Northbridge® Insurance | CYBERSCOUT A TransUnion® Brand

RISK INSIGHTS

AN OVERVIEW OF SCAMS

WHAT ARE SCAMS?

Scams are everywhere as criminals try to cash in by stealing money or valuable personal information from victims. And given our modern reliance on technologies like smartphones and the internet, if you haven't been a victim of a scam, you've likely been targeted by one.

Definitions of scam terms

There are four key terms that are important to understand when discussing scams:

- **Scam:** a fraudulent operation that has the intention of stealing money or valuable financial or personal information
- **Social engineering:** the techniques used to manipulate a victim into divulging information or taking a specific action
- **Phishing:** when a scammer poses as a legitimate person or company online with the intention of stealing money or personal information
- **Vishing:** when a scammer poses as a legitimate person or company over the phone with the intention of stealing money or personal information

Many modern scams try to push their victim into a corner, so they're forced to make a decision on the spot—i.e. pay the money or provide personal information, or face the consequences. Scammers will use recent headlines to fuel their scams, they'll pose as a local retailer that you frequent or even a family member in need in hopes that you'll give up your money or your personally identifiable information (PII).

Analysis of scam terms

Social engineering

Scammers continue to fine-tune their social engineering skills, coming up with new ways to convince you to hand over your money and PII. A few techniques that scammers use include:

- **Familiarity:** If you've seen someone around or heard their name before, you're more likely to trust that they are legitimate. (Ex: An email appearing to be from a big-name company or representative of your financial institution).
- **Hostility:** It's human nature to avoid conflict by complying with aggressive people. If you consider somebody as a threat, you may be more likely to do what they tell you. (Ex: A call from somebody posing as a police officer demanding a fine be paid in exchange for the expunging of an arrest warrant).
- **Playing detective:** It's easier than ever for someone to gather information about you. By going onto your social media accounts, they can find your location and interests. They also can rummage through your trash for credit card forms and bank statements. There are many places that cybercriminals can obtain your personal information that can help in their scams.

Phishing, vishing, and smishing

- Scammers frequently apply their social engineering techniques in online, phone and text messaging scams—respectively known as phishing, vishing and smishing. According to Statistics Canada, about one-fifth of Canadian businesses were impacted by cyber security incidents in 2021.[1]
- Phishing, vishing and smishing scams are the most common types of cyber attacks worldwide. Phishing can be executed on several different platforms: emails, phone calls or text messages, and deceptive websites.

Phishing

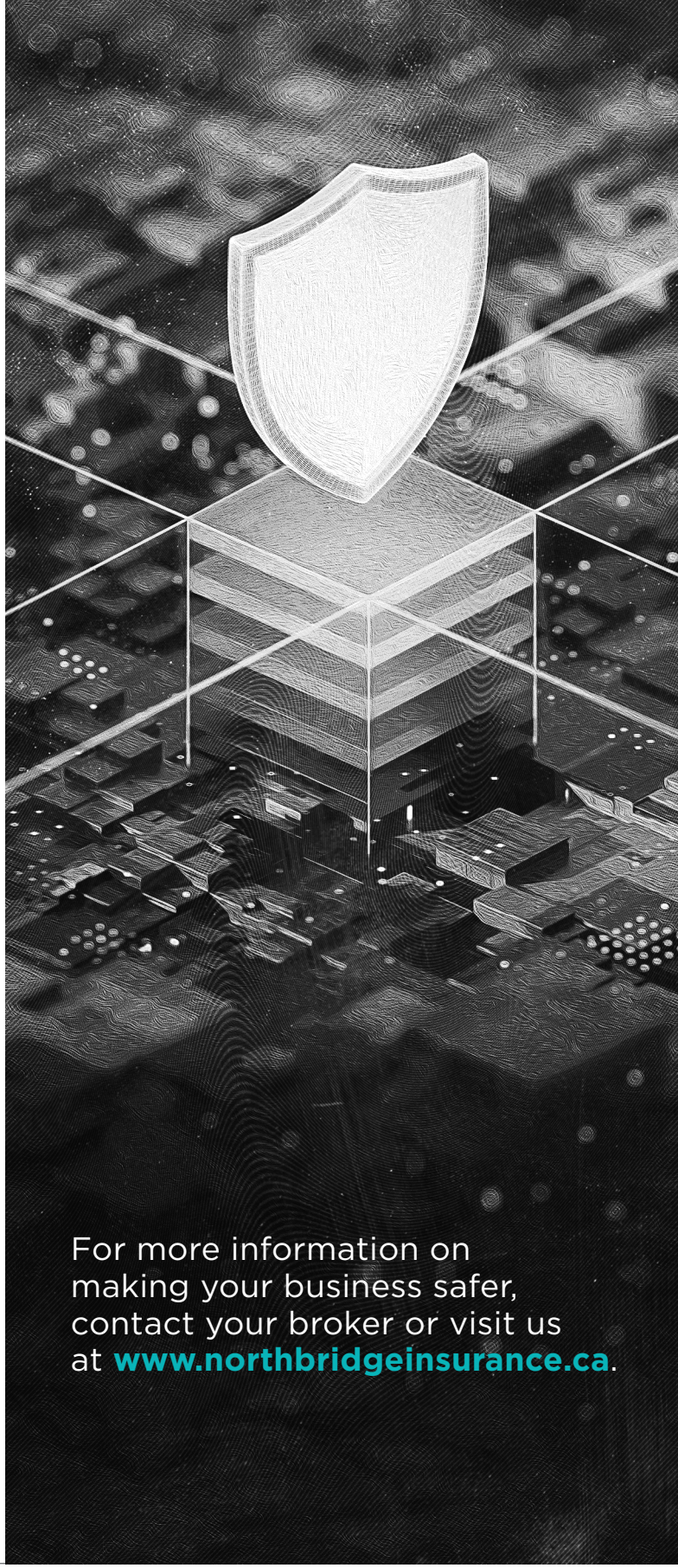
- Phishers create emails that are seemingly legitimate and rely on you to click on the link provided. These emails are designed to look official and often create a sense of urgency, so victims act quickly, clicking an embedded link before thinking. Those links typically send you to another fraudulent page, usually bearing legitimate businesses' logos or brand names to further convince you of its authenticity. Phishing emails can also launch damaging malware or spyware that is activated after clicking a link, sometimes without you even being aware.
- Phishing websites are designed to look like legitimate sites in order to fool visitors into inputting information such as a credit card number, email address, phone number, Social Insurance Number, etc. Anyone who is convinced that the site is legitimate is more likely to divulge personal information to scammers.

Vishing

- Vishing, or voice phishing, is a form of phishing by phone. Scammers will pose as a bank representative, a friend of a friend, a restaurant or another trusted person in an attempt to steal your money or PII. The difference between phishing and vishing is the platform that the scam is presented through. Rather than answering unexpected calls, today it is easy for everyone to hide behind a call screener, making vishing slightly less common than email or text scams.

Smishing

- Smishing is when a scammer sends links by SMS or text message to unsuspecting victims, similar to a phishing email. Given the shorter nature of a text message, smishing attacks try to get the victim to click on the link by offering more details to claim a prize, a refund or other messages to create urgency on behalf of the recipient.



For more information on making your business safer, contact your broker or visit us at **www.northbridgeinsurance.ca**.

[4046-001-ed03E | 05.2023]

[1] Statistics Canada, Impact of cybercrime on Canadian businesses, 2021.

Northbridge® Insurance | CYBERSCOUT® A TransUnion® Brand