CYBERSECURITY ESSENTIALS

Identifying and Responding to Phishing Scams

Phishing is a type of cyberattack that utilizes deceptive electronic communications to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. While emails are the most common delivery method of phishing scams, cybercriminals may also use text messages, social media interactions, fake or misleading websites, or even phone calls.

Employees are often targeted by phishing scams because they have access to valuable corporate systems, funds and data. These scams are among the most prevalent cybercrimes, with billions of phishing emails distributed each day. When these scams occur, they can lead to costly and disruptive cyber incidents, including data breaches and ransomware attacks. This article outlines common types of phishing scams, highlights red flags to watch for and explains what to do when you come across a suspicious message.

Common Phishing Scams

Top phishing tactics and formats include the following:

- **Deceptive phishing** is when a cybercriminal impersonates a recognized sender to steal personal data and login credentials. These emails often trick recipients by asking them to verify account information, change a password or make a payment.
- **Spear-phishing** schemes are typically aimed at specific individuals or companies and use personalized information to convince recipients to share their data. In these instances, cybercriminals will research a target's online behavior—such as whom they report to in their department and the co-workers they speak to most—to collect personal details that make them seem legitimate.
- **Vishing,** or "voice phishing," occurs when a criminal calls a recipient's phone to get them to share personal or financial information. These scammers often disguise themselves as trusted sources, such as a bank or the IRS, and rely on creating a sense of urgency or fear to trick a target into giving up confidential information.
- **Smishing** refers to "SMS phishing" and incorporates malicious links into SMS text messages. These messages often appear to be from a trustworthy source and lure recipients in by offering a coupon code or a chance to win a free prize.
- **Pharming** redirects a target to a website of the cybercriminal's choosing by installing a malicious program onto their device. The goal is to have users input their login credentials or personal information, such as credit card numbers, on the fraudulent site.

Red Flags to Watch for

Here are some red flags you can watch for to help identify potential phishing scams:

- **Unknown or copycat senders**—This includes unverified numbers, profiles or email addresses, especially those claiming to be trusted individuals or organizations. Some cybercriminals may even hack into real

CONNOR & GALLAGHER OneSource
Insurance | Benefits | HR | 401k

Provided by Connor & Gallagher OneSource

accounts or copy legitimate email addresses, only changing one character.

- **Threatening, generic or error-ridden language**—These messages may contain an unnerving sense of pressure or urgency, pushing you to take immediate action on a specific matter to obtain a reward or avoid potential consequences. They may also lack personalized greetings (e.g., "Dear account holder") or use poor spelling or grammar.
- **Unsolicited links or attachments**—This includes hyperlinked words and images with mismatched URLs and password-protected files with uncommon file extensions (e.g., .exe, .zip, .scr, .iso or .jar) or vague naming conventions. You should be particularly wary of opening links or attachments that you didn't initially request.
- **Sensitive requests**—These messages may ask you to disclose private information, such as your login credentials or workplace records, or demand that you perform unusual tasks, such as using company funds for wire transfers or downloading new software.

Handling Suspicious Messages

If you receive an unusual or off-putting message and suspect a phishing scam, take the following steps:

- **Don't interact.** Refrain from responding to the message, answering any prompts, or opening embedded links or attachments.
- **Verify the request.** If the message claims to be from a trusted individual or organization and includes a sensitive request, use an alternative method (e.g., a verified phone number or email address) to contact the supposed sender and verify the request.
- **Report it.** When you are unable to verify a message, report it immediately. Depending on the message's nature and format, this may entail forwarding it to designated IT staff or using a built-in email alert system (e.g., a "report phishing" button) to flag it for further review.
- **Delete it.** Once the message has been properly reported, be sure to remove it from your inbox (including the trash or spam folders), if applicable.

For More Information

Cybersecurity can be challenging, but you don't have to navigate it alone. Reach out to your employer for more information on cybersecurity best practices.