HTA POST

Volume 5
Issue 8
August 2021

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Last month Derrick and the team helped pull off a third stellar Pickin' on Picknic Music Festival! Held yearly in July at Lost Hill Lake – a beautiful, secluded outdoor venue in St. Clair, Missouri – this festival has been sponsored by Healthcare Technology Advisors for three years now.

UPCOMING EVENTS

Wednesday 11th 12-1pm
MGMA Live Webinar Event

In October: Wednesday 13th Annual MGMA Fall Conference

See more at: *htadvisorsllc.com/events*

IN THIS ISSUE

Healthcare Technology Advisors

REFERRAL

Want to get up to $2,000 OFF your annual IT investment?

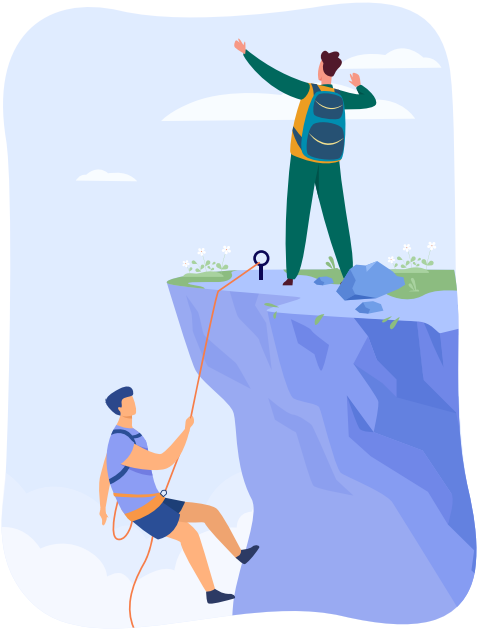
WIN a FREE iPad and EARN credits with HTA's Referral Rewards Program!

Learn more at:
htadvisorsllc.com/about-us/referral-program

This monthly publication is provided courtesy of Derrick Weisbrod, CEO, and the Healthcare Technology Advisors Team.

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.

UPPING OUR GAME



As your Managed Service Provider, you trust us to deliver the best IT service possible. That means we are constantly educating our team on the options for software, hardware, and cyber security that are available. Because the field transforms and evolves so fast, these options rise and fall in favor on a regular basis.

Keeping up with all that information is a daunting task, which is precisely why we take on that burden for our clients and why we focus on delivering comprehensive services that work with the environment your practice exists in. We may add a new service and replace an old one, because the previous solution is no longer considered best in class or does not offer the same value that a new solution does.

Many of the tools we use are also upgrading and adding more protections or streamlining their service at no additional cost.

We are always educating our team on the new solutions that exist, watching established companies mature and keeping an eye on new start-ups to see where they may be headed. In the world of technology, today's king could be forgotten in a fortnight. You can trust us to exhaustively research new solutions before adopting them. When we choose a new service, it is because it offers the best protections and value available.

TECH TIP: THE PASSWORD THAT WAS

How many new online accounts have you created over the past year?

With new work-from-home applications, video calling software, and phone apps, there has been a deluge of new accounts created. That brings a great reuse of passwords.

We are all guilty of using the same password for multiple applications. It is difficult to remember a dozen different passwords, or worse yet, minute variations of passwords. Yet this behavior poses a serious risk.

If you created a new Zoom account this past year, for instance, and you used the same password as your work email, what happens if Zoom's database gets hacked?

A cyber criminal could then use your compromised credentials to log on to your work email and steal information, distribute malicious software, or send phishing emails to your work colleagues.

How do we navigate the great password menagerie? Consider implementing a password manager. There are many free or paid applications that can help with this for personal use. For a healthcare practice, consider a program like MyGlue that can securely store all the passwords needed in your organization. These applications have the added benefit of automatically creating new, hard-to-guess passwords for you, so you don't have to come up with a new 12-digit string of nonsense every time you need to use a new program.

NEVER reuse a password that logs in to sensitive or protected data. Contact your security officer to make sure your password policy is strong and compliant.

DON'T FALL FOR BRAND IMPERSONATORS

One of the fastest, easiest ways for cybercriminals to trick your employees into falling for their lures is to convince those employees into thinking that they're someone else. Email is the primary form of B2B (Business to Business) communication, opening new vistas of opportunity for bad actors to explore. That trend is set to continue as email dependence continues to rise.

One trick that cybercriminals are using these days was recently outlined by Microsoft in a blog post.

Cybercriminals who are working their fraud through domain spoofing will use homoglyphs, or imposter domains that are so close to a company's legitimate domain as to make their messages appear authentic. Think replacing "O" with "0", or something similar, to make the domain that they're pointing folks toward seem like the real thing – but it's a trap.

Almost every major brand has been impacted by brand impersonation. So far in 2021, an estimated 45% of all brand impersonation phishing attempts were related to Microsoft. Because businesses get many emails regularly from Microsoft's brands, they are a good choice for cybercriminals. However, it's a bad choice for businesses since those messages are likely to be highly believable to employees.

