How to Detect a Phishing Campaign

Each year, cybercriminals get smarter and find new ways to get personal information from online users. A common method cybercriminals use is phishing campaigns. Phishing is an attempt by a third party to solicit confidential information from an individual, group or organization by mimicking or spoofing a specific brand, usually for financial gain.

Statistics Canada determine that more than 1 in 3 Canadians have received a phishing attack. Because it's so common, it's important for people to be able to recognize the warning signs of a phishing message.

The following are email elements to look out for when spotting phishing messages:

1. The Message Asks for Personal Information.

Anytime an email, text or phone call asks for personal information, it should raise suspicion. Sometimes it can seem difficult to say no, especially if the email looks like it is from a supervisor or someone else of authority, but it doesn't hurt to be cautious. Contact the person or organization that supposedly sent the information to verify the message. Most legitimate organizations will never ask for personal information via email or text.

2. The Message Involves a Threat.

The sender of a phishing email wants the recipient to take some sort of action, and they usually do this by using a threat, such as pursuing legal action if the request goes unanswered. It is natural to want to respond to this type of email but think carefully about whether it is a legitimate request.

3. The Sender is Suspicious.

When receiving a strange email, take a look at the sender's email. While the name might look legitimate, the email itself might have some clues. Phishing email addresses are often misspelt or do not match the normal naming structure of the organization from which it is pretending to be.

4. The Sender Wants a Link to be Clicked.

Oftentimes, phishing campaigns want the recipient to click on a malicious link to a website or to download a file in an attempt to get information off the user's computer or network. Do not click on any links unless it's known for sure it is from a legitimate source.

To learn more about different ways to prioritize cybersecurity, or for questions specific to your business, please reach out to your local advisor.

LET US HELP YOU MANAGE YOUR RISK

LOCATIONS

Edmonton: 1.800.665.5243

Calgary: 1.866.845.8330

Kelowna: 1.800.665.5243

lloydsadd.com

navacord.com

info@lloydsadd.com

Local Touch. National Strength.™