Risk Insights

Working Remotely? Follow These Five Tips to Avoid a Phishing Scam

As more employees are working remotely in the wake of the COVID-19 pandemic, businesses are being targeted by an increasing number of phishing campaigns.

Follow these five tips to keep your e-mail and your business protected from cyber threats:

01. DON'T SEND SENSITIVE INFORMATION VIA EMAIL

E-mail is convenient and universal, but it's not an especially secure way to send information. Avoid sending sensitive information like tax forms, credit card numbers, bank account information, or passwords via email.

02. CALL TO CONFIRM REQUESTS

Any time money or information is requested via e-mail from a colleague or employer, take an extra minute to call them on the phone to confirm the request. It could very well be a business e-mail compromise (BEC) scam, which has cost businesses worldwide, including Canadian businesses, more than $5 billion dollars.*

03. TAKE YOUR TIME

Phishing scams targeting businesses are often marked urgent or time-sensitive and rely on the target responding too quickly to notice anything suspicious. Take the time to double- and triple- check any e-mail that's trying to get you to urgently click on a link or open an attachment.

04. ENABLE TWO-FACTOR AUTHENTICATION

Two-factor authentication prompts a user to verify their identity by sending a code via text message or e-mail. This adds an extra level of security to e-mail and other sensitive accounts. It's not perfect, but it can prevent an account takeover, especially if a user has a weak password, or one that has been used on other accounts.

05. UPDATE YOUR SECURITY SOFTWARE

While many employees are staying quarantined at home, some don't have reliable or fast Internet access and need to rely on either public or shared Wi-Fi. A well-secured VPN connection means that employee data is encrypted and harder to intercept when being transmitted through a shared or suspect Internet connection.