Protecting your business: Employee awareness guide

Here is some important information about common business scams to keep in mind while you're working.

Anatomy of a scam: social engineering

Many of the scams targeting businesses fall under the category of "social engineering." This is a process by which scammers commit financial fraud by relying on the act of manipulation and our natural desire to help or respond to urgent requests.

Social engineering allows fraudsters to make it past security protocols by taking advantage of our human vulnerabilities.

Phishing, vishing, and smishing

Phishing is a form of social engineering in which hackers use fake emails to trick recipients into providing personal or financial information that can be used for fraudulent purposes.

Vishing is the telephone equivalent of phishing. It's the act of using the telephone in an attempt to scam the user into surrendering sensitive information that can be used for identity theft or financial gain.

Smishing is another form of phishing in which fraudsters send a text or SMS message to try to obtain sensitive information or trick the recipient into clicking a malicious link and downloading malware onto their device.

Spear phishing and business email compromise (BEC)

Spear phishing is a more targeted type of phishing, designed to trick individuals or small groups into sharing information or allowing malicious code to run on their devices. This technique uses more sophisticated technology and personalization to evade email filters, as well as manipulation tactics to lure recipients into providing sensitive information or granting unauthorized access to accounts or systems.

Business email compromise (BEC) targets companies conducting regular payment processing activities, taking advantage of employees with access to sensitive company or customer data and those responsible for vendor management and payment processing activities. Employees will receive emails requesting an immediate money transfer, a change of account number or invoice, or access to sensitive data.

Fraudsters often disguise themselves as a trustworthy contact to acquire sensitive information, typically through email or other online messaging.

Forged emails (also known as spoofed emails) are sent from scammers claiming to be in senior management, either a Chief Executive Officer (CEO), Chief Financial Officer (CFO), or a trusted vendor and may request a money transfer, account change, or access to unauthorized data, accounts, or systems.

Scotiabank®

Protecting against phishing, vishing, or smishing scams

- Remember that these scams often **contain urgent or provocative requests** and are disguised as legitimate organizations or other sources that are familiar to you
- **Always check the sender:** watch out for emails where the email address doesn't match the company supposedly sending the email
- **Stop and consider** whether a sense of urgency is truly warranted
- Slow down and **carefully evaluate emails**, phone calls, or text messages requesting sensitive information, changes to account details, or unauthorized access
- **Verify the validity** of the person or organization contacting you by reaching out to them directly by phone using a known contact number
- **Be wary of links or attachments** that you weren't expecting
- Before clicking a link, check its destination by **hovering over** it with your cursor; if you don't recognize where the link is taking you, don't click

Malware

Malware, short for "malicious software," refers to any software designed to steal sensitive data and damage or destroy computers and computer systems.

There are many different types of malware that exist, including viruses, worms, Trojan horses, spyware, adware, and ransomware. Ransomware is an extremely popular type of malware affecting businesses today, which can attack and encrypt (lock) systems with the aim of extracting a ransom.

Downloading an infected program is the most common way to unintentionally install malware on your systems. Because malware is designed to look legitimate, it's easy to mistake it for a genuine program that you might actually want on your computer.

Malware can also be installed by opening an attachment, downloading an attachment, or selecting a link in an email or text message.

Protecting against malware

- Make sure that you have **anti-virus or anti-malware software** activated on your devices and that you install updates as they become available
- Always install the **most recent operating system** on your systems and devices
- Only download programs from **legitimate sources** that are approved by your organization
- Make sure you frequently **update and patch systems**, as updates usually contain security patches to keep you safe
- **Use the internet with caution** and look out for signs of a fake website, which can include poor design and formatting, no company contact information, pop-up windows, and fake error messages
- Always be wary of attachments or links from unknown sources

Scotiabank®

Wire fraud

Wire payments continue to be a target for fraudulent activity because of the speed and higher dollar limits of the transaction. Employees who are responsible for processing wire transfers are deliberately targeted.

Common methods of wire payment fraud include business email compromise (customer email hack / vendor email hack), account takeovers, malware, and phishing (including smishing and vishing).

A common wire payment scam occurs when a fraudster sends an email pretending to be a trusted vendor requesting a change of wire payment instructions or account information. The email may request a change of account payment details, so funds are sent to an account the fraudsters control, or the email includes a malicious link that downloads malware onto your device and network.

Protecting against wire fraud

- **Never rush** when processing wire payment requests, even if the request is urgent
- Take the time to **confirm the validity** of a wire payment request and make sure all protocols are followed before a transfer is initiated
- **Validate** any unusual transaction requests by using a trusted phone number for the contact in question
- Conduct **regular reviews** of wire transfer transactions
- **Know the habits** of your customers and vendors, including the frequency and amounts of their regular transactions

Report all suspicious wire transfer requests to your manager; make sure to document all communications and maintain a list of contacts.

Scotiabank®