HTA POST

Volume 3
Issue 11
November 2019

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Phishing Attack Simulation

There is a new phishing-related data breach reported in the healthcare industry every week. It has become one of the most reliable ways for hackers to gain access to systems and data. There's only one way to combat phishing emails – employee training. What's better than slideshows, lectures, or dense articles? Actual hands-on experience! HTA offers live phishing simulations, where your employees will be tested with realistic phishing emails, and the results will be reported to you after the exercise. That way you can appropriately target, train, and improve!

IN THIS ISSUE

REFERRAL

Join the HTA Advisory Committee!

Have a coffee on us, and get a chance at a FREE iPad.

With our new referral rewards program, every qualified referral enters you into a drawing for a new iPad. Don't miss your chance to win this quarter!

UPCOMING EVENTS

Thursday, November 7th	10am-1pm Missouri Hospital Association 97th Annual Convention and Trade Show *Greater Heartland HFMA, Osage Beach, MO*
Wednesday, November 20th	3:30pm-7pm St. Louis Leadership Series *Greater Heartland HFMA, St. Louis, MO*
Wednesday , November 20th	3pm-5:30pm ID Theft and Your Business *Greater Kansas City MGMA Overland Park, KS*
Wednesday , November 20th	11:30am-1pm Online Reputation Management *Greater St. Louis MGMA St. Louis, MO*

See more at:
htadvisorsllc.com/events

Healthcare Technology Advisors

This monthly publication provided courtesy of Derrick Weisbrod & Hugh Anderson, Founding Advisors of Healthcare Technology Advisors.

Our mission is to be trusted advisors guiding healthcare businesses through the complex IT and HIPAA landscape while providing a comprehensive service that always maintains a human touch.

20,000 E-COMMERCE SITES COULD BE COMPROMISED BY MAGECART

Providing an online shopping experience is increasingly critical for SMBs looking to stay ahead of the competition. Unfortunately, malware attacks are infecting the checkout page of many stores, compromising customer payment data and undermining companies' efforts to attract business through their websites.

This reality became even more prescient this week when the notorious Magecart malware infected Volusion, a cloud hosting platform for online stores. Already, more than 6,500 stores have been compromised, and Volusion boasts a customer base of more than 20,000 companies, so the number of infected web stores might continue to grow.

Most prominently, Volusion hosts the Sesame Street Live online store, which was brought offline after the attack was revealed.

Now thousands of companies will be left grappling with the consequences of lost sales both now and in the future. Notably, this underscores the importance of understanding the specific cyberthreat landscape that most prominently impacts your business. If necessary, get third-party support from cybersecurity experts to adequately identify your risks and to establish best practice responses that ensure that your business benefits because of your IT environment.

BEST PRACTICE OF THE MONTH: LOG MANAGEMENT

Log management is the practice of recording and reviewing the logs of servers, workstations, firewalls, and other network equipment. This is a vital component of HIPAA compliance because the logs are the record of everything that happens on these devices. In the event of a security breach, the logs on a server may contain the answer as to how the serer was accessed, who the bad actor was, and what damage was done.

The problem with log management is that most devices eventually overwrite their own logs. If a breach is not discovered until months after the initiating event, the logs may be long gone and impossible to recover. That makes it difficult to determine the scope or exact timing of an incident. In addition, not having those logs is a HIPAA violation. Therefore, the logs must be archived to enable proper investigation.

For any healthcare practice that uses network connect devices, proper log management should include periodic manual or automated reviews to check the logs for security incidents. If this is handled properly, it can alert your IT staff to a problem before other evidence surfaces via workstation problems. Considering that many security breaches are not discovered until long after they have occurred, proper log review is vital for best-in-class cyber security. Archiving the logs so that they can referenced is the second part of the best practice, as these logs are the best evidence for analysis in case of a security breach.

LYDIA'S HOUSE FAMILY PROJECT

This holiday Lydia's House charity is hosting a donation drive for 50 families. These families are in need of assistance with creating a warm and loving holiday, and Lydia's House is collecting gifts and meal basket donations.

Lydia's House is a non-profit organization that works through faith to help women and their families find strength and stability after escaping domestic violence. They do this by providing long-term transitional housing, advocacy, education, job training, community, and assistance with childcare. After a maximum of two years in confidentially located, fully furnished apartments, the women who move through Lydia's House's program are empowered to take the reins in their life with independent banking, housing, and employment.

This holiday, Lydia's House has 50 diverse families that organizations can 'adopt' to collect donations for. These families range from single women, mothers with just one child, to mothers with two or more children. Each family has provided a wish list with clothing sizes and meal basket suggestions. Donation will be collected on December 13th.

If your organization would like to adopt one of the families of Lydia's House, please contact Lydia's House at (314)771-4411 ext. 107 or by email at holidayproject@lydiashouse.org.

Join us this holiday season in bringing joy and comfort to those who need it most.

HIPAA FINE SPOTLIGHT - $10,000

Does your practice have reviews posted on Yelp, Google, or Facebook? Most do these days. Those reviews are vital for attracting new customers, as many people check online reviews before committing to a new product, restaurant, or service. Of course, misunderstandings can lead to undeserved poor reviews, but keeping a professional demeanor when responding is the best way to turn that perception around.

Unfortunately, with medical practices, there is an added layer that must be considered when responding to reviews – PHI, and how to protect it. It may be tempting to address a patient's concern directly, but if the patient's protected health information is mentioned in that response it is a violation of the HIPAA Privacy Rules.

This was highlighted in a recent OCR settlement. Elite Dental Associates of Dallas, TX, (Elite) agreed to pay $10,000 to settle its potential violation. The complaint, received on June 5, 2016, alleged that Elite disclosed a patient's last name and health condition details while responding to an online review. The subsequent investigation revealed that Elite had disclosed the PHI of several patients while responding to reviews on the practice's Yelp review page. Elite also had no policy in place regarding disclosure of PHI as it related to social media.

Elite is a privately-owned dental practice that provides general, implant, and cosmetic dentistry. Their settlement agreement included adopting a corrective action plan. While the settlement amount may seem smaller than most, it should be noted that "OCR accepted a substantially reduced settlement amount in consideration of Elite's size, financial circumstances, and cooperation with OCR's investigation."

"Social media is not the place for providers to discuss a patient's care," said OCR Director, Roger Severino. "Doctors and dentists must think carefully about patient privacy before responding to online reviews."