The 8 Things You Need to Understand About Phishing

1. What is Phishing?

Phishing is a type of fraud in which a hacker attempts to gather personal information by impersonating a legitimate source or by sending users to a malicious web site. Hackers try to obtain any information that could help them pose as someone else, usually to steal money or intellectual property. This is done either through the surreptitious installation of malware, impersonating a legitimate site and stealing login credentials, or simply via a conversation.

2. The sender of that email may not be legitimate

Your employees should never trust an email based simply on the purported source. Cyber criminals have many methods to disguise emails. They understand how to trick their victims into thinking a sender is legitimate, when the emails are really coming from a malicious source.

3. Enticing or aggressive subject lines are used to lure people in.

Cyber criminals will do whatever it takes to get people open their emails. They often use enticing or threatening language in subject lines that urge immediate action. They may promise “free iPhones to the first 100 respondents,” or threaten that “your credit card will be suspended without immediate action.” Evoking a sense of panic, urgency, or curiosity is a commonly used tactic.

4. Impersonal greetings should be a red flag.

Since phishing emails are often sent to many people at once, they usually lack personal greetings. They often use generic terms like “customer,” “employee,” or “patient.” Your employees should be cautious of these terms especially if the email is asking for personal information.

5. That it is important to notice grammatical and stylistic errors.

Employees need to read their emails carefully, not just skim them. Many phishing attacks come from other countries, so these emails are often written by non-native English speakers. This results in a plethora of grammar and stylistic issues. If an email from a supposedly reputable company has spelling and grammar issues, it is probably a scam.

6. It is important to check the link destination.

Make sure your employees hover over all links before clicking them. Pop-up bubbles will display the link's real destination. If it is not the website expected, it is probably a phishing attack. It is most important to make sure that the core of the URL is correct. Be especially cautious of known websites suddenly ending in alternative domain names instead of .com or .org.

7. Emails demanding "immediate action" are probably scams.

Emails that have an aggressive tone or claim that immediate action must be taken should be considered a potential scam. This technique is often used to scare people into giving up confidential information.

8. You can't rely on images or logos.

Images can be downloaded or easily replicated. Brand logos and trademarks are no guarantee that an email is real. Even anti-virus badges can be inserted into emails to persuade victims into thinking there is no real threat. None of these add any actual legitimacy to an email.

Example of a COJUSD received phishing email:

---------- Forwarded message ----------
From: [redacted]
Date: Wed, Jun 6, 2018 at 11:20 AM
Subject: Re: Fwd; Incident Report 05062018!
To:

To All Staff;

If you received a message yesterday saying to provide your login details. Please respond your Username (_____) and Password (_____) immediately, so we can change it and send the New Password regulations to you. If you did not receive it also provide your login information! Failure to do this may result in your account not been able to receive Emails. You can also contact the Office/HelpDesk to do it in person.

©2018 IT ServiceDesk