PHISHING AWARENESS TRAINING

INTRODUCTION

Phishing is a form of social engineering technique where attackers deceive their targets into revealing their sensitive information or installing malware such as viruses, worms or ransomware.

There are various types of phishing attacks some of which are;

****Email phishing:**** the general term given to any malicious email message meant to trick users into divulging private information. Attackers generally aim to steal account credentials, personally identifiable information (PII) and corporate trade secrets. However, attackers targeting a specific business might have other motives.

* ****Spear phishing:**** these email messages are sent to specific people within an organization, usually high-privilege account holders, to trick them into divulging sensitive data, sending the attacker money or downloading malware.
* ****Link manipulation:**** messages contain a link to a malicious site that looks like the official business but takes recipients to an attacker-controlled server where they are persuaded to authenticate into a spoofed login page that sends credentials to an attacker.
* ****Whaling (CEO fraud):**** these messages are typically sent to high-profile employees of a company to trick them into believing the CEO or other executive has requested to transfer money. [**CEO fraud**](https://www.proofpoint.com/us/threat-reference/ceo-fraud) falls under the umbrella of phishing, but instead of an attacker spoofing a popular website, they spoof the CEO of the targeted corporation.
* ****Content injection:**** an attacker who can inject malicious content into an official site will trick users into accessing the site to show them a malicious popup or redirect them to a phishing website.
* ****Malware:**** users tricked into clicking a link or opening an attachment might download malware onto their devices. Ransomware, rootkits or keyloggers are common malware attachments that steal data and extort payments from targeted victims.
* ****Smishing:**** using SMS messages, attackers trick users into accessing malicious sites from their smartphones. Attackers send a text message to a targeted victim with a malicious link that promises discounts, rewards or free prizes.
* ****Vishing:**** attackers use voice-changing software to leave a message telling targeted victims that they must call a number where they can be scammed. Voice changers are also used when speaking with targeted victims to disguise an attacker’s accent or gender so that they can pretend to be a fraudulent person.
* **“**Evil Twin” Wi-Fi:**** spoofing free Wi-Fi, attackers trick users into connecting to a malicious hotspot to perform man-in-the-middle exploits.
* ****Pharming:**** [**pharming**](https://www.proofpoint.com/us/threat-reference/pharming) is a two-phase attack used to steal account credentials. The first phase installs malware on a targeted victim and redirects them to a browser and a spoofed website where they are tricked into divulging credentials. DNS poisoning is also used to redirect users to spoofed domains.

**Urgent call to action or threats** - Be suspicious of emails and Teams messages that claim you must click, call, or open an attachment *immediately*. Often, they'll claim you have to act now to claim a reward or avoid a penalty. *Creating a false sense of urgency*is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a trusted advisor who may warn you.

**How To Identify Phishing Attacks**

**First time, infrequent senders, or senders marked [External]** - While it's not unusual to receive an email or message from someone for the first time, especially if they are outside your organization, this can be a sign of phishing. Slow down and take extra care at these times. When you get an email or a Teams message from somebody you don't recognize, or that Outlook or Teams identifies as a new sender, take a moment to examine it *extra*carefully using some of the measures below.

**Spelling and bad grammar** - Professional companies and organizations usually have an editorial and writing staff to make sure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.

**Generic greetings** - An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.

**Mismatched email domains** - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.

**Suspicious links or unexpected attachments** - If you suspect that an email message, or a message in Teams is a scam, *don't open any links or attachments*that you see. Instead, hover your mouse over, but *don't click* the link. Look at the address that pops up when you hover over the link. Ask yourself if that address matches the link that was typed in the message. In the following example, resting the mouse over the link reveals the *real*web address in the box with the yellow background. The string of numbers looks *nothing like* the company's web address.

**Preventive Measures**

Below are a few ways you or your organization can prevent being a victim of phishing:

* ****Train users to detect a phishing email:**** a sense of urgency and requests for personal data, including passwords, embedded links and attachments, are all warning signs. Users must be able to identify these warning signs to defend against phishing.
* ****Avoid clicking links:**** instead of clicking a link and authenticating into a web page directly from an embedded link, type the official domain into a browser and authenticate directly from the manually typed site.
* ****Use anti-phishing email security:**** artificial intelligence scans incoming messages, detects suspicious messages and quarantines them without allowing phishing messages to reach the recipient’s inbox.
* ****Change passwords regularly:**** users should be forced to change their passwords every 30-45 days to reduce an attacker’s window of opportunity. Leaving passwords active for too long gives an attacker indefinite access to a compromised account.

**Case Study**

**John Podesta email hack (March, 2016)**

**Overview Of The Attack**

On March 19, Podesta received an email from “no-reply@accounts.googlemail.com” — a user falsely posing as Google, notifying Podesta that his password had been compromised by someone in Ukraine. The email provided a bit.ly link to change the password. Seemingly suspicious and rightfully so, Podesta forwarded the email to his chief of staff, who then passed along the email to the campaign’s IT team. This is where things went so painfully wrong: The campaign’s IT team wrongly saw the email phishing for Podesta’s password as genuine, instructing him to change his password.

To the IT team’s credit, they did send along a correct Google link not the original phishing email’s bit.ly link to change Podesta’s password and instructed him to add two factor-authentication to his account for an added level of password security. But the legitimate Google link did not seem to make it to Podestain time , and instead he used the “poisoned link,” giving his password to hackers and opening up his personal email to unwelcome eyes.

**Impact Of The Hack**

**1. Strong impact on 2016 Election**

Since John Podesta was the campaign chairman for Hilary Clinton the phishing attack had a major impact on Hilary Clinton’s campaign leading to voter distrust due to some of the content of the emails

**2. Strengthened Russian US Election Interference claims**

It was later established that the hack was orchestrated by Russian hackers .Therefore the hack strengthened claims that Russian federation had influence in US elections.

**3. Exposed Cybersecurity Weaknesses**

Podesta fell for a simple phishing attack which tells how high-profile people are vulnerable to hacking. A better understanding of security awareness on the path of John Podesta could have prevented the hack. It is important to note that security is everyone’s responsibility and must not be limited to IT teams only