HealthTech

Source Material: https://healthtechmagazine.net/article/2020/10/phishing-attacks-healthcare-4-proven-ways-prevent-breach

by Mike Chapple

Mike Chapple is associate teaching professor of IT, analytics and operations at the University of Notre Dame.

OCT 01 2020

SECURITY

Phishing Attacks in Healthcare: 4 Proven Ways to Prevent a Breach

Innocuous-sounding messages from cybercriminals can pose a major security threat. Learn to spot (and avoid) trouble.

Healthcare professionals aren't immune to phishing scams.

In a study published last year in the Journal of the American Medical Association, researchers sent almost three million simulated phishing -messages containing innocent subject lines such as "Mandatory online workplace safety training" and "Someone sent you a Halloween e-card" to hospital employees.

Many recipients fell for the trap: An astonishing 422,062 clicks occurred. That's 1 out every 7 phishing emails sent during the study, over a seven-year period.

More than one-third of health IT staffers don't conduct phishing tests, despite nearly twice that number (59 percent) citing email as the most common point of compromise, according to the 2019 HIMSS Cybersecurity Survey.

The prevalence of these incidents presents a serious risk. A stray click might seem harmless, but it could easily lead to the installation of malicious software on a hospital system or compromise a staffer's credentials.

Here's how hospitals can take action to reduce their vulnerability to phishing attacks.

1. Minimize the Amount of Information Available

Many phishing attackers search for easy targets by scouring websites for email addresses and other contact information that they can use to feed their spam machines.

Healthcare organizations should take care to ensure that they don't publish staff directories or other contact information on their public websites to avoid falling victim to these vacuum cleaner-style approaches to phishing.

Incident Response
Online publishing directories and organizational charts can also fuel more sophisticated spam campaigns, known as spear-phishing attacks. In these attacks, phishers aim for quality over quantity, seeking out specific targets and designing carefully crafted email campaigns using the names of senior administrators or other key details to give them an air of legitimacy.

IT teams should look at the public materials they present to the world through the lens of an attacker. Are they giving away information that presents little public benefit but might be useful in crafting phishing attacks?

Reducing the amount of publicly available data minimizes the organization's public profile and reduces the likelihood of a successful phishing attack.

2. Train Your Workforce for Cyber Incidents

Phishers depend on employees to act as the weak link in the security chain by clicking a link or responding to a message.

Employee education and awareness is an important pillar of any campaign to protect against these attacks, helping employees recognize suspicious messages and react properly. These educational campaigns should include real examples of phishing attacks experienced by the organization to lend credibility and urgency.

Avoid "naming and shaming" individual victims of an attack, but make it clear that real employees have fallen victim to transforming the threat of phishing from a theoretical boogeyman to a real threat that has compromised their colleagues.

READ MORE: Get tips on how to conduct tabletop exercises in advance of a cybersecurity incident.

The JAMA phishing study included a valuable finding: Repeat exposure to phishing simulations helps employees recognize attacks.

Hospitals conducting their first five phishing simulations experienced a median click rate of 25.1 percent, the study found. Those running more than 10 campaigns found that click rate almost halved, at 13.4 percent.

3. Filter Out All Suspicious Content

Technical controls can also help stop phishing attacks by preventing them from reaching their targets in the first place.

Healthcare providers running their own email systems should ensure those systems use the best available filtering to block inbound phishing attempts. This includes using phishing blacklists that quarantine inbound messages from known spam sources. Sending these messages to the digital dustbin eliminates the chance that an employee will inadvertently click a malicious link.

Stay Protected
Still, some messages will inevitably slip through the cracks and land in a user's inbox. Filtering technology can also help blunt the impact of these messages by restricting the URLs that users may visit in their web browsers.

Similar to email filters, URL filters restrict access to the malicious websites attackers use to harvest user credentials, install malware or perform other dangerous actions.

4. Deploy Multifactor Authentication for Your Organization

The goal of most phishing campaigns is simple: Steal the usernames and passwords of the organization's employees.

After clicking the link in a message, the victim might be redirected to a legitimate-looking website asking them to log in to the system for more information. That site, run by the attacker, serves only to harvest passwords for use in attacks against other systems belonging to the target organization.

One of the best ways to diminish the effectiveness of a phishing campaign is to reduce the value of the credentials they harvest.

Healthcare organizations that have not already deployed multifactor authentication to protect user accounts should consider doing so immediately. This is commonly done by requiring that users possess a specific, registered device to complete their logins, thereby rendering the credentials stolen in phishing attacks fairly useless and reducing the likelihood that attackers will continue to target the organization.

Providers who take these diverse and assertive steps will find themselves well-prepared to avoid the devastating impacts of a digital compromise.