Phishing: Don’t Be the Catch of the Day

Welcome to week two of Cyber Security Awareness Month! This week, we are diving into social engineering and how it can result in phishing, smishing, and vishing attacks. If you recall from last week’s article, we talked about how social media can provide information someone can use in a social engineering attack against you or your organization. But what does that mean? And what would an attack look like?

Refresher: Social Engineering

Social engineering is the use of deception to exploit human nature, our habits, and our trust in order to gain information or access to information systems. Threat actors want to obtain confidential information such as passwords and login credentials, or personal information.

Gone Phishing!

Phishing is the most common form of social engineering attack. Phishing occurs when a threat actor impersonates a trusted entity through email to try and fraudulently get information or access to systems. Being caught in a phish could mean clicking on a link, providing information, opening an attachment, downloading a file, or providing remote access to a workstation.

Throwing Back the Phish

It is important to know what to look for to detect a phishing attack. Here is what to look for:

- Comes from an unknown user, organization, or domain name which is the unique name that appears after the @ sign in an email address.
- Comes from someone within the organization, but with a non-organizational domain name.
- Expresses an unusual level of urgency.
- Contains errors such as misspelled names, misused organizational terms, or misrepresented logos.
- It has attachments with unusual file names or links.
- Driven by a motivation such as a financial benefit or another benefit.

Smish of the Day

Smishing is a form of phishing that uses text messages instead of email. Smishing is also known as SMS phishing because messages can arrive by SMS (short message service) such as iMessage, Facebook Messenger, WhatsApp, and other messaging platforms.

No Smish for Me, Thanks!

- Do not reply to the text message, call the number, or click on any links in the message.

- Look up the phone number and message to see if others have received similar messages.
- Contact the organization or person directly- inquire about whether the message you received is legitimate.

Caught in the Vishing Net

Vishing is a form of phishing that uses phone calls instead of email. Vishing is also called voice phishing. Vishing occurs when a threat actor impersonates a trusted entity over the phone to fraudulently obtain sensitive information or access to systems. Threat actors disguise their phone numbers to make it appear like they are calling from a legitimate institution.

Don’t Be a Vishing Hook, Line, and Sinker

- Be aware of unsolicited phone calls from institutions or people asking you for sensitive information.
- Verify suspicious phone calls by hanging up and calling the institution back through their published customer service number or call the person back with a verified phone number.
- Never provide your social insurance number, password, or PIN over the phone, or take actions on your computer when directed over the phone.

Recent Phishing Trends

Did you know that during the same six-month period at the start of the COVID-19 pandemic, 34 percent of Canadians experienced a phishing attack? Meanwhile, 14 percent of respondents received phishing emails that were related to COVID-19. It is important to think about how current events can bait us in a phishing attack! For more information, check out these resources on Social Engineering.