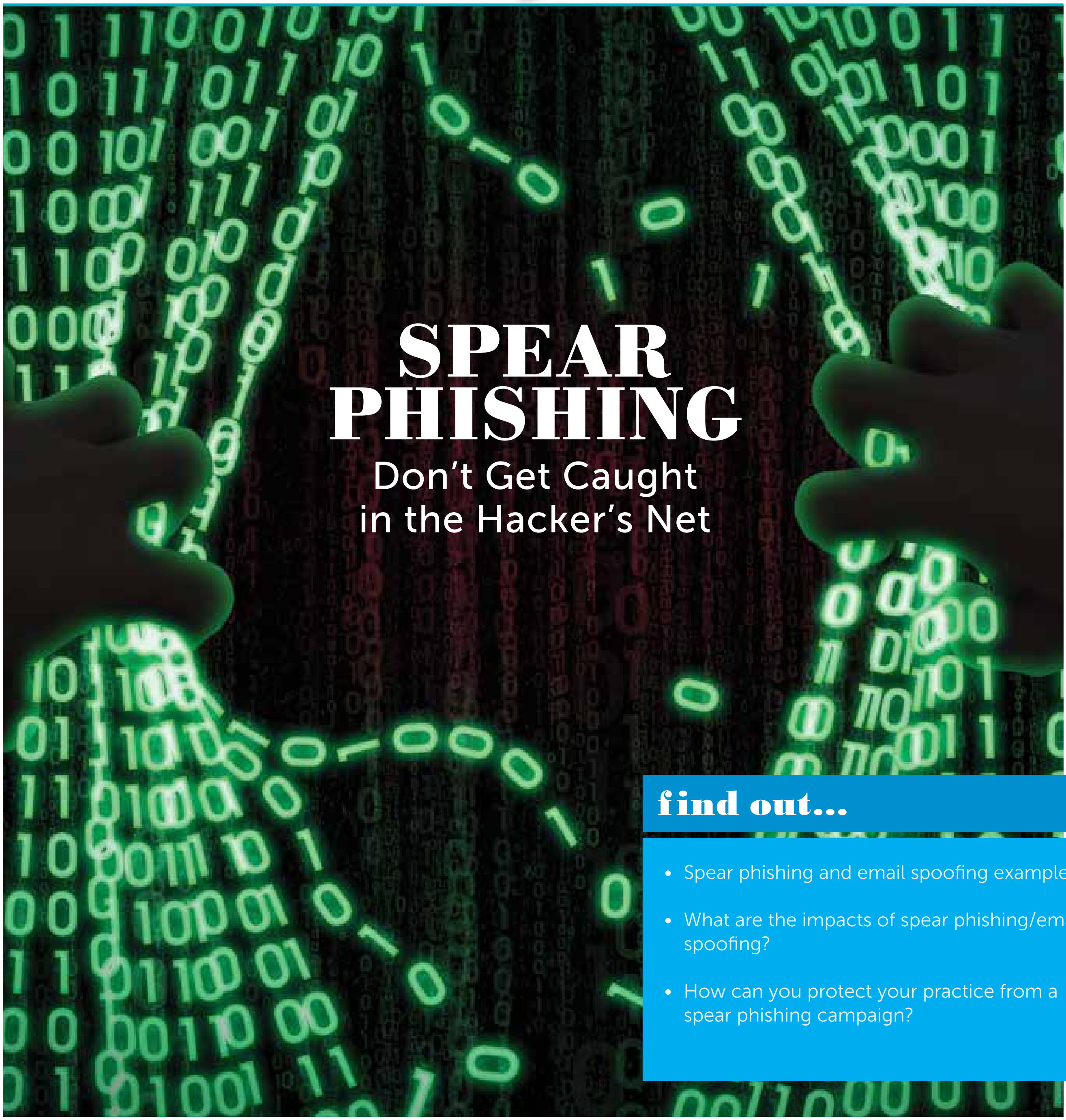
Publication of Medical Mutual / Professionals Advocate®

DOCTORS RX

Volume 30, No. 2

Fall/Winter 2022



SPEAR PHISHING

Don't Get Caught in the Hacker's Net

find out...

