CNA

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

Phishing Attacks Use Bar Complaints and HIPAA Audits as Bait

Attorneys have access to sensitive information and large sums of money, and although they are experts in many areas, they are seldom on the cutting edge of new technology. It should come as no surprise, then, that a growing number of email scams are targeting attorneys and other similar professionals. By mirroring an email from a state bar, legal organization, disciplinary board or government entity, these scams take a narrower focus than scattershot emails offering a free cruise or a once-in-a-lifetime deal with a Nigerian prince.

This brand of phishing uses a victim's trust (or sometimes fear) of an institution as a way of influencing that person to download a malicious attachment, click on a malicious link, or transmit sensitive information to a third party. While some phishing emails remain easy to detect, others have begun displaying an incredible attention to detail. "Spoofing," a phishing tactic that involves the technical manipulation of the email header or IP address so that it appears to have been sent from a trusted source, is especially difficult to counteract.

The two examples below illustrate the targeted nature of newer phishing attacks and the level of sophistication they employ, but also present an opportunity to educate attorneys on what they can do to avoid becoming a victim.

BAR COMPLAINT SCAM

Officials from state bars across the country continue to warn of fraudulent emails purportedly conveying notice of a disciplinary complaint. Attorneys in Alabama, California, Florida, Georgia and Nevada reported receiving the phony emails as early as last summer, but emails have continued to surface through 2017. A variant of the scam appeared in Florida alleging a past due invoice rather than a bar complaint, but the details have remained more or less the same.

Like most phishing attempts, the email appears to have originated from a trusted source, whether it is the state bar, bar association, or even attorney general's office. It includes an urgent call to action, typically a response within ten days, and prompts the recipient to download an attachment or follow a link to view the relevant complaint or invoice. Following these instructions, you may have guessed, triggers the introduction of malware onto your system.

This malware may directly extract data from your network, but with growing frequency devices are instead infected with ransomware which encrypts the recipient's hard drive. Only upon paying a fee, subject to strict, time-sensitive instructions, will the device be decrypted and restored. Failing to comply leaves your data unusable and likely compromised.

While some phishing emails remain easy to detect, others have begun displaying an incredible attention to detail.

Avoiding the Scam

This scam, although cleverly taking advantage of an attorney's trepidation upon receiving a bar complaint, is still somewhat crude. The emails often do not use letterhead or formatting that might accompany an official email, may include misspellings, and contain only a brief and vague description of the "rebuttal" process. In the example provided by the New York Attorney General's Office, the display name of the sender is "The Office of the State Attorney," but the sender's email address is "com.department@outlook.com" which should raise a red flag.[1]

Even so, attorneys who receive an unexpected email should avoid answering any call to action before confirming the message's authenticity with the organization that allegedly sent it. Any government or private entities that request your immediate action via email will be able to confirm by way of a secondary, independent[2] method of communication that they have contacted you. They will then assure you that the email is authentic, or spread the word to others who may have also received the malicious email.

Although most state bars warn that they never send disciplinary correspondence via email, some do, and many state bar associations send email requests for dues. Attorneys should be on the lookout for similar bar complaint scams in their states and, as always, periodically back up their hard drives to protect their firms in the event that they fall victim to ransomware.

HIPAA AUDIT SCAM

As the Health Insurance Portability and Accountability Act of 1996 continues to evolve, attorneys should take note of a scam that targets practitioners who may not be familiar with HIPAA's newest rules and procedures. An unknown number of emails styled as official letters from the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), complete with OCR Director Jocelyn Samuels' signature and very convincing office letterhead, have been sent under the guise of OCR's HIPAA Privacy, Security and Breach Notification Audit Program.

On January 17, 2013, the OCR issued amendments to the HIPAA Privacy, Security, and Enforcement Rules which imposed HIPAA compliance upon attorneys in their role as potential "business associates" under HIPAA. Sanctions for failure to comply include significant civil monetary penalties. Part of this expansion includes regular audits initiated through email. Now, seizing upon the uncertainty surrounding HIPAA expansion and the ease with which potentially thousands of entities can be targeted via email, a third party has attempted use the threat of an audit for financial gain.

The fraudulent email prompts the recipient to follow a link which appears to lead to a government website. In reality, the link leads to a non-governmental website marketing a firm's cybersecurity services. Although the effect of this particular scam does not appear to be particularly damaging, apart from exposing countless professionals to unwanted marketing materials, attorneys should remain vigilant against similar phishing tactics that may inflict far more destructive consequences.

Avoiding the Scam

Given the careful attention to detail behind this phishing email, it is especially difficult for a recipient to detect without any advance warning. The letterhead and signature show no signs of fraud, and the sender email and URL are nearly identical to their legitimate counterparts. The fake URL ends in ".us" rather than ".gov," but the ".us" domain is used by some federal government agencies. The email also lacks spelling or grammar mistakes that often accompany a phishing attempt.

- Legitimate Sender: OSOCRAudit@hhs.gov
- Fraudulent Sender: OSOCRAudit@hhs-gov.us

- Legitimate URL: http://www.hhs.gov
- Fraudulent URL: http://www.hhs-gov.us

It may have been useful, in this instance, to search for the correct HHS website and compare the URL to the one included in the email. Using this technique for every questionable email could become tedious, however, and may not always be effective. The best strategy, and the one recommended by the OCR, is to simply contact the office and verify that the audit email is real.[3]

1 See here for the full email
2 Meaning that the recipient should not, for example, call a number listed only on the possibly fraudulent email, or reply directly to that email

3 The OCR directs all questions regarding official communications to OSOCRAudit@hhs.gov.

CLOSING ADVICE

Recognizing specific phishing attacks is critical, but for many professionals such awareness comes too late. Instead, attorneys should focus on developing the following strategies:

- **Keep antivirus, web browsers and email clients updated.** Even momentary gaps in protection can be exploited by third parties.
- **Routinely back up your hard drives.** If disaster strikes, having a copy of valuable information secure and ready will help to mitigate the exposure.
- **Exercise caution with links and attachments.** Simply opening an email is safe—modern email clients (e.g. Outlook, Gmail) will not allow messages to automatically run scripts—but be wary of a call to action.
- **When in doubt, contact the sender directly.** You cannot assume that a fraudulent email will contain misspellings or other obvious mistakes; it is almost always worth the time to verify the email.
- **Educate and test your support staff.** A workforce is only as prepared as its weakest employee, so be sure to regularly instruct your entire staff regarding threats to data security.

As the previous phishing attacks illustrate, scammers are becoming more refined, with respect to both the tactics they use and the victims they target. As an attorney, you have a duty to your business and your clients to be familiar with the warning signs, remain educated on emerging threats, and prepare your firm accordingly.

This article was authored for the benefit of CNA by:
Matthew Fitterer

Matthew Fitterer is a Risk Control Representative for CNA's Lawyers Professional Liability Program. He is responsible for providing risk control guidance to CNA insureds in the form of written publications, online and live presentations, and direct consultations. Prior to joining CNA, Matt worked in the Chicago-area as an attorney for a small law firm specializing in criminal defense and civil rights litigation, and for a solo practitioner focusing on commercial litigation. Matt is licensed to practice law in Illinois and has been designated as a Commercial Lines Coverage Specialist (CLCS) by the National Underwriter Company.

CNA

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com.