Cybersecurity Check-In: New Study Reveals Phishing Attempts Soared in 2018

With the new year well underway, it's a good time for healthcare providers to look back on 2018 to determine patterns of cybersecurity attacks and better cyber-strategize for the year ahead.

Proofpoint researchers recently released a new study that reveals that phishing attacks were dramatically on the rise last yea the hackers' overwhelming focus: credential compromise. This type of attack surged by more than 70% over 2017, beyond ev malware infections. Credential phishing attacks were noted by 65% of the infosec professionals participating in the study, whe only 38% of participants reported that kind of attack in 2017. Malware attacks remained steady at just under 50% for both 201 2018.

Credential compromise: a "dangerous trend"

The authors of the report noted that phishing emails of this sort represent a "dangerous trend given the serious ramifications o successful credential compromise attack… This is of particular concern given that multiple services often sit behind a single password."

The Proofpoint project surveyed 15,000 infosec professionals from across the globe and across industries, and it also studied millions of phishing emails sent between October and September of 2018. The researchers determined that 83% of survey participants had been the target of phishing schemes, as opposed to 73% for 2017.

"More respondents said they experienced attacks during 2018 than in 2017," the study's authors wrote. "Phishing and spear phishing saw the biggest increases, but all types of attacks happened more frequently than in 2017."

The healthcare industry didn't get the worst report card grades, but there's much room for improvement

Healthcare cybersecurity is of the utmost importance considering the level of sensitivity of patient data, but that doesn't mean professionals' best efforts can prevent all attacks. For instance, 2018 saw the New York Oncology Hematology breach, in whi staff members failed to recognize the phishing attack for what it was, and ultimately, the data of 128,000 individuals (patients employees) was compromised.

However, when compared with other industries, healthcare's cybersecurity prognosis was nowhere near the worst. The repor determined that healthcare's "average failure rate" was 8%. This compared to the entertainment industry, which suffered a fai rate exactly double that at 16%. When it came to the click-through rate for malicious links embedded in phishing emails that s the victim to a page to enter their personal data, however, the healthcare sector came in at 13%.

Those malicious links, used in nearly 70% of all attacks, are the most common type of phishing attempt, according to the Proofpoint researchers. Only 17% of phishing campaigns employed a direct data form for collecting victims' personal informat rather than a link sending them to another page, and 14% of phishing attempts use malicious email attachments to try to stea

Before you click that link . . .

Among the types of schemes that most commonly compelled victims to enter their personal information were emails that alert users to password changes, invoice payments, toll violations, and new building evacuation plans.

“Across the board, infosec professionals identified a more active social engineering landscape in 2018,” the report authors wrote. “The vast majority—96%—said the rate of phishing attacks either increased or stayed consistent throughout the year.”

Nearly all professionals surveyed are training users in anti-phishing security

The news isn’t all bleak, however; the study included a promising statistic: 95% of infosec professionals reported training end users on identifying and avoiding phishing campaigns. Further, the majority of the survey respondents said they already use threat monitoring platforms, URL rewriting, and spam filters in the ongoing effort to boost cybersecurity and be proactive.

“They are also shifting to a more people-centric model by proactively identifying phishing susceptibility, measuring end-user risk, and delivering regular security awareness training,” the Proofpoint researchers stated.