- Spear phishing and email spoofing examples.
- What are the impacts of spear phishing/email spoofing?
- How can you protect your practice from a spear phishing campaign?

A LETTER FROM THE CHAIR OF THE BOARD

Dear Colleague:

The ongoing cyber threat to Physicians and their practices has evolved. Hackers and other nefarious actors are developing sophisticated ways to infiltrate protected health information and practice's vital resources and information. However, this newsletter addresses straightforward risk mitigation tactics so that you can avoid being caught in the hacker's net.

George Malouf

George S. Malouf, Jr., M.D., FACS
Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate Insurance Company

ISSUE HIGHLIGHTS

WHAT IS SPEAR PHISHING? 2

WHAT CAN TRAINING AND EDUCATION DO FOR YOUR PRACTICE? 3

ADDITIONAL CYBERSECURITY REMINDERS 5

DOCTORS RX

Michael Doll, Editor,
Director of Risk Management

Dr. George S. Malouf, Jr., M.D., Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

Articles reprinted in this newsletter are used with permission. The information contained in this newsletter is obtained from sources generally considered to be reliable, however, accuracy and completeness are not guaranteed. The information is intended as risk management advice. It does not constitute a legal opinion, nor is it a substitute for legal advice. Legal inquiries about topics covered in this newsletter should be directed to your attorney.

All individuals involved in the creation and planning of continuing medical education activities sponsored by MEDICAL MUTUAL are expected to disclose to program participants any real or apparent conflict(s) of interest related to the content of their presentation. All individuals in control of content for this education activity have indicated that they have no relevant financial relationships to disclose.

CONTACT

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	800-492-0193
Risk Management Program Info	ext. 215 or 204
Risk Management Questions	ext. 169
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	mmlis.com proad.com

SPEAR PHISHING:
DON'T GET CAUGHT IN THE HACKER'S NET

Jeremy R. Krum
Trial Attorney and Partner at Armstrong, Donohue, Ceppos, Vaughan & Rhoades

Cyber attacks are on the rise. Hacking is becoming more sophisticated, more traumatic, and more personal.

Consider the following examples:

THE TARGETED SPEAR PHISHING

Your newest staff member has been set up with a computer workstation and an email address. They have been added to your company's website, complete with a detailed biography, photograph, title, and direct contact information. They have reviewed your company's employee handbook and written policies and procedures and are up to date with HIPAA training and compliance. Three days into the job, the new employee receives an email from your IT consultant. In the email, the IT representative apologizes for the hassle but notifies the employee that their new user account for the patient portal was bouncing back with invalid credentials. The email identifies the employee's direct supervisor by name. The email further instructs the employee to reset their username and password via an attached link, or to simply forward their credentials to the IT consultant to manage. The employee complies, and later that afternoon the practice's network becomes disabled by encrypted ransomware.

THE SOPHISTICATED SPOOFING

On Tuesday afternoon, your practice manager receives an email from one of the group's busiest Physicians. The sender's email address includes the Physician's name and appears legitimate. However, the practice manager does not realize that the email address was manipulated and actually includes a hidden, unfamiliar domain name. The email requests that the practice manager urgently send payment to a new vendor for the medical group and provides specific instructions on how to complete the transaction. An invoice is attached. The email further explains that the Physician is tied up with appointments for the day and needs the transaction to be completed quickly to avoid additional fees to the practice. Accordingly, the practice manager promptly complies and sends the purported vendor $8,250.00. Two weeks later, the practice manager learns that no such vendor exists, and the email was a spoof. The payment is not recoverable.

Through these examples, we highlight steps you can take to minimize a cybercriminal's opportunity to target your practice. This article will further provide guidance to help you avoid falling victim to a malicious phishing attack and getting caught in the hacker's net.

