Morrison Cohen

Client Alert | October 18, 2024

Morrison Cohen Cyber Watch: Navigating the Cyber Landscape Safely, Part Three

Top Tips to Avoid Getting Hooked by Phishing Threats

Stay ahead of the game: unveiling scam tactics, spotting red flags and partnering with trusted advisors for comprehensive security

Phishing Scams Are Everywhere

According to a 2024 study, nearly half of U.S. adults polled have personally encountered a cyber threat or scam, and approximately one in five of those persons fell victim to, and lost money in, the scam. Phishing, whether by email, phone call, text message, or other media, comes in many forms, and is, at its core, intended to deceive recipients into releasing sensitive information, installing malware on their device that sends sensitive information to threat actors, or manipulating individuals or accounts for the benefit of the threat actor. For example, a common scam is to send emails that appear to come from the victim's bank, asking the victim to log into their account, often claiming that they need to resolve a fraudulent charge, but routing the victim to a different website that appears indistinguishable from that of the victim's bank, and stealing the victim's credentials after they are input, therefore allowing the threat actor to obtain access to the victim's real bank account.

How New Technology Is Being Leveraged

Threat actors have been using phishing attacks for decades, but such attacks have become increasingly more sophisticated and harder to detect, particularly since generative artificial intelligence (AI) tools have become widely and cheaply (or freely) available. These tools can quickly create believable websites and emails, and deepfakes which appear to be convincing images and videos of known individuals. These AI tools have also made it possible for threat actors to spoof email addresses and phone numbers much faster and more convincingly than before.

In this alert, we aim to highlight a few recent phishing trends that we have observed, and to provide some tips that will hopefully assist in identifying some of these attacks early on.

Recent Trends in Phishing Attacks

Diverting Transfers of Funds. Threat actors are always on the lookout for ways to divert funds from intended recipients. A threat actor may gain access to an email inbox in any number of ways (e.g., sending emails containing links or documents that, once opened or clicked, will download malicious code onto a device; getting someone to provide their email login credentials by pretending to be a member of a company's helpdesk; etc.). Once the threat actor has access to someone's email account, they can lay in wait, and monitor the progress of a transaction until the time comes for a wire or digital assets transfer to be made, or for funds to be deposited in escrow. The threat actor can then swap out wire transfer or recipient details. Because these messages come from a trusted source, the email recipient might not question the change. For example, a manufacturing company suffered over $5 million in losses after an employee opened a phishing email, purportedly from the company's bank, and entered his account

credentials into a fraudulent website, thus allowing the threat actors to access the company's bank account and transfer the funds to themselves.[1]

Spoofing. A threat actor may disguise their email address, phone number, or name in order to impersonate a trusted source, and may use generative AI to mimic the voice and/or appearance of a known individual in phone or video calls. Please note that the strategy of email "spoofing" can be used for a similar purpose (e.g., modifying the From, Reply-To, and Return-Path sections of an email header to resemble a legitimate sender, when in fact the email originates from a different server). The threat actor may then seek sensitive information, like login credentials or banking information. For example, a software development company suffered an estimated $4 million in losses after transferring digital assets to a threat actor who used an imposter email address that resembled the email domain of the software company's financial institution. [2]

Posing as a Creditor or Collections Agency. Threat actors may gain access to an email account, receipts, hard copy mail, trash, or purchase histories, and impersonate the company who provided products/services or a collections agency purportedly acting on the company's behalf. Once the threat actor connects with the business or individual being targeted, they will impersonate the legitimate creditor and attempt to divert funds rightfully payable to a service provider or other entity to themselves. The threat actors in these instances may use similar methods discussed herein (e.g., imposter emails, spoofing, bots) in perpetrating these scams.

Pig Butchering. Threat actors cold-contact individuals by phone, text or email, or on social media platforms, with a message aimed at striking up a conversation and establishing a relationship, often, although not always, pretending romantic intentions. Once trust has been established, the threat actor will introduce the idea of an investment, business deal, or other transaction (frequently a crypto purchase), and encourage the recipient to participate. The threat actor often then sends a fraudulent app or web platform that frequently appears quite convincing (e.g., shows real-time market data, offers video calls with the threat actor, appears to show the victim's investment "growing" after they deposit funds, allows the victim to withdraw small amounts of their funds from the platform, etc.). Once it appears that the victim has deposited all money or cryptocurrency that they have or can borrow, the threat actor shuts down the account, retains the funds, and disappears. For example, a former CEO of a Kansas-based bank sent an estimated $47 million over a period of eight weeks to cryptocurrency wallets controlled by threat actors, after being convinced that such "investments" would lead to profitable returns.[3] Pig butchering scams may leverage generative AI to develop convincing, articulate scripts and deepfakes that can be used when targeting victims.

