How susceptible are hospital employees to phishing attacks?

March 11 2019

Table 1. Email Category and Click Rates Among 95 Simulated Phishing Campaigns[a]

Email Category	Example Lures	No. (% Total) of Campaigns
Office related	You have received a new fax...	37 (38.9)
	You are expected to review this document on an annual basis...	
	Mandatory online workplace safety training...	
Personal	Someone sent you a Halloween e-card...	22 (23.2)
	Your new credit card has been shipped...	
	We are pleased to announce that you are eligible to receive double rewards...	
IT related	Your mailbox has exceeded the storage limit, which is 20 GB as set by your administrator...	36 (37.9)
	We are currently updating our database and email center. All unused accounts will be deleted...	
	If you are receiving this message, it means that your email address has been queued for deactivation...	

Abbreviation: IT, information technology.

[a] Emails were placed into 1 of 3 categories based on expert review. Shown are example lures from each of the categories, highlighting the type of content that is used to solicit further engagement with the phishing email from employees. Also shown are the number of campaigns from our sample that fell into each category.

A multicenter study finds high click rate for simulated phishing emails, potential benefit in phishing awareness training. Credit: Brigham and Women's Hospital/*JAMA Network Open*

Cybersecurity threats are a rising problem in society, especially for health care organizations. Successful attacks can jeopardize not only patient data but also patient care, leading to cancellations and disruptions in the critical services that hospitals provide. While many hospitals have taken steps to educate, inform and forewarn their employees about cybersecurity attacks, few studies have quantified how susceptible hospital employees are to phishing attacks. A new study led by investigators from Brigham and Women's Hospital addresses these

questions through a multicenter study that aggregated data from six health care institutions that ran phishing simulations over the course of seven years. The team reports a high click rate for simulated phishing but also a reduction in click rates with increasing campaigns, suggesting a potential benefit for raising awareness. The team's findings are published in *JAMA Network Open*.

"Information security is increasingly important for health care organizations, and cybersecurity attacks are a major risk to a hospital's ability to operate and deliver care," said corresponding author William Gordon, MD, MBI, of the Brigham's Division of General Internal Medicine and Primary Care. "But our study suggests that while the risk is high, there is an opportunity to mitigate it through training."

Phishing attacks via email can lure individuals into disclosing sensitive personal information or clicking on links that download malicious software. Many organizations have made a concerted effort to train their employees to recognize and report these attacks by sending simulated phishing emails, ranging from office- and IT-related to personal-related correspondence, and subsequently training those who inappropriately click or enter their credentials.

Brigham investigators aggregated data from six anonymized U.S. health care institutions representing a broad spectrum of care and geography. In total, they analyzed click rates for more than 2.9 million simulated emails. The team reports that 422,052 of these emails were clicked (14.2 percent)—roughly one in every seven. However, the odds of clicking on a phishing email decreased with increasing campaigns. After institutions had run 10 or more phishing simulation campaigns, the odds went down by more than one-third.

The authors note that many factors may go into why an individual clicks on an email and that their study, which did not drill down to the level of

individual employees, could not take all of these complexities into account. In addition, the study could not answer whether the improvements may be sustainable, and for how long, after a campaign ends.

"The rates that we report here are consistent with findings across other industries, where click rates can range from 13 to 49 percent, depending on the industry, but we know that in health care the stakes are high. Patient data, patient care, patient trust and financial stability may be on the line," said Gordon. "Understanding susceptibility, but also what steps can be taken to mitigate it, are critical as cyberattacks continue to rise."

More information: William J. Gordon et al, Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions, *JAMA Network Open* (2019). DOI: 10.1001/jamanetworkopen.2019.0393

Provided by Brigham and Women's Hospital