Although Email-Borne Attacks on the Healthcare Industry Are on the Rise, Help is at Hand

Healthcare providers depend on email to communicate internally, with patients and other facilities, but email systems and people are increasingly vulnerable to cyber threats. In Mimecast's *The State of Email Security 2020* report, 57% of healthcare organizations said they believed it inevitable or likely they would suffer negative impacts from an email-borne attack this year.

Cybersecurity problems have shifted and intensified during the COVID-19 pandemic. In April, the FBI issued an alert about COVID-related email phishing attempts against U.S. medical providers.[1] The international police organization INTERPOL reported a significant increase in ransomware attacks launched against hospitals and medical services providers during the crisis.[2]

In addition to email-based cybercrime on their own networks, healthcare organizations must contend with brand-damaging email and website spoofing attacks, in which a hacker creates phony emails and fake websites in the provider's name in order to steal user credentials or commit other types of fraud spoofing the healthcare organization's online brand.

Keeping healthcare organizations safe from email-related attacks today requires a two-pronged approach, said Matthew Gardiner, Principal Security Strategist at Mimecast. "There's no single silver bullet. You need a combination of technology and user training."

"There's no single silver bullet [to preventing email-related attacks]. You need a combination of technology and user training."

MATTHEW GARDINER

PRINCIPAL SECURITY STRATEGIST | MIMECAST

Here are some of the most effective technology and employee training tactics healthcare organizations can use to counter email-focused cybercriminals.

Use technology to prevent or mitigate cyberattacks

Launching an email attack is a multi-step process. “If you can disrupt any of the steps, you disrupt the attack,” Gardiner said.

Cybercriminals generally begin by sending phishing emails to lure healthcare employees into clicking a link or opening an attachment containing malware, such as ransomware. Malware, or malicious software, can slow computer performance, initiate remote monitoring, or encrypt or steal data. Ransomware is a specific type of malware that encrypts data and prevents an organization from accessing it unless it pays the attacker a ransom, which is increasingly in the hundreds of thousands or millions of dollars via bitcoin.

If a cybercriminal sends a phishing email containing a malicious link or attachment, today’s more sophisticated email security systems can often block malware from being downloaded or causing an exploit. But, “there’s no such thing as 100% prevention in any security realm,” Gardiner said.

Many people believe that once malware is installed or a credential is stolen that the organization will be immediately exploited. But, that’s not necessarily true.

“Attackers gain a foothold, but they don’t necessarily exploit the hacked system right away,” Gardiner said.

For example, ransomware criminals need more than an ill-advised click to execute an attack. Once their initial malware is installed on a computer, it generally will communicate with the attacker to get an encryption key for locking up the data at that specific organization. A web security system can eliminate or restrict the malware’s ability to interact with the cybercriminal’s infrastructure, thereby foiling the attack before it can progress. This clearly demonstrates the requirement to have layered as well as tightly integrated security systems.

Attacks often also take time to spread. If a user reports a suspicious problem – such as an odd email or system activity – the security team can isolate that computer from the network and scan it, uncovering the malware or other aspects of the attack and address it before the attack can spread.

Make sure an independent backup system is in place

Healthcare organizations need a strong data backup and recovery system for their applications and data so they can resume serving patients as quickly as possible if the network or system is compromised.

“A single click in an email should not bring an organization to its knees,” Gardiner noted.

One mistake some healthcare organizations make is allowing the backup system to be persistent on the network. “If a machine can persistently reach the backup system, so can malware, such as ransomware,” Gardiner said.

Instead, organizations should use an independent, cloud-based backup system that doesn’t connect to the company network or the attacker will encrypt your backup data as well. Fortunately, this is extremely easy to accomplish with the use of cloud-based email security and archiving gateways.

> ***Attacks often also take time to spread. If a user reports a suspicious problem – such as an odd email or system activity – the security team can isolate that computer from the network and scan it, uncovering the malware or other aspects of the attack and address it before the attack can spread.***

Prevent email and web spoofing with DMARC and continuous scanning services

Attackers no longer confine email and web spoofing attacks to big internet brands such as PayPal and Amazon. They are increasingly hitting regional or less well-known targets, including healthcare providers. In the Mimecast study, healthcare organizations reported detecting nine web or email spoofing attacks using lookalike domains on average in the past year, and 88% of respondents expected similar attacks to continue apace or accelerate.

Brand-damaging email spoofing can be prevented with a technology standard called Domain-based Message Authentication, Reporting & Conformance (DMARC), which prevents fraudsters from sending emails using the protected organization's email domains.

To prevent successful web spoofing, specialized security systems can continually scan the internet to find, block and take down brand spoofing, cloned websites – cloned websites are typically used in conjunction with phishing attacks.

Provide comprehensive and regular employee security training

An email-based attack can't succeed unless someone clicks on or interacts with an email that they shouldn't.

"Users often get all the blame, but if they're well-informed, they can be part of the solution," Gardiner said. "I call them your last line of defense."

Because email and other types of attacks evolve quickly, organizations should offer security training at least monthly, according to Gardiner. The Mimecast report found that only 15% of healthcare organizations do so currently. Training needs to be engaging, relevant and short to work. With some training platforms, providers can combine pre-loaded security awareness training with content specific to the company.

Traditional written content often fails to capture employee attention.

"Today, you need short videos with comedy snippets and scenarios that are like reality TV, built for the YouTube generation," he said. People are more likely to recall visual, scenario-based content when a suspicious incident occurs, according to Gardiner.

Reducing healthcare-targeted cyber-threats requires constant vigilance

To get ahead of threats, healthcare providers should conduct an email security risk assessment as a key element of their overall security and risk program and develop a budget for areas that need improvement.

"If organizations do that on a consistent basis over time, they can significantly reduce their risk," Gardiner said.

9	average number of web or email spoofing attacks each organization was aware of in the past year
88%	of respondents expected similar attacks to continue apace or accelerate
15%	of healthcare organizations offer security awareness training at least monthy

To learn more about achieving email security amid growing threats, read Mimecast's *The State of Email Security 2020* report.

References

1. American Hospital Association. 2020. FBI flash. April 21. https://www.aha.org/system/files/media/file/2020/04/fbi-alert-tlp-white-covid-19-email-phishing-against-us-healthcare-providers-4-21-2020.pdf.

2. INTERPOL. 2020. Cybercriminals targeting critical healthcare institutions with ransomware. April 4. https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

mimecast™

About Mimecast

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.