Dental Managers Society Newsletter
We Welcome Medical Managers!
July 2024

Securing Your Practice

As your technology evolves, so do your practice's risks. Hackers have become more sophisticated and utilize the Dark Web to purchase ransomware schemes, access to server credentials, credit card accounts, and many other nefarious activities.

Here are some of the most important things you need to know:

1. **You Aren't Too Small to Attract Hackers**

Small Businesses Are Especially Vulnerable

Given that small businesses have fewer resources to dedicate to cybersecurity, it is unsurprising that they are more vulnerable to cyber-attacks. In fact, 43% of all cyber attacks are directed at small businesses. If you run a small business, it is critical to take data protection seriously and invest in robust cyber-security measures that can keep your organization safe.

2. Enclosed you will find our Phishing Postcard to put near your computer as a reminder. If you'd like complimentary copies for every computer in your office, go to ACTSmartIT.com/phishing. The first step in protecting your business is to identify the assets that are most important to your company. This includes financial data, customer information, or intellectual property. Your assets also include the hardware upon which your company runs. If the hardware is made inoperable from a cyberattack, the inability to transact business can be equally devastating.

2. Phishing Attacks Are a Major Threat

Cybercriminals have an endless arsenal of methods to infiltrate a company's systems. However, one of their favorite tactics is phishing. This involves sending an email that appears to be from a legitimate source but is meant to trick people into revealing sensitive information such as passwords or bank account details.

In fact, as many as 90% of data breaches occur as a result of phishing attacks. If your organization wants to stay protected, it's crucial to be vigilant about phishing attempts and take steps to minimize the risk of falling victim.

If you'd like complimentary copies for every computer in your office, go to:

ACTSmartIT.com/phishing

3. You and your employees could be easily scammed! Today, AI makes it even easier for a scammer to trick you into sending money, making changes to financial records, disclosing sensitive information or allowing access to critical data.

- **Scammers pretend to be someone you trust.** They impersonate a company or government agency you recognize to get you to pay. But it's a scam. Artificial intelligence can even impersonate a voice. If the request is unusual, hang up and call the person back using a number that you know, not the number on caller ID.
- **Scammers create a sense of urgency, intimidation, and fear.** They want you to act before you have a chance to check out their claims. Don't let anyone rush you to pay or to give sensitive business information.
- **Make sure procedures are clear for approving purchases and invoices and ask your staff to check all invoices closely.** Pay attention to how someone asks you to pay and tell your staff to do the same. If someone demands that you pay with a wire transfer, cryptocurrency, or gift cards, don't pay. It's a scam. Since scammers often fake their phone numbers, don't trust caller ID. If you get an unexpected text message or email, don't click any links, open attachments, or download files. That's how scammers load malware onto your network or try to convince you to send money or share sensitive information.
- **Scammers sometimes even hack into the social media accounts of people you know,** sending messages that seem real — but aren't. Be wary of what you and your team post on social media. Too much information can give scammers credible facts that can make them more believable.

(Continued on page 3)

Letter from the Editor

Pam Snell,
DMS Advocate

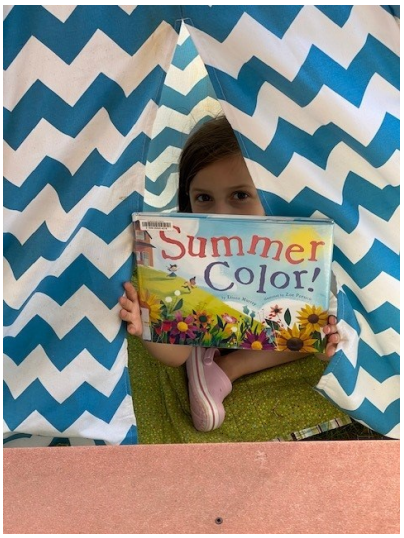
July! WOW! We have vacation weather!

After several years of rainy, cool summer weekends, we are finally enjoying summer, even if it's hot weather! David's gardens are thriving and the hydrangeas that I complained about last year are glorious!

The grandkids got out of school, but with summer reading, which they loved! They received Olympic BINGO cards where they can earn medals for completing one line, three lines, or the whole board. You know what they are going for!

Squares didn't include only book subjects; they also "Read a book in a tent," and "Read a book with 'Summer' in the title."

The kids got 3 squares completed in one reading outside (another square) by reading in a teepee that my brother, Eric, gave them years ago.



If your summer includes traveling, we want to remind you: ***Hackers do not take a vacation,*** and they are excited that you may let your guard down as you unwind and forget about the challenges back home.

Last year, we put out a Safe Travel Guide. You can review it here: **https://actsmartit.com/travelsafe/**

You'll also be interested in reading the AI Scams to be aware of on pages four and five.

Enjoy these summery days!

(Continued from front page...)

- **Cyber scammers can trick employees** into sending them money or giving up confidential or sensitive information like passwords or bank information. It often starts with a phishing email, social media contact, or a call that seems to come from a trusted source — for example, a supervisor or other senior employee — that creates urgency or fear. Other emails may look like routine password-update requests or other automated messages, but are actually attempts to steal your information. Scammers also use malware to lock organizations' files and hold them for ransom.

