Health-ISAC Weekly Blog -- Hacking Healthcare®

Hacking Healthcare | TLP:WHITE | Alert ID : 4e755950 | Sep 10, 2024, 04:13 PM

This week, Hacking Healthcare® is going phishing. Phishing remains a significant risk for the healthcare sector, and raising awareness and educating your workforce about how to spot and avoid phishing attacks are good practices to adopt.[1] This iteration of Hacking Healthcare® focuses on internal phishing testing and analyzes a few examples that may have accidently done more harm than good.

Welcome back to Hacking Healthcare®.

Phishing Training Gone Awry

It is well documented that phishing is a significant cybersecurity risk to organizations. A few years ago, numerous articles were citing the statistic that 91% of all cyberattacks began with a phishing email.[2] [3] Other organizations have pegged phishing as "a leading cause of healthcare data breaches."[4] It is only natural that organizations have taken steps to mitigate this risk by tightening technical controls and, perhaps most critically, emphasizing employee awareness training and conducting phishing tests.

When done correctly, these tests can be a valuable way to raise employee awareness. However, there are numerous examples of how well-intentioned implementations have gone awry. We hope the following examples will inform how Health-ISAC members approach phishing training and tests to avoid unintended results.

Employee Benefit Bait-and-Switch

In September 2020, deep into the COVID-19 pandemic, the major U.S. news publisher Tribune Publishing Co. sent an email to employees announcing that successful cost-cutting measures were going to allow them to payout bonuses between $5,000 and $10,000.[5] With employees working through the uncertainty

of the pandemic, and in a sector already struggling to maintain adequate pay to retain personnel, it shouldn't be a surprise that at least some employees clicked on links within the email. Those who did were informed that there was no bonus and they had failed a simulated phishing test.

As you might imagine, there was significant public backlash on social media from employees who were incensed that they would dangle such a potentially impactful sum of money to "overworked and underpaid" staff who were already deeply concerned with their financial stability.[6] The security company that partnered with Tribune Publishing Co. described the incident as a "custom" exercise that backfired.[7]

This kind of bait-and-switch is more common than you might think. Another example involved the West Midlands Railway organization located in the UK. In 2021, it sent a phishing test email thanking the frontline workers who had maintained the rail system during COVID-19 and offered a one-time bonus for their hard work.[8] Once it was understood to be a test, the incident quickly resulted in public backlash from workers and the transportation union.

Health Scare Tactics

Another phishing test topic that has come under scrutiny is that of a fake health scare.[9] In one incident, an organization sent an email out to its personnel informing them that a staff member had contracted a serious contagious illness and that contact tracing and containment measures were being introduced. A link within the email promised to provide updated information on what was sure to be an evolving situation.

As might be expected from such a serious healthcare warning, numerous individuals clicked the embedded link and were directed to a webpage belonging to a well-known cybersecurity company informing them that this was a test.

Needless to say, while it was very likely meant with the best of educational intentions, this approach did not go over well with many of those associated with the organization. Individuals bemoaned using something as potentially life-threatening as a serious contagious disease scare for phishing awareness purposes. Others noted that the backstory provided by the email on the origin of the contagion could be perceived as needlessly reinforcing negative stereotypes.

Action & Analysis

Included with Health-ISAC Membership

[1] https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing

[2] https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec#footnote2

[3] https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

[4] https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/

[5] https://www.bankinfosecurity.com/blogs/how-phishing-readiness-test-goes-very-wrong-p-2948

[6] https://www.bankinfosecurity.com/blogs/how-phishing-readiness-test-goes-very-wrong-p-2948

[7] https://www.bankinfosecurity.com/blogs/how-phishing-readiness-test-goes-very-wrong-p-2948

[8] https://www.theguardian.com/uk-news/2021/may/10/train-firms-worker-bonus-email-is-actually-cyber-security-test

[9] Due to the sensitivity of this topic, the entities involved and the details of the incident are being kept intentionally high-level.

Report Source(s)

Health-ISAC

Release Date

Sep 10, 2024, 11:59 PM

Reference | References

Microsoft Blog
deloitte
HIPAA Journal
The Guardian
Bank Info Security
CISA

Tags

Hacking Healthcare, Training, Education, Awareness, Phishing, cybersecurity

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org