What is phishing and how can you prevent it?

Submitted by **Reza Kamrani, Account Representative, Associations** | www.federated.ca

You don't always need a sophisticated hack to gain access to into a business' database. In fact, all it could take is one click in an email to compromise your data security. Fraudulent emails, phone calls, and text messages are all common mediums for phishing attacks that cybercriminals use to hack and steal sensitive information.

These attacks can cause a business to experience reputational damage with clients and customers, financial losses, data leaks, or even legal trouble. That's why it's important to educate yourself and your employees on what phishing schemes are and what to look out for to help protect your business from this growing threat.

What is phishing?

Phishing is a type of cybercrime where fraudulent communications are used to trick users into revealing sensitive information, like passwords or credit card information.

Phishing attempts can occur through a number of different mediums, including email, phone calls, text messaging, or even faxing. Sometimes phishing schemes will target large groups of users at once, employing a strategy known as "volume mailers," or they'll be more specific and direct their efforts toward a business area, such as a call center or finance department. In some instances, they'll even target their phishing emails or phone calls to a specific role (e.g. a finance clerk) or individual. For instance, they may reach out to the CFO or someone in accounting since they have the most direct access to the company's finances.

Examples of common phishing scams

The more emotionally charged the message, the more likely you'll click or comply before really considering all the details. The most recent approach is to use the COVID-19 pandemic in phishing scams and take advantage of people who are worried about the virus.

Scammers have been seen to pose as health professionals, claiming to represent organizations like The Canadian Red Cross or World Health Organization (WHO), to send out false information. The goal is to trick people into clicking malicious links in order to steal sensitive information from your database. However, it doesn't end at emails, messages connected to COVID-19 can also come in the form of spam phone calls and text messages.

Other examples of common phishing schemes include impersonating the Canada Revenue Agency, especially during tax season, or impersonating members of law enforcement.

How to spot a phishing email

It's vital that all employees know how to spot a phishing email, so they don't accidentally click a dangerous link or send out information they shouldn't. Learning a few quick tricks on how to spot a suspicious email can save your business a lot of money and time in the future. Below, we outline some tips:

- **Be suspicious:** First, ask yourself a few questions like, "Was this an email I was expecting?" or "Do I normally do business with this person?" Sometimes phishing emails are meant to make us panic, claiming things like information has been stolen and then offering a quick fix. Be wary of emails like this, as they're generally a scam.

- **When in doubt, proofread:** Sometimes hackers will miss spelling mistakes and incorrect grammar. Read any communications you receive very carefully, and if you do spot some mistakes, be wary.

- **Check e-mail addresses and links:** Some phishing emails will be sent from email addresses you can immediately tell are not legitimate. In other cases, you may have to use your mouse to hover over the name of the email sender to see the address it came from. If someone claims they are emailing you from a trusted financial institution, but their email address doesn't end in that institution's name, that could be a red flag. It's also important to hover over any links that are included in the email to make sure the URL matches the one it purports to lead to.

- **Be on the lookout for calls to action:** In order for a phishing email or phone call to be successful, they need the recipient to take some sort of action, whether that be providing your login credentials, clicking a link, or performing a certain task. Be on the lookout for calls to action. Does the email request information from you? Does it ask you for your username or want you to log in to a website to access something? Does it contain links or password, an attachment you weren't expecting? If it does include any of these requests, use some of the other tips provided to make sure it's from a legitimate source.

Help protect your business

Despite all of your precautions and employee training, sometimes a phishing email or phone call can be successful and lead to a range of problems for your business. You may have to deal with financial losses, data leaks, reputational damage with clients and customers, or even legal trouble.

Cyber risk insurance can help with the costs of some of these issues and ensure your bottom line isn't negatively impacted. Visit our cyber risk insurance page today to learn more about how we can help your business!

Reza Kamrani is the Account Representative for Associations at Federated Insurance.