5-2019

Bar Bytes: Phishing Update - A Whale of a Tale

Aaron Glenn

BAR BYTES

Phishing Update – "A Whale of a Tale"

By Aaron Glenn, JD, MLIS

Bar Bytes has previously addressed the dangers posed by "phishing" emails: messages that seek to trick recipients into revealing secrets and clicking on links or attached files that contain malware.[1] The points raised then remain valid today, and this update seeks to offer additional information and strategies for combating phishing attempts. Detecting and avoiding this threat requires constant vigilance; it only takes one mistake to compromise your data.

Know the threat

Phishing attempts take many forms, crafted with varying degrees of deception by scammers. While basic phishing attempts can be relatively easy to spot, targeted phishing attempts – known as "spear-phishing" – are much more troublesome. A spear-phishing email will attempt to trick you or others at your firm by masquerading as a message from a trusted sender. The message may appear to be from a co-worker, a client or a third party such as a financial institution. Indeed, some scammers have used targeted emails to redirect wire transfers.[2] The scammer may include publicly available information, such as details gleaned from an online directory, or even your own website to make the attempt look more convincing. A related tactic, known as "whaling," is used to prey on an employee's eagerness to please an employer and occurs when scammers impersonate the management or leadership of an organization. Instead of currying favor with a supervisor, the employee then unknowingly does the bidding of a scammer.

If you believe that an email is a phishing attempt, delete it and do not interact with the message in any way. Once the recipient of a phishing email has taken the bait and clicked on a malicious link or infected attachment, there is no going back. The recipient of the message may be tricked into revealing confidential information or the email account may be hijacked and used for further phishing attacks. The affected computer may be stricken with "ransomware," a type of malware that will encrypt your files and make them inaccessible unless you pay a fee to the scammers. A new risk, dubbed "cryptojacking," allows scammers to syphon processing power from your computer for their own projects – such as mining for cryptocurrencies like BitCoin.[3] The best way to avoid these outcomes is to practice a balanced approach of detection and preparation.

Know your contacts

To defend against all forms of phishing, it is helpful for everyone in a firm who is using a computer to be well-versed in recognizing the hallmarks of a phishing email, including: typos, an unfamiliar domain name in the sender's email address, and demands for an immediate response. The increasingly sophisticated nature of spear-phishing and whaling attempts has made it imperative that suspicious emails be given additional scrutiny. If a dubious email appears to be from an acquaintance or co-worker, it is much better to call that person for verification than take the chance of being hoodwinked.

A recently reported example of a whaling scheme was directed at academia; scammers posing as deans or department heads attempted to trick faculty at multiple institutions into purchasing gift card codes for them as a favor (promising reimbursement, of course).[4] Those who responded to the phishing messages often found the requests odd, unprofessional or otherwise unlike the individual the scammers were attempting to emulate. However, for newer faculty members – or those unfamiliar

with the writing style of a new administrator – these messages can be harder to detect.

This scenario could easily play out in a law firm setting. Let's suppose a newly hired employee receives such an email that appears to be from a supervisor, or even a partner. The email could ask the employee to perform any number of tasks: authorize a purchase, provide log-in credentials or review an attached document that is infected with malware. Newer hires are especially at risk since they may not yet be familiar with the conversation style or writing habits of others in the firm.

Know your plan

Hope for the best but prepare for the worst. Here are a few steps that you can take right now to shore up your defenses:

- Prepare a plan that details how your firm will respond to a successful cyberattack. Include procedures for isolating infected machines, responding to client inquiries and for minimizing chaos in the wake of the attack. Consult an IT security professional for addressing additional concerns and consider your insurance options to ensure you have adequate coverage.
- Offer cybersecurity training for all employees and especially new employees.
- Ensure that your computers and software are updated and have the latest security patches.
- Make routine back-ups of your files and keep at least one copy saved off-site. If your security is compromised, you may be able to restore your operations using one of these recent backups.

Despite the best efforts at detecting phishing attempts, one may still slip past your defenses. If that happens, your preparation will be vital to preserving not only your data, but your reputation as well; how will your clients respond if your firm suffers a breach and you are caught completely off guard?

For more information and helpful resources, please visit the University of South Carolina Law Library's cybersecurity resource guide: https://guides.law.sc.edu/cybersecurity.

Additional information on protecting your data also can be found on the South Carolina Bar Technology Committee's page at www.scbar.org/tech.

Aaron Glenn, JD, MLIS, is a reference librarian at the University of South Carolina Law Library.

Endnotes

[1] Courtney Kennaday & Emily Worley, *Protection from Phishing*, SC Lawyer, July 2016, at 10.

[2] Mark Bassingthwaighte, *How to Minimize the Risk of Becoming a Victim of Wire Fraud*, South Carolina Bar (Jan. 18, 2017), www.scbar.org/bar-news/article/how-minimize-risk-becoming-victim-wire-fraud/.

[3] James M. McCauley et al., *Is It Ethical for Lawyers to Accept Bitcoins and Other Cryptocurrencies?*, N.C. St. B.J., Fall 2018, at 36.

[4] Lindsay Ellis, *Gift-Card Phishing Scheme Targets Professors' Zeal to Please the Dean*, The Chronicle of Higher Education, February 1, 2019, at A21.