Earlier this year, the Federal Bureau of Investigation (FBI) reported an unprecedented increase in cyber attacks and malicious cyber activity. In fact, data published in the FBI's 2021 Internet Crime Report identified that phishing and other related email scamming techniques increased from 25,443 in 2017 to 323,972 in 2021. Losses from phishing scams alone totaled over $44 million, and losses from business email compromise totaled nearly

Consider

Both large and small medical practices are at risk, as cybercriminals have become increasingly sophisticated at spear phishing with online social engineering.

$2.4 billion. According to the 2021 Internet Crime Report, there were 11,693 victims of cybercrime in Maryland, ranking 14th in the country. Virginia ranked slightly higher at 12th overall with 11,785 victims.

ACCORDING TO THE 2021 INTERNET CRIME REPORT, THERE WERE 11,693 VICTIMS OF CYBERCRIME IN MARYLAND, RANKING 14TH IN THE COUNTRY.

Physicians and their staff are routinely targeted by cybercriminals. Both large and small medical practices are at risk, as cybercriminals have become increasingly sophisticated at spear phishing with online social engineering. The impacts of a cyber attack are not just financial. They also can include time spent responding to and investigating an attack, time spent away from patient care, damage to reputation, and lost revenue. With more daily business activity and transactions conducted via email, Physicians and their staff must remain vigilant in carefully reviewing and authenticating email traffic and ensuring that all employees have proper training and awareness of evolving email scams and cyber threats.

Even if you are cautious and prudent, a sophisticated spear phishing or spoofing attack can be difficult to recognize. So, what can you do? How can you avoid losing time, revenue, and patient data due to a cyber attack?

Here are several ways to improve your practice's email safety and security:

Planning

First, as simple as it sounds, you should expect phishing emails. Be on the lookout. Despite junk email programs and quarantine software, phishing emails will make their way to your inbox. Be leery of emails that are not specific to you, along with emails using unusual language or tone. Question unexpected emails. While obvious grammatical and syntax errors can be an easy giveaway, many phishing emails are well drafted and well prepared. As outlined above, many phishing emails are quite clever, while others are as basic as, "Can you handle a task for me this morning?" Once you respond, your email server may accept the hacker's email address as a recognized contact.

WHAT IS SPEAR PHISHING?
DEFINITIONS

Phishing*: The use of unsolicited email, text messages, or telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

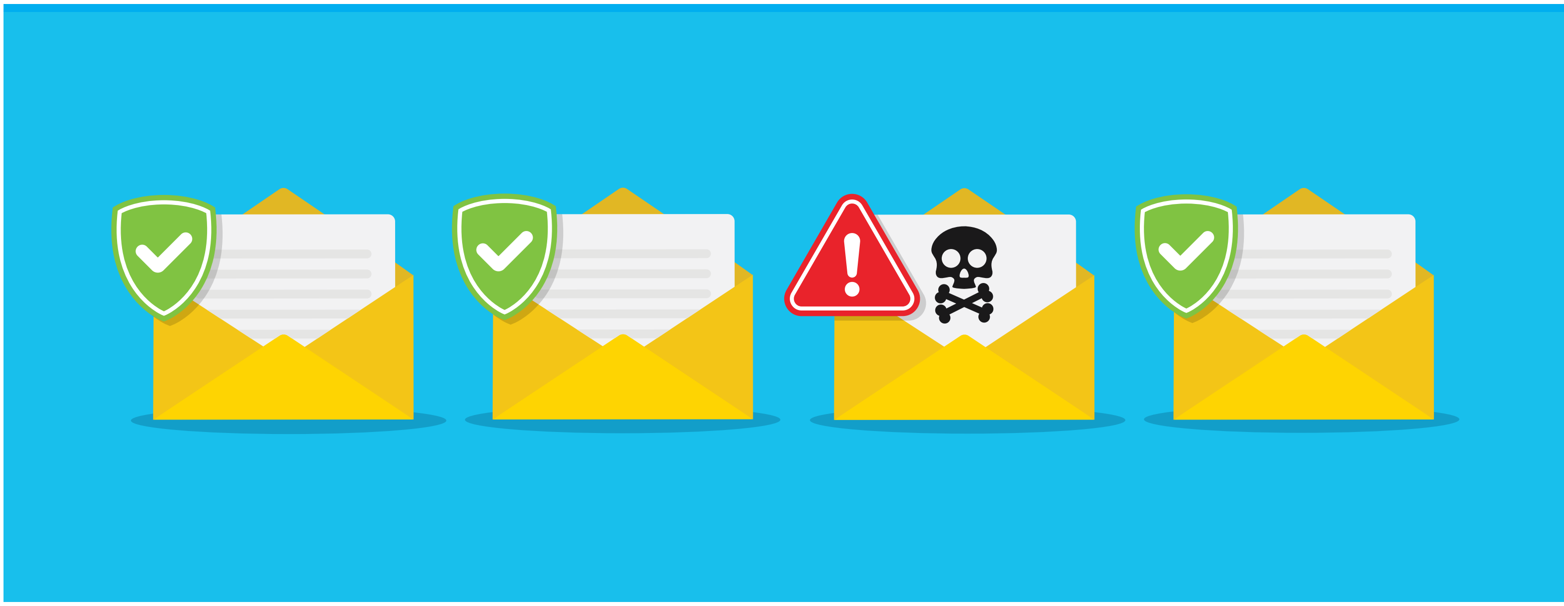
Spear Phishing: A type of phishing campaign that targets a specific person, and generally includes particular requests or personal information unique to the target.