A great way to reduce your company's chance of falling victim to a brand impersonation attack is to make sure that you're keeping security awareness training up to date with a solution that teaches employees to spot and stop new threats, like BullPhish ID. After all, security-savvy employees are your organization's best defense against cybercrime.

DID LINKEDIN LEAK YOUR DATA, AGAIN?

In April 2021 hackers exploited a vulnerability in LinkedIn that allowed them to scrape 500 million user accounts. Three months later, the same exploit was used to expose 700 million accounts. That is more than 92% of LinkedIn's estimated total users. The breach represents a massive load of exposed data.

This hack is both wide and deep. It isn't just basic user data that is exposed. It's a veritable gold mine of personally identifiable information. What causes more concern is that this information is almost uniformly business class. LinkedIn users should be aware that the data exposed in this incident includes the following:

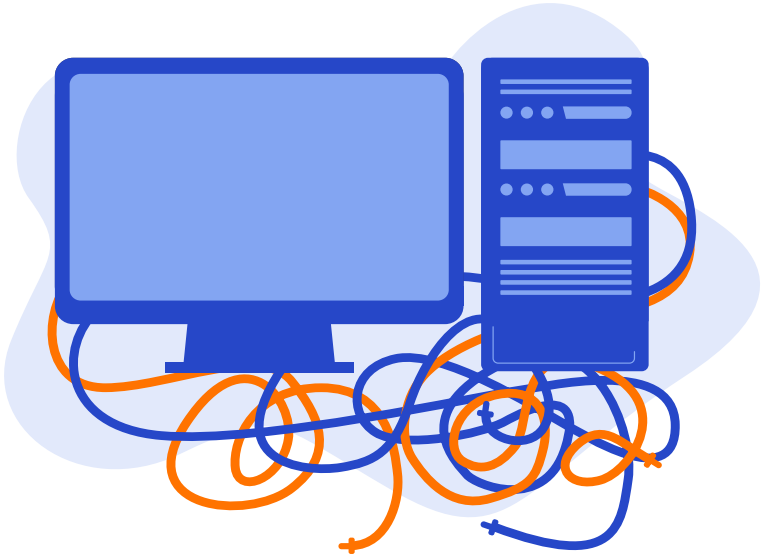
Email Addresses, Full names, Phone numbers, Physical addresses, Inferred salaries, Geolocation records, LinkedIn username and profile URL, Personal and professional experience/background, Genders, Other social media accounts and usernames.

This means that your organization could be at greater risk of a spear-phishing attack, where a cyber criminal impersonates a trusted contact to garner login credentials, banking information, or fiscal transfers.

So how do you protect yourself?

Establish Standard Operating Procedures for money transfers. Always navigate independently to login pages, rather than following a link. And consider contacting your IT department to learn about targeted training to protect your staff from cyber attacks.

CAN YOU PROTECT YOUR SYSTEM FROM RANSOMWARE?



Just before July fourth weekend, a prolific data company was hit by a massive ransomware attack. This attack exploited the data company to target its customers. It is a Managed Service Provider's worst nightmare. Their systems were being used to harm their customers.

Kaseya provides many services to MSPs and by extension to thousands of businesses throughout the world. This attack targeted their Remote Management software. It hit both a small town in Maryland and a grocery store chain in Sweden. The affected companies numbered between 800 and 1,500. The result? These companies were met with a ransom notice, unable to access their data and prompted to pay a ransom ranging between $45,000 and $5 million.

By the end of July, Kaseya had obtained a universal key to decrypt their files and were working with their affected customers to restore access to data. Over the weeks where their systems were compromised, they advised all customers to shut down specific functions to stop the malicious software from affecting more systems.

This latest attack only highlights the true vulnerability of our technology infrastructure. One of the most elite companies in the tech space had their own software compromised and used to lock down and ransom businesses' data. It is truly a matter of when, not if, the cyber attacks will reach your organization. The question is, how well will you respond?

There are many resources to help you prepare.

On June 2nd, the White House released the memo "What We Urge You To Do To Protect Against The Threat of Ransomware."

Within it, they outlined 5 steps to take NOW to prepare and protect your organization against ransomware.

These steps include backing up your data and testing your recovery capabilities, updating and patching systems promptly, testing your incident response plan, using 3rd party testers to review and check your system, and segmenting your networks.

Perhaps the most effective protection against ransomware is offline backups. Ransomware encrypts data and makes it impossible to access your systems. However, if you have a complete backup that is stored offline (and thus unreachable by the malicious software attacking your active systems) you can completely restore your operations from your latest backup and resume normal functions with only the loss of a few hours or days.

Ransomware attacks have disrupted organizations around the world, from hospitals across Ireland, Germany, and France, to pipelines in the United States and banks in the U.K. The threats are serious and they are increasing.