4. Treat your email like the valuable asset that it is to your business.

Your email password must be strong and DIFFERENT from every other password that you use. If a hacker gets into any of your secured sites, the first thing they will try to do is change the password so you can't get back in. How do they do that? They request a password reset — sent to your email address. If they can get into your email, they have the keys to your kingdom and can access every account that you have.

5. Secure your mobile devices, too.

70% of internet fraud is achieved via mobile devices. The majority of all internet traffic comes from mobile devices. Hackers recognize this, and they're able to commit cybercrimes with them as well. Keep apps to a minimum to keep the threat of malicious apps low. If possible, only use company-owned smart phones to maintain control and security.

6. Cybersecurity Awareness Training for Everyone!

Human error is the biggest threat to cybersecurity Cybersecurity training makes your business more secure. Cybersecurity training may be required for your industry's compliance regulations Training that is interesting, interactive, and fun will be more effective The owner and/or management must be invested as well. Don't use training as a punishment or it will always be resented.

7. When an employee leaves…

Many businesses don't think past getting back the keys when an employee leaves, whether by choice or not. It is important to make sure that they are disconnected from all access to company files and data. Remove access to email; forward it to another employee for 1-6 months so nothing is missed.

Change all passwords, especially if they shared them with others. Remove references to them from all company documents, including your website and voice mail Contact your IT provider to be sure they know not to allow access.

AI Travel Scams to Watch

Travel scams driven by AI processes are on the rise. To keep yourself safe, verify website legitimacy, check for SSL, grammar, and social media presence. Also, be wary of AI-generated images and reviews. It's best to stick to legit travel sites when making bookings.

From fake websites to AI-generated reviews, cybercriminals are leaving no stone unturned in their efforts to deceive unsuspecting travelers. With that in mind, here are a few AI-powered travel scams to watch out for when researching or making bookings for your summer holiday. Don't let thieves ruin your plans!

AI-Generated Travel Websites

A 2024 McAfee report noted that one of the most common types of scams facing travelers involves unauthorized transactions due to banking or credit card details entered on a fake website. With AI tools like ChatGPT, creating a fake website has become easier than ever. To take things one step further, cybercriminals are even using AI deep fakes as travel agents to help persuade potential travelers to complete a booking. If you're considering booking your stay or flight tickets through a new website, make sure to verify its legitimacy before you enter any sensitive data into it. Look for misspellings in the web address as well as the SSL certificate. A legit website's URL should start with "HTTPS" (the "s" stands for secure). If it, instead, begins with "HTTP," the website may just be run by a bad actor. Note that some websites still use HTTP, but any website worth its salt that sells expensive tickets, holidays, and so on will use HTTPS as it is more secure.

It's also a good idea to review the content on a website. Poor grammar or spelling is a telltale sign that the website isn't run by a real company. You can also verify the company's identity, presence, and reviews through social media. For instance, you'll want to check to see how many followers the company has, if it posts regularly, and what the engagement is like on its posts. A number of negative reviews and comments on a company's social media pages are a definite red flag.

AI Imagery

Another trick scammers are using to entice unsuspecting travelers is using AI-generated images on their websites or social media posts. These images can depict vacation spots, accommodations, and tour experiences that seem appealing to most but don't actually exist.

For instance, when searching for accommodation options, you might come across a rental property that seems too good to be true based on its images and the price it's listed at. Not wanting to pass up on this deal, you go ahead and book the property for the duration of your stay. When you reach the destination, you might find that the property doesn't exist or that it's pretty rundown. To keep this from happening to you, be sure to familiarize yourself with a few ways to identify

Out for This Summer

AI-generated images. Also, it's best to avoid falling for deals that seem too good to be true. I always check the prices of similar properties I n the area. If the price of the property I'm considering booking is not in line with that of other properties in the area, I consider it a red flag and continue my search.

Fake AI-Generated Reviews

Before you book a tour or accommodation, it's best to check the reviews left by previous customers to get a sense of what you're signing up for. The problem with this, however, is that scammers know you're going to do this, so they try to get ahead by leaving fake 5-star ratings and positive reviews for fraudulent listings. These fake reviews are usually generated by AI, and given how good AI has gotten, it can get pretty hard to spot inaccuracies or fake text.

For example, here is an AI-generated review for the fake infinity pool hotel in the previous section:

The good news is that there are ways to detect AI-generated reviews. Although I don't use AI text detectors in everyday life, it's something I recommend if you're making a booking worth hundreds or thousands of dollars.

- **Title:** Paradise Found!
- **Rating:** ☆☆☆☆☆ (5/5)
- **Review:** I recently had the pleasure of staying at this breathtaking resort, and I must say it exceeded all my expectations. From the moment I arrived, I was captivated by the serene and luxurious atmosphere. The infinity pool, surrounded by lush palm trees, creates an almost surreal connection with the ocean, making you feel like you're swimming straight into the horizon. The poolside area is meticulously maintained with lush green grass and comfortable seating. It's the perfect spot to relax and unwind with a book or enjoy a refreshing cocktail from the nearby bar. The staff were incredibly attentive and made sure I had everything I needed to enjoy my stay. One of my favorite moments was watching the sunset while lounging by the pool. The sky turned into a beautiful canvas of colors, reflecting off the water, creating a truly magical experience. Overall, this resort offers a perfect blend of luxury, tranquility, and natural beauty. It's a paradise for anyone looking to escape the hustle and bustle of everyday life. I can't wait to return!