Spoofing*: Contact information (phone number, email or website) is deliberately falsified to mislead and appear to be from a legitimate source.

Business Email/Account Compromise*: A scam targeting businesses or individuals regularly performing wire transfer payments, including sophisticated scams compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

**Adapted from the 2021 Federal Bureau of Investigation Internet Crime Report.*



Training and Education

Every member of your staff should be trained and educated on email security and spear phishing/spoofing. More importantly, training should begin on day one for any new employee. As identified above, hackers often target the newest employees. New employees can be vulnerable, as they may not yet know what types of business transactions in your practice occur via email. They also may be more reluctant to immediately question an email inquiry. Additionally, conduct refresher training for all staff members at least every two years, if not more often, depending on evolving threats or changes to the law. While there are many online options for cybersecurity training, there are in-service programs that can often be provided by your practice's IT provider, or even a local or regional computer forensics provider. You can even incorporate your practices's cybersecurity training with other in-service HIPAA programs or staff meetings.

Reviewing Email Domains

The easiest way to be tricked by a spear phishing email is not to look at the sender's complete email domain. It's quite easy for a hacker to manually alter an email username to spoof the identity of someone you know. Hackers also can spoof email addresses by simply changing one letter of an otherwise legitimate email address. Don't rely on the sender's email username. Rather, read and review the full and complete email domain name. Many email service providers automatically display email domain names. However, with some service providers, you may need to hover your curser over a sender's email username or click on the name to reveal the full domain name. If you are not certain of how to review a full email domain name, ask your IT provider.

External Email Alerts

Many practices have set up automated external email alerts, and most email service providers/server programs offer this feature. Thus, when an email is received from an external source, you receive an alert imbedded in the email. This alert can remind you to proceed cautiously and also may identify that an email which appears to come from an internal source (such as a colleague or staff member) is indeed a fake email from an external threat. Be mindful of 'alarm fatigue' when implementing these external email warnings. If the vast majority of your emails are tied to an alert, the alert risks being ignored.

Note

The easiest way to be tricked by a spear phishing email is not to look at the sender's complete email domain.

Consider

Not only should you consider having a qualified IT professional guide your day-to-day technology and security operations, you should also consider having an IT professional available for email or phone consultation.

Email Hyperlinks

To the extent possible, avoid clicking or using imbedded hyperlinks in emails. If you don't know where the hyperlink will take you, don't use the link. If you know where the link will take you, use your web browser and go to the webpage, directly. If you are sent the link by someone you trust, call the person to verify the source's intentions. While this may not always be an option, especially for web locations with complex URLs, the best practice is to always avoid email hyperlinks.

