Revenue Cycle Advisor
powered by HCPro
ComplyAssistant

Phishing trends to monitor in 2021

April 5, 2021 | Briefings on HIPAA

One year into the coronavirus (COVID-19) pandemic, phishing attacks against healthcare organizations remain a chief concern. Threat actors are constantly finding new vulnerabilities to exploit. It's like a game of whack-amole: When healthcare organizations swat away one problem, another pops up.

In March, Cofense, a Virginia-based network security company specializing in phishing detection and response solutions, released its Annual Phishing Report, providing a comprehensive look at cybersecurity trends in 2020 as well as a breakdown of how different sectors stack up against one another.

The report found that the majority of sectors were mostly targeted by credential theft attempts. Malware and business email compromise made up a smaller percentage of the attacks.

In healthcare specifically, 59% of the phishing attempts were in the form of credential theft, while 15% were business email compromise and 5% were malware. The percentage of business email compromise attempts in healthcare was higher than any other sector listed, including education, administrative, real estate, public, and finance. Though malware generates a lot of headlines, the percentage of malware attacks against healthcare organizations (5%) is lower than the percentage of malware attacks against other sectors such as construction (31%), real estate (17%), utilities (16%), and finance (14%).

Let's take a closer look at the numbers and what the trends of 2020 might mean for healthcare going forward.

Healthcare at risk

How does healthcare compare to other sectors in the report?

As **Jason Tahaney**, director of technology at Community Options in Flemington, New Jersey, points out, healthcare provides a treasure trove of data for bad actors. A 2019 CBS News report indicated that Social Security numbers sell for $1 on the dark web, while credit card information sells for up to $110 and patient medical records can command as much as $1,000. The reason for that last price tag? Records contain the full set of sought-after information: date of birth, place of birth, credit card details, Social Security number, physical address, and email addresses.

"Some of the sectors listed—banking, financial—learned early on that they were targets," says **Jay Hodes**, president and founder of Colington Consulting in Burke, Virginia. "I think [the] healthcare sector is still catching up."

Hodes looks at healthcare through two separate lenses: the larger organizations and the small to mid-sized providers. The latter are the weakest links, simply due to a lack of resources. In many small organizations, the task of cybersecurity is dumped onto the plate of an employee who is already juggling multiple other responsibilities.

Those organizations should be diligent in seeking out OCR cybersecurity guidance at a minimum. Utilizing some of the tools ordered by OCR, such as the cybersecurity checklist, and signing up for the OCR Privacy and Security listservs can provide an organization with a strong starting point. From there, organizations can implement more advanced training methods to educate the workforce on the ever-evolving nature of phishing attacks.

Combatting credential theft

The Cofense report indicated that credential theft is by far the most common type of phishing attack deployed against healthcare organizations. Experts agree that this should come as no surprise.

"Seeking healthcare credentials is the easiest way in," says Hodes. "If you can obtain user credentials, that's your gateway in."

The No. 1 defense against credential theft is getting employees to recognize what the phishing attempts look like. In other words, their antennas should go up if they click on a link that takes them away from the organization's system and asks for a username and password.

Although this sounds simple, many employees can be tricked. Hackers often spoof the Microsoft login page, for example, stealing the logo for their page in hopes that an employee—perhaps not fully paying attention—will enter credentials without recognizing that they're on an unfamiliar URL.

"We're asked for passwords all the time," says Tahaney, who previously served as the director of information technology at Hunterdon Medical Center in Hunterdon, New Jersey. "You go into autopilot mode, unfortunately. It's just training to have that pause. If you're clicking a link in an email that is taking you out of your organization and prompting you to use your password, that's what you really have to highlight."

Gerry Blass, president and CEO of ComplyAssistant in Colts Neck, New Jersey, says healthcare credential theft attempts may be on the rise for a reason.

"I think we all know healthcare over the past year has been so distracted by the pandemic," says Blass. "Implementing telehealth, and the remote workforce as well, all that leads to the attackers being highly motivated and doing different attacks. They would expect that they could be successful in healthcare due to the environment. I wouldn't think other industries are as distracted as healthcare workers, overall."

As a result, organizations must strike the balance of getting the proper information and training to employees, but not overburdening them with so many reminders that they begin to tune out the message.