These images were created with AI.

No matter the kind of deal you spot, it's best to stick to legit and well-known flight and hotel booking platforms. Although the allure of rock-bottom prices can be tempting, using these websites reduces your chances of falling for a scam. You can even use AI and ChatGPT apps to create instant itineraries that are in line with your travel plans and preferences.

Thanks to
https://www.makeuseof.com/ai-travel-scams-to-watch-out-for-this-summer/
for this information.

In our last edition, we reviewed a few different scams and some tips on ways you can protect yourself and what to do if you think you were the victim of a scam.

If you missed our first alert, just stop by our East Wareham branch, and we'll give you a copy

It is more important than ever to make sure that you are aware of the many scams fraudsters are trying to get away with. This month, we are going to review a different type of scam and what you can do to protect yourself if you believe you are being scammed, or have been a scam victim.

One of the more common scams that we are seeing almost once per week is the "Advertisement for Sale" scam. This scam is very common on nearly any website someone can advertise something for sale.

Some very common websites we see this from are Facebook, Craigslist, and Offer-up; sometimes we even see these on websites for rental properties.

The way this scam works is you may be browsing Facebook Marketplace for a specific item, let's say a new boat. You find someone selling a boat but the deal just looks a little bit TOO good to be true. The scammers know that an attractive price will bring in more possible people to scam.

The most important thing to be careful of is if anyone selling a product wants you to send money via Venmo, Zelle, or Cashapp. These apps send your hard-earned money electronically, and the funds leave your account instantaneously.

Part of the agreement to use these applications indicates that you are solely responsible for any transactions that are sent and there is ZERO recourse if you hit that send button. Once you send the funds to the scammer, they will no longer answer you, they will block your number, or even worse completely disconnect the original number you were communicating with. They use a fake name, and fake profile to stay under the radar. You are out your money and you definitely aren't going to get the boat.

How can you protect yourself from this scam? To start, if you are buying an item from a third-party online, it's very important to make sure this is a legitimate person. It sounds silly, but look at their Facebook to see if they have a lot of friends. If they are selling the item locally, do they have any friends locally?

These are big red flags, as scammers will typically create a new account to do a new scam. Another great tip is to NOT send any money until you can see the item you are buying. Make sure you can verify that the item physically exists.

My final tip, which is the most important… Never ever send a Zelle, Venmo, or Cashapp to someone you do not 100% know and trust. These apps can be very helpful, but only with people you know; they are easy methods for fraudsters to get funds!

Vincent A Pircio, Branch Manager II,

Rockland Trust

2995 Cranberry Highway, East Wareham, MA 02538

Phone (508) 295-6900 | Fax (508) 295-7178

Vincent.Pircio@RocklandTrust.com

* IMPORTANT DEPARTMENT OF LABOR AND EEOC UPDATES *

Changes regarding non-exempt and exempt minimum salary threshold

BEGINNING July 1, 2024, the US Department of Labor's (DOL) final rule to the Fair Labor Standards Act (FLSA) increases the minimum salary threshold for overtime eligibility for most salaried workers. Most salaried workers who earn less than $43,888 annually will be eligible for overtime. That reflects a change in the exempt classification from $684 to $844 per week. The overtime exemption amount will increase again on JANUARY 1, 2025, to $58,656 annually ($1,128 per week).

New EEOC definitions resulting in the need to review and update anti-harassment and anti-discrimination policies

The agency's guidance addresses some new topics, such as "misgendering," and also notes "outing" an individual as potential harassment. In terms of definitions, national origin harassment now includes *cultural and linguistic* characteristics while race harassment has been expanded to include protections extending to *name, cultural dress, and hairstyle* linked to a person's race. The guidance further clarifies "associational harassment." With regard to liability, the EEOC recognizes an employer's defense to hostile environment claims where the employer takes prompt remedial action to correct and prevent further such harassment.

Attorney Helene Horn Figman combines specialized legal knowledge in employment law with the skills and perspectives uniquely suited to Human Resources Consulting. www.figmanlaw.com

Information about her anti-harassment and anti-discrimination education programs can be found at www.workplaceawarenesstraining.com

This article has been prepared by the Law Offices of Helene Horn Figman, P.C. for general informational purposes only. It does not constitute legal advice and is presented without any representation of warranty whatsoever.

Helene Horn Figman

Law Offices of Helene Horn Figman, P.C.

Employment Law & HR Resource Management

45 Bristol Drive Suite 207, South Easton, MA 02375

FigmanLaw.com hfigman@figmanlaw.com

508-238-2700

In This Issue:

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
508 272-5120
SusanR@GrammarGoddess.com