IT Resources

Not only should you consider having a qualified IT professional guide your day-to-day technology and security operations, you should also consider having an IT professional available for email or phone consultation. Large practices may have this expertise on sight. Smaller practices can secure these services from an IT vendor or consultant. From time to time, you will receive legitimate emails that appear suspicious. Perhaps a genuine email will arrive from a new contact or vendor with a hyperlink to an invoice. If you are not certain whether the email is actually from the vendor, have an IT professional isolate the email and verify its authenticity without exposing your network to malware. This verification could help you avoid clicking on a nefarious email link.

Company Websites

Striking the proper balance between marketing your practice and ensuring cybersecurity can be difficult. You want to market your practice and present your team of providers and staff to the public. You also want your patients to have easy access to contact information and other information about your practice. At the same time, you need to maintain system security. With that in mind, you may consider limiting individual contact information, detailed biographical data, and company affiliations from your website. You also may consider limiting the types of information contained on Facebook, Twitter, LinkedIn and other social networking sites. We know that hackers spend a significant amount of time researching their targets and use social engineering to trick and mislead their victims through spoofing and phishing emails. Hackers use your website or social media sites to identify new employees, learn which employees work for which supervisors, and gather individual contact information

and personal data to create fraudulent communications.

Software

There are numerous software programs that can reduce the incidence of 'junk mail,' including spear phishing and spoofing emails. There are also several software programs that can help protect your network if you inadvertently click on a malicious email hyperlink or attachment, or download malware. You should consult a reputable IT professional to assess the software options that will meet the specific needs of your practice.

Wire Transfers

Wire transfers are becoming more common for fast and efficient business transactions but can be very risky. We recommend implementing the highest degree of verification and authentication before engaging in any wire transaction. Even when you are confident that a wire transfer is appropriate, never engage in a wire transfer by email verification alone. Rather, make ***direct telephone contact*** with the person with whom you wish to make the transfer ***at the time*** of the transfer. Verify transaction data directly, and if any suspicions or concerns arise, change the method of payment. As noted below, you also may consider implementing and utilizing dual factor accounting practices.

Dual Factor Accounting

Let there be no single point of failure. What does that mean? For any significant business transaction, consider implementing policies and procedures requiring participation of at least two qualified individuals. A simple set of checks and balances in accounting can help mitigate the risk of a successful scam. Adding another layer of review and approval can also provide additional protection your company may need to prevent internal and external accounting losses.

ADDITIONAL CYBERSECURITY REMINDERS

Although it can be inconvenient, utilize complex passwords that are changed every ninety days, if not sooner. The longer the password, the better. Likewise, if possible, enable dual-factor authentication (with a separate unique code sent to you by text or email). Dual-factor authentication is now the gold standard for added identity theft protection.

If you have remote access to your network servers, make sure to regularly monitor access. Shut down any old or outdated remote access

Remember

Dual-factor authentication is now the gold standard for added identity theft protection.

Remember

With vigilance and proper controls in place, you and your practice can better identify and mitigate cyber risks and avoid being the next target caught in the hacker's net.

workstations. The easiest way to allow a cybercriminal into your network is to leave an old remote access workstation open with a weak password. Consult your IT professionals to routinely review remote access users.

You may even consider hiring a qualified computer forensics company to perform annual or biennial vulnerability assessments of your computer network. Often referred to as an "ethical hack," a vulnerability assessment is a "test" of your systems by a trusted IT vendor to determine what areas of your IT systems are vulnerable to potential penetration by hackers. Knowing where your vulnerabilities are will give you the tools you need to fix any potential flaws in your cybersecurity.

KEY "TAKEWAY" POINTS

- Cybercrime is escalating and will continue to present significant risks to medical practices.
- Be vigilant in carefully reviewing external emails and verifying sender data and domains.
- Train employees and staff early and often. Without additional safeguards in place, one well-crafted email sent to one unsuspecting individual could expose your entire network to cybercrime.
- Be cognizant of social engineering vulnerabilities. Everything you post online about you and your staff is subject to exploitation by cybercriminals.
- Meet with those responsible for your IT systems regularly to ensure that your network security is well monitored, maintained, and updated.

