor or employee. They may successfully overtake the authentic email of the vendor or create an email account that is very similar and then contact your business requesting payments to services or products to an account owned by the fraudsters. The two most common forms of BEC scams are CEO and Senior Executive scams, wherein the fraudster poses as an executive of the business and requests personal information or a transfer of money to an account, and invoice scams, which are described below. "Phishing" is a term used to describe attempts to lure individuals into providing sensitive information such as account numbers or passwords.

2. Fake invoice scams

A form of BEC fraud, invoice scams are two-fold: the fraudster may pose as a known vendor **requesting your business to provide updated billing information**, or request payment for an upcoming invoice that is **out of line with your business' typical billing cycles**. Unbeknownst to your employees that it is fraud, they release the funds to the fraudster, often resulting in irrevocable funds that your business is now held liable for.

3. Ransomware

In ransomware fraud, **malicious software (malware) is installed on your computer** that allows a fraudster to remotely lock your important files and prevent access to them. This data may also be extracted and used for other fraudulent purposes in the future. Victims of this scam will often receive pop-up messages stating that the files are locked and **demanding a ransom be paid** by sending untraceable funds to the fraudster's account in order to regain access to your documents.

Note: ransomware is often installed onto a computer when the victim clicks on a suspicious link from a phishing email or a popup window from a suspicious website. In some instances, it may request the victim to download an embedded file, masking as a software download. "Vishing," like phishing, is used to lure individuals into providing sensitive information but instead of through email, it is conducted by phone.

4. Merchant scams

In a merchant scam, fraudsters disguise themselves as a legitimate entity **claiming to offer free product samples or sell products they do not actually carry**. They may call or email your business requesting a wire transfer, credit card information and an address before shipping the merchandise. **Once funds or sensitive information is sent to the fraudster, they cease all contact with you** and do not ship the products as advertised. Many small and medium businesses have been hit by merchant scams particularly during the COVID-19 pandemic, where scammers claim to sell face masks in exchange for funds.

The 5 best practices you can implement right now to help protect your business against fraud

1. Verify payment instructions received via email or telephone

Always read payment instructions and requests to change account payment details with skepticism, whether through email or telephone. Ensure your employees contact a known representative of your vendor(s) that they have previously spoken to, at a phone number on file. You may also want to consider coordinating a face-to-face method of payment confirmation details via Microsoft Teams, Skype, or other secure technologies.

2. Educate your employees on fraud and Know Your Client (KYC) procedures

Teach your employees about cybercrimes and fraud trends so that they can distinguish between real and fake communications. Furthermore, empower them to practice Know Your Client (KYC) procedures when conducting business. These include:

- Understanding who your business' clients are and whether emails or requests from them make sense
- Having a phone call verification process with trusted contact numbers between your CIBC Business Advisor and clients, so that transactions can be verified and suspicious activity investigated

3. Ensure your cybersecurity systems are robust and up-to-date

Run system scans on your computers with antivirus software regularly to detect and remove malicious software from your devices and use a firewall to block unauthorized access to your business' networks. Do your research to ensure that you are using up-to-date operating systems and cybersecurity protection. Back up your business' information to a secure cloud or other backup software to keep them secure from potential ransomware and cyberattacks that may occur to your computer.

4. Slow down. Don't rush.

Fraudsters are demanding and want you to act quick. Maintain control of any situation by slowing down; think carefully about what is being asked of you and whether it makes sense. Investigate any requests for personal information and verify that it is legitimate before giving it out.

5. Establish strong internal controls over who manages your business' data

It is important to limit authority and handling of confidential data to a select few, especially in a small business. Implement controls such as:

- Restricting employee access to financial data, computer records and inventory
- Using audit trails to track all financial transactions and regularly checking them
- Enforcing multi-person sign-off for expense claims, overtime, cheque writing, and payroll functions

Know your fraud, before it knows you

Please contact CIBC at 877-448-6500 immediately if you believe you have been a victim of fraud, your business accounts have been compromised, or your identity has been stolen.

Protect your business

Fraud prevention is about being proactive, educating your employees on the risks they can be exposed to, and being aware of all documents, online activity, and purchases that your business makes. Having a fraud prevention and cybersecurity plan in place can help your business better prepare against financial fraud.

Additional resources

Cybersecurity and Infrastructure Security Agency (CISA)
Cyber resources
https://www.cisa.gov/uscert/resources

Free cybersecurity services and tools
https://www.cisa.gov/free-cybersecurity-services-and-tools

Ransomware
https://www.cisa.gov/stopransomware

National Institute of Standards and Technology (NIST)
Cybersecurity framework
https://www.nist.gov/cyberframework

Federal Communications Commission (FCC)
Cyberplanner and the cybersecurity tip sheet
https://www.fcc.gov/cyberplanner

Federal Trade Commission (FTC)
Cybersecurity for small business
https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

Association of Certified Fraud Examiners (ACFE)
Fraud prevention check-up
https://www.acfe.com/fraud-resources/fraud-prevention-check-up

Federal Bureau of Investigations (FBI)
Fraud alert poster
https://www.fbi.gov/file-repository/fraud_alert-2.pdf/view

Scams and safety
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

For more insights and ways CIBC can help simplify banking for your business, please visit us.cibc.com.