NOW +
NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

April 12, 2019

What’s trending on NP Privacy Partner

JAMA study exposes a big cybersecurity risk for health care organizations, the internal struggle between Facebook’s fact-checkers and the company itself and more. Here’s what’s trending in data privacy and cybersecurity.

Cybersecurity

JAMA study highlights the dangers of phishing attacks for health care organizations

On March 8, 2019, JAMA published a study analyzing the effects of simulated phishing emails at U.S. health care organizations. Concluding that the click rates for the simulated phishing emails present a big cybersecurity risk for health care organizations, the study provides helpful insight into how to prepare an organization’s workforce to detect harmful emails.

Phishing emails are deceptive communications intended to trick recipients into disclosing their security credentials or otherwise sharing sensitive information. Oftentimes, a sender’s identity is spoofed, tricking the recipient into thinking that the email originated from within their organization or that it was sent by a colleague or superior. Hospitals and other health care organizations are attractive targets of cyberattacks, as they have high-value personal and health data.

The study analyzed six health care organizations across the United States as they participated in simulated phishing emails between August 1, 2011 and April 10, 2018. The phishing emails fell into three categories: office-related, personal, and information technology-related. The emails were sent to employees in all types of roles. In total, approximately 2.9 million simulated phishing emails were sent, and recipients clicked on approximately 422,000 of them (approximately 14%). This means that the employees from the studied health care organizations clicked on an average of almost one in seven of the simulated phishing emails.

The study showed that the median click rates were higher for the information technology-related simulated phishing emails (18.6%) than the office-related emails (12.2%).

The study noted that repeated phishing simulations decreased the odds of an individual clicking on a simulated phishing email, which highlights the importance of the phishing simulation process and other forms of personnel training on these types of attacks.

This newsletter is intended as an information source for the clients and friends of Nixon Peabody LLP. The content should not be construed as legal advice, and readers should not act upon information in the publication without professional counsel. This material may be considered advertising under certain rules of professional conduct.

As hospitals and other health care organizations face financial and care-related consequences from cyberattacks, this study emphasizes the need for health care organizations to train their workforces on cybersecurity best practices, including through simulated phishing emails. As the study noted, it only takes one successful phishing incident to paralyze a system that is critical to the patient care provided by a health care organization. The study cited to several elements that may make a health care organization more vulnerable to a cyberattack, including a continuous stream of new employees, the use of a large number of information technology systems, and devices and systems that are highly interdependent. It also discussed other techniques that health care facilities can use to prevent or limit personnel from clicking on phishing emails, including using technology to try to filter suspicious emails and indicate on emails when they are sent by a person outside of the organization. *–Valerie Breslin Montague*

OIG audits of HHS Operating Divisions highlight need for better cybersecurity

In March 2019, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) released its summary report of penetration testing of certain HHS Operating Division networks. The purpose of the audits was to determine whether the Operating Divisions' existing security controls were effective to prevent cyberattacks, the level of sophistication that an attacker would need to compromise the Divisions' systems or data, and the Operating Divisions' ability to detect and respond to cyberattacks.

The OIG conducted penetration testing at eight HHS Operating Divisions in fiscal years 2016 and 2017. Following this testing, the OIG concluded that the existing security controls at the audited HHS Operating Divisions needed to be improved to better detect and protect against cyberattacks. The OIG informed HHS of a number of vulnerabilities, including issues with access control, data input controls, configuration management and software patching.

Following the audits, the OIG provided HHS with four recommendations to implement across its operations to address the identified vulnerabilities. The OIG summary report noted that HHS management agreed with the OIG's recommendations and that HHS and the eight Operating Divisions audited have or are working to implement the recommendations.

After the initial audit findings, the OIG summary report details how the OIG is working on new audits, reviewing for active threats on HHS networks, as well as past breaches by threat actors.

The OIG's audits of the HHS Operating Divisions serves as a reminder to health care entities to review their own cybersecurity processes and controls and to take steps to address and mitigate any identified issues. *–Valerie Breslin Montague*

Social Media

Facebook fact wars: The internal struggle between Facebook's fact-checkers and the company itself

In the days following the 2016 United States presidential election, many were left wondering how the country had become so divided. Never before had the voters on either side of the aisle come to the polls with not only different opinions, but different facts upon which those opinions where based. This realization led to the ongoing period of reflection that still envelopes the country. News sources have not been impervious to such reflection, and have begun to look into the vetting process they currently employ with respect to the "news" they publish. Aside from obvious ethical and professional standards, the 2016 presidential election provided perhaps the most jarring example of the effect of inadequately vetted, partisan news.

One such news source that has received scrutiny is Facebook, Inc. The social media giant had to reconcile the fact that it had become a primary source of news for millions of individuals, a role for which it was decidedly ill-equipped. As a potential solution, Facebook launched a "global fact-checking initiative" in December 2016. This initiative involves, in part, employing groups of fact-checkers to review news published on the site. When an article has been deemed to be uncorroborated or misleading, the fact-checkers are tasked with publishing an explanatory article, notifying the user that posted the misleading article and ensuring the misleading article is then shown less prominently on the site.

Facebook currently has 43 fact-checking organizations across the world, covering news in 24 different languages. However, the fact-checkers themselves are uncertain as to whether they are having a material impact. Facebook requires fact-checkers to sign non-disclosure agreements, but this has not stopped many from anonymously speaking up about Facebook's lackluster procedure with respect to the fact-checking process. Editors have reported feeling underutilized, and admitted that fact-checking, despite outward appearances, is not a priority for the Facebook brass. In fact, editors have noted that certain fact-checking groups cease operations when nearing the payment cap, which is a cap on the number of fact-checks for which Facebook has agreed to pay in a given month. This cap on explanatory articles results in a backlog from month-to-month, and the current cap is not nearly enough to provide a thorough fact-check of many of the articles posted to Facebook each month. Indeed, one fact-checker noted that its firm had nearly 500 articles in queue to be checked at the end of a certain month.

The current initiative will have to undergo an overhaul, especially when the number of articles to be reviewed are combined with articles posted to Facebook's other networks, such as WhatsApp and Instagram. Facebook is acutely aware of the shortcomings of the current process, but as Mark Zuckerberg and other executives begin to explore alternatives, it appears a solution to this Herculean task remains far off. –*Wesley Gangi*

For more information, please contact:

— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485

— Wesley Gangi at **wgangi@nixonpeabody.com** or 312-977-4478

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team