CONCLUSION

Spear phishing and spoofing emails are likely here to stay for the foreseeable future. However, Physicians and their practices can take steps to lessen the risk of these cyber attacks. With vigilance and proper controls in place, you and your practice can better identify and mitigate cyber risks and avoid being the next target caught in the hacker's net.

CME TEST QUESTIONS

1. Spear phishing is a type of campaign that targets a specific person, and generally includes particular requests or personal information unique to the target.

   A. True B. False

2. You should never expect phishing emails since they will most likely be caught in your spam or junk folders.

   A. True B. False

3. It is not easy for a hacker to manually alter an email username to spoof the identity of someone you know.

   A. True B. False

4. It is best to try and avoid clicking on imbedded hyperlinks in emails if you don't know where the link will send you.

   A. True B. False

5. Having a qualified IT professional guide your day-to-day technology and security operations is important.

   A. True B. False

6. You don't need to limit individual contact information or biographical data on company sites.

   A. True B. False

7. It is good practice to make direct telephone contact with the person you wish to make a wire transfer to at the time of the transfer.

   A. True B. False

8. A simple set of checks and balances in accounting can help mitigate the risk of a successful scam.

   A. True B. False

9. Short passwords are convenient and should be changed every year.

   A. True B. False

10. A vulnerability assessment is a "test" of your systems by a trusted IT vendor to determine what areas of your IT systems are vulnerable to potential penetration by hackers.

    A. True B. False

Instructions – to receive credit, please follow these steps:

Read the articles contained in the newsletter and then answer the test questions.

1. Mail or fax your completed answers for grading:

   Med•Lantic Management Services, Inc. | Fax: 443-689-0261
   P.O. Box 8016 | 225 International Circle | Hunt Valley, Maryland 21030
   Attention: Risk Management Services Dept.
2. One of our goals is to assess the continuing educational needs of our readers so we may enhance the educational effectiveness of the *Doctors RX*. To achieve this goal, we need your help. You must complete the CME evaluation form to receive credit.
3. Completion Deadline: March 31, 2023
4. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

CME Accreditation Statement

MEDICAL MUTUAL Liability Insurance Society of Maryland is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians.

CME Designation Statement

MEDICAL MUTUAL Liability Insurance Society of Maryland designates this enduring material for a maximum of one (1) *AMA PRA Category 1 Credit*.™ Physicians should claim only the credit commensurate with the extent of their participation in the activity.

CME EVALUATION FORM

Statement of Educational Purpose

Doctors RX is a newsletter sent twice each year to the insured Physicians of MEDICAL MUTUAL/Professionals Advocate.®
Its mission and educational purpose is to identify current health care-related risk management issues and provide Physicians with educational information that will enable them to reduce their malpractice liability risk.

Readers of the newsletter should be able to obtain the following educational objectives:
1) Gain information on topics of particular importance to them as Physicians
2) Assess the newsletter's value to them as practicing Physicians
3) Assess how this information may influence their own practices

CME Objectives for "Spear Phishing: Don't Get Caught in the Hacker's Net"

Educational Objectives: Upon completion of this enduring material, participants will be better able to:
1) Understand what spear phishing is and what to look out for
2) Common risk mitigation strategies to combat potential hacker intrusion
3) Key takeaways that can help prevent a successful spear phishing campaign

	Strongly Agree				Strongly Disagree
Part 1. Educational Value:	5	4	3	2	1
I learned something new that was important.	❑	❑	❑	❑	❑
I verified some important information.	❑	❑	❑	❑	❑
I plan to seek more information on this topic.	❑	❑	❑	❑	❑
This information is likely to have an impact on my practice.	❑	❑	❑	❑	❑

Part 2. Commitment to Change: What change(s) (if any) do you plan to make in your practice as a result of reading this newsletter?