A step as simple as implementing standard once protocol can go a long way, says Hodes. If an email or link looks suspicious, employees should be trained to call the sender and verify that they sent it. If your organization utilizes Offce 365® as its platform, the recipient can right click on the email, bringing up an extensive toolbar, hover over the "Report Spam" option, and then follow the arrow to "Report Phishing." Other platforms over similar capabilities.

In addition to training employees to flag suspicious emails, organizations can consider the following options.

Branded login page. As shown in the Cofense report, bad actors can easily mimic the generic Microsoft login page. They will have a much more diffcult time duplicating a page that has a unique logo, however. Office 365 gives organizations the capability to use custom logos on login pages, a feature that Tahaney's organization has utilized. This way, employees become accustomed to seeing the company logo on the login page. Many credential theft attempts will simply use the Microsoft logo; they are casting a wide net hoping to get a few employees to bite. Organizations that take the time to use branded logos on their login pages instead of the typical Microsoft logo will have a leg up against credential theft attempts.

Targeted training. Yes, it's important to hold general training sessions and disseminate information and cybersecurity tips in a timely manner to the entire staff", but organizations should consider training on an individual level, too.

The goal: Identify the organization's most vulnerable employees and provide them with the specific training that they need.

"I would go out on a limb and say it's more important to target your most [targeted] individuals than the broad training," says Tahaney.

Various email security platforms run analytics against known malicious links and keep track of click rates on those links, Tahaney says. This feature enables organizations to see who is clicking which links, providing the company with an ongoing assessment. If the organization notices one employee is repeatedly making the same mistake, steps can be taken immediately to educate the employee.

In addition, organizations can utilize more robust security measures for certain employees.

"We've been unable to implement two-factor authentication for the entire organization, and I don't know many organizations that can do that, but what we have done is turn on two-factor for our very targeted individuals," says Tahaney.

Tahaney recommends that organizations partner with a vendor to track some of the information being collected by email security platforms.

"It's a lot to look at, especially when you're in IT and you're keeping the lights on," he says. "So definitely work with a third party, a vendor that you trust. If nothing else, it's another set of eyes on that data. It's a lot of data that gets generated."

Malware on the decline?

According to the Cofense report, malware attacks, particularly against healthcare organizations, are occurring at a low rate.

"While malicious attachments still play a role in phishing, the frequency of this has dramatically declined over the years. In fact, most phish attachments these days are not even malware, but instead, conduits to open a browser to further credential theft," Cofense co-founder and CTO Aaron Higbee wrote in the report.

Experts warn that the numbers should not fool organizations, however. Malware is still a very serious threat.

"Credential theft is bad—it's all bad—but ransomware really has the ability to cripple you completely, stop your business in its tracks," says Tahaney. "The other tactics are very quick wins and are easy to pull off."

Blass cites the recent ransomware attack against the University of Vermont (UVM) as proof. The attack deposited malware on more than 5,000 computers and laptops used by UVM Medical Center, according to the Burlington Free Press, and forced the hospital to operate offline. It took nearly a month for UVM Medical Center to restore electronic access to medical records.

"Even if malware is a lower percentage [than credential theft], the impact that happens with malware, you've got to say, 'If we get it, we're in big trouble,' " Blass says. "Stats are interesting to look at. They're interesting to analyze, but the reality comes into play, as well."

Organizations cannot afford to become complacent when training against malware threats.

Other report highlights

Cofense found several themes across phishing attacks throughout 2020. The report stated that organizations were frequently targeted by emails relating to the following topics:

- COVID-19 office infection data/contact tracing
- Federal financial relief packages for small or medium business loans
- Financial claims related to COVID-19
- Pandemic updates and guidance purporting to be from global, federal, or local health organizations
- Teleconferencing platform invites or required updates related to platforms like Zoom®, Teams®, and WebEx®
- Updates on remote working changes—company news and meeting invites

Healthcare organizations were—and still are—particularly susceptible due to the number of distractions created by the COVID-19 pandemic.

"They have incredibly important things on their mind," says Tahaney. "As IT, we have to remember that. A lot of times IT is the last thing, and you take it to cybersecurity, and that's even a layer under IT."

This is unlikely to change going forward. So the challenge for healthcare security professionals remains the same in 2021: Identify phishing trends, identify an organization's vulnerabilities, and implement a targeted plan to address the issues and spread awareness within the organization.

"In healthcare, you're trusting people and you're taking care of patients, so the mindset is a little different as opposed to a financial rganization," says Tahaney. "In a financial organization, security is in front of you every day. That's just not necessarily the case in healthcare. We have to work on doing that.