Compromising Multifactor Authentication (MFA) Methods. Threat actors may use "bots" (software applications that are programmed to perform tasks autonomously, without human intervention) to deceive recipients into sharing MFA codes (e.g., legitimate access codes sent by a financial institution, credit card company, loan servicer, etc.). For example, the bot may send a text message or place a robocall (e.g., appearing as though it is coming from a bank, credit card company, or loan servicer, etc.), asking the recipient to authorize a charge or help resolve a technical issue with their account. Then, the bot may prompt the recipient to share the security/access code received from their financial institution, which the threat actor then uses to gain access to the account.

---

1 *Experi-Metal, Inc., v. Comerica Bank*, No. 09-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011). *See also Beins, Axelrod, PC v. Analytics, LLC*, No. CV 19-3794 (JEB), 2020 WL 1952799 (D.D.C. Apr. 23, 2020) (threat actor compromised law firm's email account and redirected a payment intended for the law firm into the threat actor's bank account).

2 *Nibi, Inc. v. John Doe*, No. 5:24-CV-06184 (N.D. Cal. 2024).

3 *See USA v. Hanes*, Case No. 6:24-CR-10013 (D. Kan).

Morrison Cohen

Detecting Signs of Phishing Attacks

While new technologies such as generative AI have made phishing attacks increasingly convincing, there are still often perceptible signs that such communications may be a scam, such as:

- Sense of urgency/emergency, and tight deadlines to take action.
- Unexpected email requests containing links or attachments.
- Promises to return high profits in a short period of time.
- Threats of criminal charges, if action is not taken.
- Requests for financial account information.
- Vagueness/lack of details relating to investment vehicles or purported debts.
- Requests that the recipient click on links or download files.
- Refusal to provide a mailing address, verifiable physical address, or phone number (e.g., an email that does not provide any other methods of contacting the sender).
- Phone numbers or email addresses which are unknown, or which appear similar (though not identical) to known senders, but include variations in the domain (e.g., @Amaz0n.com).
- Changes/updates to previously-issued wire or escrow instructions.
- Display names that don't match the reply-to email address.
- Grammar, punctuation or spelling errors.
- Inconsistencies in the appearance of logos, fonts, and other branding elements that do not match official communications.
- Generic greetings like "Dear User".

Protections to Consider

Businesses may be well advised to establish, implement, and frequently update their policies and procedures relating to transfers of assets and electronic communications. Some strategies may include:

- Examine all communications carefully for signs of phishing scams.
- Conduct regular simulated phishing exercises to familiarize your employees to the risks of phishing, and how to detect them.
- Establish clear policies for employees to follow if phishing attacks are suspected.
- Consider cyber insurance with coverage limits appropriate to the company's business and data processing activities.
- Consider password managers and passkeys, and avoid using the same password for multiple accounts.
- Require high complexity passwords, and multi-factor authentication for any sensitive systems (e.g., access to financial data).
- Activate already-existing multi-factor functionality offered by financial institutions and service providers.
- Select and retain personnel, technology and service providers with adequate experience and skill to help your business minimize and detect threats (including technology advisors).

Morrison Cohen

- Establish, maintain, and routinely update (1) incident response plans, and (2) protocols for financial transactions, and train personnel with respect to same.
- Implement robust email filters to automatically detect and block phishing emails containing suspicious content, links, or attachments.
- Ensure spam filters are properly configured to move potentially harmful emails into quarantine or the spam folder.
- Encourage users to report phishing emails through a designated button or process, enabling immediate investigation and blocking of threats.
- Install and regularly update anti-malware and anti-virus software.
- Utilize tools that scan email links in real-time to detect and block access to malicious websites.
- Continuously monitor for unusual activity that may indicate phishing attempts or compromised accounts.

Key Contacts

In the event of a phishing attack successfully perpetrated against your business (whether it results in unauthorized access to or disclosure of data, financial losses, and/or threat actors compromising or introducing malicious content into your systems), our Technology, Data & IP team is available to answer your questions and provide guidance regarding next steps, including advice as to potential claims or remedies that may be considered to try to redress the fraud perpetrated against your business.

Jessica L. Lipson
Partner & Co-Chair
D 212.735.8683
jlipson@morrisoncohen.com

Fred H. Perkins
Partner & Co-Chair
D 212.735.8647
fhperkins@morrisoncohen.com

Tess Bonoli
Associate
D 212.735.8728
tbonoli@morrisoncohen.com

Allison O'Hara
Associate
D 212.735.8807
aohara@morrisoncohen.com

The authors would like to extend their thanks to Morrison Cohen's Chief Information Security Officer, Thomas Catenaccio, for his invaluable contributions to this article.