Don’t Take the Bait in 2021

By Brian Johnson

2020 was a difficult year, unprecedented in many ways. As organizations across all industries scrambled to implement work-from-home strategies, healthcare organizations faced the COVID-19 pandemic head on. Hospitals and medical practices focused on caring for patients, but sadly cybercriminals pounced on the opportunity to attack. Among all industries, healthcare saw one of the largest increases with a 42% rise in hacking incidents[1]. IBM reported, in the X-Force Threat Intelligence Index 2021, that across all industries, phishing emails provided the initial entry point 33% of the time.[2] Based on its ease of use and high success rate, phishing is a longtime favorite of cybercriminals who are financially motivated, attacking those who they perceive as most likely to pay a ransom. Knowing that healthcare facilities rely on their information systems to treat patients and that any down time could negatively impact patient care, cyber criminals ramped up their ransomware attacks hoping for a big payday during the pandemic. Given this trend, it is important to understand phishing emails and the threat they impose on healthcare. This article will break down the anatomy of a phish, discuss common traits, identify the red flags and methods to identify a phish, and discuss defense and mitigation of phishing attacks.

In its simplest form, a phish is any attack that is delivered via email. The objective of the attack will vary, but the most common include ransomware, credential theft, fraud, and theft of intellectual property. For you to be duped, the cybercriminals need to develop a relevant and realistic email to pique your interest. Phishing emails are as much psychological as they are technical in nature. Security professionals use the term “social engineering” to describe the tactics used by phishing. These tactics rely on your human nature and social tendencies, tricking you into divulging sensitive information, clicking malicious links, downloading malware, and unknowingly enabling fraud.

Phishing emails impersonate brands, companies, people, and processes you trust. Next, they play on emotional triggers that manipulate your social tendencies that include authority, urgency, fear, duty, and a desire to be helpful. For example, cybercriminals often impersonate a CEO, CFO, or other important figure in your organization. For some, a rightly worded email from the “CEO” will induce several emotional triggers.

To help identify a phish, examine the **To** and **From** addresses of an email. Sometimes the email is not even addressed to you, other times you might be included in a long list of recipients that have no relation. Examining the **From** address can help uncover impersonation attempts. For example, you probably know your CEO’s email address because it follows a common naming convention particular to your company. Emails that come from any other addresses pretending to be your CEO, such as CEOname@gmail.com, are a phish.

Misspellings, grammatical errors, and spelling variations are other phish red flags. The cybercriminals behind phishing emails are often operating in a foreign country where English is not the primary language, and this will often come through in the message. Spelling variations such as using an S instead of Z are also clues about the person behind the email.

Phishing emails often contain malicious hyperlinks and attachments. Hyperlinks can lead to fake login pages where cybercriminals harvest your username and password, or potentially lead to a website that downloads malware, such as a backdoor or ransomware, to your computer. Attachments can also contain malware designed to compromise your computer. It is very easy for a cybercriminal to create a hyperlink that displays one address but goes to another. Hovering the cursor over a hyperlink will always show the true destination address. Look for identity and brand mismatches. For example, if an email says, “Elizabeth has shared a file with you,” and it is branded with a Dropbox logo with a hyperlink displaying www.dropbox.com, when hovering over the hyperlink, it will display a Dropbox address. Conversely, a phishing link will display and unrelated address with no resemblance to Dropbox.

When examining an email, you want to review all the red flags and establish an overall context for the message. Knowbe4 provides a convenient one-page printout that shows all the red flags.[3] When looking at context, ask yourself the following questions: Do I know this person? Is the email address correct? Does the tone of the message make sense? Where do the hyperlinks go? Does the attachment align with the subject of the message? If something feels wrong, follow your gut, and do a little more investigating. Never reply to the email because you might be talking to the cybercriminal directly. Often, someone replies to a compromised email account asking if the attachment is legit, and the cybercriminal kindly replies, “yes.” The best option is to call the individual using a number you have on file, not a number contained in the message.

Now that you are familiar with the composition of a phish and the tactics used by cybercriminals, it is time to develop a plan to mitigate and defend against phishing attacks. First, bring awareness to your team. Let them know what phishing is and that the organization is a target. Next, educate your employees on the red flags and how to recognize phishing emails. The best way to recognize a phish is to experience them firsthand, but in a safe environment. Knowbe4 has an image library comprised of real phishing emails.[4] Look at their examples and see if you can recognize the red flags. Many organizations test their employees using a paid solution that sends safe phishing emails and tracks the results. Paying for a solution might not appeal to you, but most solutions offer a free test or trial period. Lastly, encourage your employees to report suspicious emails. Many email solutions now have built-in features to report suspicious emails. If your email solutions do not offer a reporting feature, encourage your employees to ask for help when an email does not feel right. This could be forwarding it to your information technology department or another employee for a second opinion.

Phishing continues to be a favorite attack vector for cybercriminals and is predicted to

increase over the next several years. Assess your current situation and determine your organization's ability to detect and combat phishing emails. Do not delay, start implementation of awareness training to avoid becoming the next attack statistic. SVMIC members have access to educational content that covers phishing and other cybersecurity topics at **vantage.svmic.com**.

[1] HIPAA Journal, https://www.hipaajournal.com/2020-saw-major-increase-in-healthcare-hacking-incidents-and-insider-breaches

[2] IBM X-Force Threat Intelligence Index 2021, https://www.ibm.com/security/data-breach/threat-intelligence

[3] KnowBe4 Red Flags Printout, https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf

[4] KnowBe4 Phishing Examples, https://www.knowbe4.com/covid-gallery-phishing-examples