Protect Your Organization and Employees From Cyber Fraud

An email asking you to confirm your social insurance number. A text message asking you to provide your phone number and address to confirm delivery of a prize. A social media chat asking you to re-enter your password to update your account.

These are just three examples of cyber fraud that people deal with every day. Cyber fraud is definitely on the rise and now is the ideal time to keep the conversation going with your colleagues, friends, and family members about realities of fraud and cyber fraud.

Here are a few things you should consider when you want to increase the knowledge level of cyber fraud: what it is, what are the types of cyber fraud, what are the signs of cyber fraud, and what are cyber fraud prevention best practices.

> “The digital economy is changing the way Canadians work, live and interact. Being connected also means that our exposure to fraud has grown exponentially. No one is immune to fraud, so everyone should learn to protect themselves, and know that reporting can help prevent more harm.” Josephine Palumbo, Deputy Commissioner of the Deceptive Marketing Practices Directorate, Competition Bureau of Canada

Fraud Facts for 2020

The Canadian Anti-Fraud Centre collects information on fraud and identity theft. This agency is a powerful resource, providing stats and details on the latest cyber fraud and fraud scams.

Based on its data and research, the centre says the impact of fraud so far this year as of January 31, 2020 is:

- 3,493 Canadian reports of fraud (46,317 in 2019)
- 2,020 Canadian victims of fraud (19,285 in 2019)
- $4.2M lost to fraud ($98M in 2019)

These stats emphasize why it is so important to have consistent communication, training, and cyber security awareness training. To further underscore the prevalence of fraud, consider this alert on the Canadian Anti-Fraud Centre website:

> ### Have you received a call from 1-888-495-8501?
>
> This is the toll free number for the Canadian Anti-Fraud Centre and it's being spoofed. No representative from our office is trying to reach you. Fraudsters are masking their phone number with ours.
>
> When you miss a call and the caller doesn't leave a message, don't return the call. if it's important, they'll call you back. If it's a long distance number, you could be charged long distance fees.

What Are the Types of Cyber Fraud?

The types of cyber fraud range from email messages, spoofed or faked websites, malicious website popups, text messages, social media chats, and other social engineering tactics.

The Royal Canadian Mounted Police (RCMP) has a broader definition of cyber fraud that includes a wide range of fraud schemes, types, and scams:

> *The Royal Canadian Mounted Police (RCMP) generally interprets cybercrime to be any crime where cyber – the Internet and information technologies, such as computers, tablets, personal digital assistants or mobile devices – has a substantial role in the commission of a criminal offence. It includes technically advanced crimes that exploit vulnerabilities found in digital technologies. It also includes more traditional crimes that take on new shapes in cyberspace.*

These types of cyber fraud are a common threat to anyone, regardless of where you work or live:

Phishing

Phishing is cyber fraud that uses deceptive emails, websites, and text messages to steal your confidential and personal information. Using convincing language, cybercriminals trick people into giving up personal

information such as their social insurance number, address, credit card information, passwords, and date of birth.

A common example of phishing is identity theft. A cybercriminal sends an email that looks like it comes from a company you do business with and asks you to update your password. This makes it easy for the cybercriminal to log into your account and steal your credit card information, address, and phone number – just the information needed to commit fraud in your name with your account.

Spear Phishing

Spear phishing uses targeted emails to carry out cyber fraud against a business or individual. Both approaches use specific targeted emails written to appear to come from a business, colleague, or partner that the recipient is familiar with. Spear phishing is a personalized approach to phishing that typically includes personal information about the recipient.

A common spear phishing example includes a cybercriminal sending an email to two or three people in your organization. The email appears to come from the recipients' manager, and it asks them to provide confidential company information that the manager cannot access because they are traveling.

Business Email Compromise (BEC)

BEC is a savvy email scam that targets employees who regularly send wire transfers to their partners and customers. BEC uses spoofed email accounts to trick victims into sending wire transfers to faked accounts or recipients. BEC emails typically impersonate company executives or accounting departments of partners or clients.

The bogus invoice scheme is a common example of BEC. The cybercriminal spoofs the email address of a company email account that is frequently used to request invoice payments and fund transfers. The recipient recognizes the email address and doesn't hesitate to transfer the funds. Unfortunately, the funds are transferred to an account associated with the cybercriminal.

Ransomware

Ransomware is a type of cyber fraud that holds data for ransom. Access to data on computer networks, mobile devices, and servers is locked until the victim pays a ransom.

A common ransomware attack method uses a spear phishing email. A carefully worded email is sent to the victim urging them to download a file that has important company information. This file installs ransomware on the computer and potentially the entire network, shutting it down until payment is made.

CEO Fraud

CEO Fraud is a sophisticated email scam that uses savvy emails impersonating the company CEO or other company executives that asks employees, typically in HR or accounting to help out by sending a wire transfer.

A common example of CEO fraud requires the cybercriminal to do research about the targeted organization and email recipient. Using tools like LinkedIn or Facebook, the criminal learns enough about the company structure, who reports to who, and the travel schedule of executives. With this information, the cybercriminal sends a faked email from the CEO who is away on business asking someone in the accounting department to quickly transfer money to a new client or they risk losing the business.

The common thread connecting these types of cyber fraud is social engineering. Social engineering is a manipulation technique used by cybercriminals to trick recipients into giving up information. Social engineering relies on the human instinct of trust and our human need of wanting to help to convince people to provide confidential and personal information.

8 Cyber Fraud Prevention Tips and Best Practices

People are your first line of defense against cyber fraud. The more your colleagues, friends, and family members know about cyber fraud, the safer everyone is.

Share these eight cyber fraud prevention tips and best practices with your colleagues, social network, friends, and family members:

1. Be click aware. Think twice before opening and responding to an email from a recipient you don't recognize. When in doubt – delete and ignore.
2. Pay attention to details. Take a close look at the spelling of the email address, the company URL, and the link details.
3. Ask questions. Before installing a software update or responding to a request from a colleague, talk to the sender in person. Pick up the phone or walk over to your colleague's desk and ask them about the request.
4. Slow down and read. Cybercriminals know you're busy and receive a lot of email, so they hope you won't read their email too carefully. Look out for spelling errors, awkward use of language, and urgent requests.
5. Keep your computer and devices up to date. Install operating system, browser, and app updates. Companies like Microsoft, Apple, and Google send these updates to fix known security flaws or to improve the security of your computer or device.
6. Shop carefully. Cybercriminals know that most of us shop at the big online retailers and send emails that pretend to offer special deals from your favourite retailer. However, the links to these deals take you to a faked website that steals your information, your money, and potentially installs ransomware. Always visit the online retailer website directly by entering the URL in your browser.
7. Never use free public Wi-Fi. Do not shop, do online banking, or send emails on an open public Wi-Fi network. You do not know who is operating this network and it's very easy for cybercriminals to spy on the network and steal your information and transaction details. Always use secure, password protect Wi-Fi – or better yet, wait until you're home or at work and connected to trusted Wi-Fi.
8. Do not give out personal information. No Canadian government agency will email (or phone) you asking you to send them personal information. Do not respond to any emails that ask you for your mailing address, phone number, social insurance number, tax information, or credit card details.

Learn more about fraud prevention and cyber fraud with these resources:

- Canadian Centre for Cyber Security
- Canadian Anti-Fraud Centre
- Stop Scams and Frauds USA Gov
- IdentityTheft.gov
- European Anti-Fraud Office

TERRANOVA SECURITY