____
____
____

Part 3. Statement of Completion: I attest to having completed the CME activity.

Signature:______________________________________ Date:____________________________

Part 4. Identifying Information: Please PRINT legibly or type the following:

Name:____ Telephone Number:________________

Address:____
____
____
____

RISK MANAGEMENT NEWS CENTER

YOU CAN PHONE A FRIEND IN RISK MANAGEMENT

Although we offer many resources on our web sites (**www.mmlis.com/resources** and **www.professionalsadvocate.com/resources**), we understand that sometimes it's just easier to talk to someone. Insureds of MEDICAL MUTUAL and Professionals Advocate can call 410-785-0050 or 1-800-492-0193 to speak to a qualified risk management (RM) specialist anytime 8 a.m.-4:30 p.m. Monday-Friday. No matter your specialty, if you have a practice-related question or concern, we're ready to listen and offer guidance to help you identify and reduce your liability risk exposure. Please note, however, that any advice given from MEDICAL MUTUAL /Professionals Advocate should not be construed as legal advice.

THERE'S STILL TIME TO RECEIVE YOUR DISCOUNT AND CMES

It's not too late! Insureds who complete their risk management education by December 16, 2022, will be eligible to receive a 5% discount on a 2023 renewal policy and CME credits. Home study and online risk management education programs are available. For additional information and to register, visit our web site at **mmlis.com** or **proad.com**

INTRODUCING RISK MANAGEMENT DIRECT

We have updated the way you can locate important risk management resources on our website. Through Risk Management Direct, you will be able to choose from a variety of specialties such as Internal Medicine, Dermatology, Surgery and more, as well as general topic areas pertinent to your practice. These resources will then be "pushed" automatically to your Insured dashboard. Whenever you log in, new information will populate this area. Keep a look out in the coming weeks for Risk Management Direct!

MEDICAL MUTUAL and Professionals Advocate offer a variety of online tools and resources that are specially designed to help Doctors identify and address preventable issues before they escalate into potentially serious legal action.

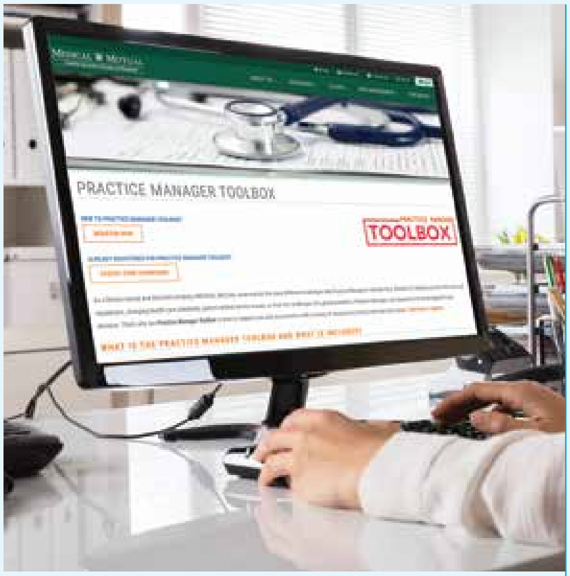
MEDICAL MUTUAL Liability Insurance Society of Maryland

Professionals Advocate® Insurance Company

Home Office: Box 8016, 225 International Circle
Hunt Valley, MD 21030 • 410-785-0050 • 800-492-0193

DOCTORS RX

Publication of MEDICAL MUTUAL / Professionals Advocate®



ARE YOU LEVERAGING THE PRACTICE MANAGER TOOLBOX?

If they haven't already registered, please encourage your Practice Managers to register for our Practice Manager Toolbox online at **mmlis.com/content/practice-manager-toolbox** or **professionalsadvocate.com/content/practice-manager-toolbox-pap**. The resources provided through the PMT covers topics such as cybersecurity, patient engagement, compliance, billing and insurance, and EHR optimization.

REGISTER TODAY!

MEDICAL MUTUAL
Liability Insurance Society of Maryland

PROFESSIONALS ADVOCATE®
Insurance Company