Data Breach Today
Prevention. Response. Notification.
https://www.databreachtoday.com/

Cloud Access Security Brokers (CASB) , Data Breach , Fraud

Phishing: Mitigating Risk, Minimizing Damage

In Wake of Recent Incidents, Experts Offer Insights on Critical Steps to Take

Marianne Kolbasuk McGee (HealthInfoSec) • May 20, 2019

As phishing attacks continue to menace healthcare and other business sectors, security experts say organizations must take critical steps to prevent falling victim and help limit the potential damage.

See Also: Webinar | The Future of Adaptive Authentication in Financial Services

"Phishing continues to be among the top causes of cybersecurity breaches, and defensive technology will always lag what the attackers are creating," says former healthcare CIO David Finn, executive vice president of security consulting firm CynergisTek. "We will certainly need the [security] technology, but the phishers or spammers are actually relying on the human frailties of trust."

A new research study by security vendor Proofpoint found that healthcare email fraud attack attempts increased by 473 percent over the past two years.

"Healthcare employees are especially vulnerable to email-based attacks due to the high volume of personal health information they access, their frequent email communication with patients and other providers, time constraints in critical care settings, sensitive intellectual property healthcare researchers handle and highly publicized ransoms being paid by healthcare organizations," Chris Dawson, threat intelligence lead at Proofpoint, tells ISMG.

Recent Incident

Oregon State Hospital was among the most recent healthcare targets of a spear-phishing scam on employees. Fortunately, unauthorized access to a hospital worker's email was discovered quickly and the attack hampered, a spokeswoman of the Oregon Health

Authority, which operates the facility, tells Information Security Media Group.

"The phishing email was received on May 3. However, the security breach occurred on May 6 when the bad actor accessed the staff person's email box," she says. "The unauthorized access began at approximately 9:50 a.m. and was shut down by 10:30 a.m.," she says.

The health authority is still assessing what information - and how much - was potentially exposed, and what kind of data, she says. "We are hiring an outside entity to determine exactly what information was in the email box and how many individuals were impacted."

The Oregon State Hospital, operated by the Oregon Health Authority, shut down a phishing attack breach within one hour of detection.

Technology staff members were able to detect the breach and shut down the unauthorized access very quickly, the spokeswoman says, because "we learn from each incident how to make our systems even more secure."

All Oregon Health Authority employees must take annual information security and privacy training, "which includes strategies for how to avoid phishing scams," she adds.

As of Monday, that incident was not yet posted on the Department of Health and Human Services' HIPAA Breach Reporting Tool website of major breaches impacting 500 or more individuals.

Detection Delay

But several other breaches involving phishing have been added to the tally in recent weeks, including some that took quite a while to detect.

For instance, Medical Oncology Hematology Consultants, based in Newark, Delaware, reported to HHS on April 26 a hacking incident involving email that affected nearly 8,600 individuals. A breach notification statement notes that the attack occurred in June of last year.

In a statement, MOHC says that since discovering the attack, it has taken a number of steps to bolster the security of its email systems. That includes implementing a new portal for delivery of secure emails from external sources, deploying malware

Medical Oncology Hematology Consultants recently reported a phishing-related breach that apparently occurred almost a year ago.

blocking measures, facilitating suspicious email reporting, establishing notifications to alert users that they may be attempting to send un-encrypted sensitive data, facilitating encryption of outgoing emails and providing additional data security training.

"Further, the practice will soon implement multifactor authentication and take additional steps to bolster its email phishing defenses," MOHC says.

As of Monday, the HHS breach reporting website, commonly called the "wall of shame," shows 94 breaches so far in 2019 involving hacking/IT incidents impacting a total of nearly 3.9 million individuals. Of those, more than half - 54 incidents impacting nearly 1.4 million individuals - were reported as involving email.

So far in 2019, 154 major health data breaches affecting a total of 4.3 million individuals have been added to the HHS website.

Taking Action

Proofpoint's Dawson offers tips on avoiding falling victim to spear-phishing attacks.

"First, deploying a multilayered approach to network defenses is essential, with a focus on securing your email channel and identifying and protecting your most attacked individuals," he says.

In addition to firewalls and other perimeter security, a dedicated advanced email security gateway must be in place, stopping threats before they ever reach employees - and providing mitigation solutions if they do, he says.

"Be sure to deploy email authentication protocols such as DMARC [Domain-based Message Authentication] and look-alike domain defenses as well to protect your organization from email fraudsters attempting to use your brand to lure victims."

In addition, a cloud access security broker solution can help provide visibility needed to safeguard an organization as it adopts Microsoft Office 365, Google G Suite, Box and other applications, he suggests.

Other Steps

Tom Walsh, president of consulting firm tw-Security, suggests priority action items to limit the impact of attacks include disconnecting the affected workstation or mobile device from the network and immediately unplugging any external hard drives or USB drives.

If the organization has cyber insurance, the insurer, once alerted, will likely bring in their legal team and forensic experts, Walsh notes. "Follow instructions from the insurance experts. Do not delete any files, include log files," he advises.

Walsh offers additional steps to help prevent phishing emails from reaching employees:

- Use a banner to notify users when an email sender is external to the organization;
- Train the workforce - "over and over again" and get tough on repeat offenders;
- Make employees aware of subject lines attackers commonly use as attention getters to entice email recepients to open a message;
- Block inbound and outbound traffic to foreign countries and implement blacklisting/whitelisting at the firewall;
- Block emails from domains with poor reputations.

Newer Technologies

Organizations should consider deploying advanced endpoint protection and a next-generation firewall, Walsh also suggests.

Finn adds: "This is one attack vector where I believe artificial intelligence holds a great deal of promise - coupled with your other defenses and with machine learning."

Machine learning can be used to delay - for deeper analysis - certain emails and block others that are clearly spam or phishing, he notes. "It is safe to assume that the bad guys are using AI to create and even time phishing campaigns. We should be able to get ahead of those and recognize multivector attacks - email, text, vmail. We can also build that information into our regular, ongoing training for phishing."