INSIGHTS FOR EXECUTIVES

# THE CHALLENGE AHEAD: ADVANCED PHISHING THREATS

How much do you really know about advanced phishing threats? Phishing threats are designed to deceive you and to result in shocking levels of business compromise. They can ultimately cost you your organization's reputation and millions of dollars in losses. On average, scammers siphon off more than $47,000 per incident via fraud schemes related to executive-level phishing schemes and impersonation attempts. The latter have cost businesses as much as $25 million.[1]

Although CEOs don't parade down corridors with bags of cash or checks in-hand, CEOs and executive leadership teams should consider how they embody ideas about wealth, and historical tropes promising streets paved with gold. Cyber criminals are after the money. In guarding against exploit, CEOs and business leaders should focus on a combination of fraud-related knowledge gain, recognition of advanced phishing threats, and layering defense-in-depth solutions to protect people, systems, and assets.

## KNOWLEDGE ACQUISITION: WHAT IS CEO FRAUD?

CEO fraud refers to a diverse group of deceptive practices that exploit a Chief Executive Officer for criminal gain. Despite the characterization as "CEO fraud," all executives are at-risk of encountering deceptive fraud attempts.

Nearly 50% of all executive-focused cyber criminal activity takes the form of phishing; hence the focus in this report. Given executives' proclivity to conduct business at lightning speed, it pays to slow down, to take a moment to master must-know phishing info, and to avoid a ruinous fraud situation.[2]

[1] Robert Best, What is CEO Fraud and How Much Will it Cost Your Business?
https://www.infotech.co.uk/blog/what-is-ceo-fraud-and-will-it-cost-your-business

[2] Office 365 Phishing Attack Financial Executives Key Targets
https://www.cybertalk.org/2021/03/22/office-365-phishing-attack-financial-executives-key-targets/

A CEO attack can cost an organization millions.

## JEFF BEZOS: BUSTED BY PHISHING

Phishing attacks can target the most business savvy and well-respected of CEOs. In 2020, tech titan Jeff Bezos experienced a targeted phishing attempt (spear phishing) via WhatsApp. Jeff had participated in a WhatsApp group conversation, after which he downloaded a video clip containing malware. The malware whipped through Jeff's phone and exfiltrated data. The costs associated with this specific CEO attack are unknown to the public, however CEO attacks have been known to result in as much as $75.8 million in losses.[3]

## EXECUTIVES AT 150+ COMPANIES

Also in 2020, executives across 150 different companies simultaneously received targeted attack emails. The majority of the victims worked in the financial sector, although victims were reported across all industry verticals. The attackers aimed to deceive executives into handing over Office 365 login credentials via a falsified login site. The attack methodology involved sending a PDF file containing a link to a service page. Cyber security researchers could not confirm a motive for the attack, but access to a CEO's email account gives hackers lots of leverage; CEO fraud options, data exfiltration, intellectual property access, account numbers, banking information and more. Any of these companies could have (and may have) experienced a breach.

### Phishing in All Forms

The term phishing has come to broadly encompass a variety of different sub-categories of this general operational schematic; spear phishing, whaling, vishing, smishing, angler phishing, catfishing and pharming. Discovering the differences can help you defend accordingly.

- **Phishing:** A phishing attack involves a malicious message sent by cyber criminals, usually to a large swath of people. Historically, a single message could hit anywhere from 250 to 250,000 inboxes. The aim is to manipulate persons, usually employees, to download malware onto systems, unwittingly exfiltrated data, share credentials and follow-through on wire fraud activities. Ninety-six percent of phishing attacks are conducted via email.[4] What's in your inbox?

[3] Adam Kavon Ghazi-Therani and Henry N. Pontell
https://www.utica.edu/academic/institutes/cimip/Phishing_Evolves_Analyzing-the-Enduring-Cybercrime.pdf

[4] ibid

- **Spear phishing:** Rather than reaching hundreds of potential targets, these phishing schemes often focus on CEOs and other high-value targets. A cyber criminal may explore a CEO's social media profiles or other online information ahead of deploying the spear phishing bait. Data leaks and privacy abuses have created the potential for hackers to create detailed dossiers that lend credibility to their online trickery.

  Spear phishers often known an individual's name, place of employment, job title, email address, specific information about their professional role, and retain personal information about trusted colleagues, family members or other contacts. This enables criminals to create conniving and convincing spear phishing lures.

- **Whaling:** Whaling attacks target senior management and others in similarly high-level positions. These attacks typically appear as messages that originate with the CEO. Whaling attacks are premised on the same intended objectives as other types of phishing attacks. They often leverage highly personalized content in closely crafted campaigns. From Q4 of 2019 through Q3 of 2020, 25% of businesses contended with a whaling attack. For mid-sized firms with more than 50 employees, the frequency of whaling attacks was even higher.

- **Vishing:** Think phishing, but via phone. Using emotional appeals, cyber criminals fabricate situations that convince callers to divulge information that they ordinarily would not share over the phone. A scammer, for example, could pose as a CEO or another executive, making the person on the receiving end feel as though it is his/her obligation to hand over the requested information.

- **Smishing:** The word 'smishing' derives from the words "SMS" and "Phishing." In a smishing scheme, cyber criminals send fraudulent text messages to unsuspecting victims.

- **Angler phishing:** This type of phishing involves the using fake social media accounts to impersonate the accounts belonging to real organizations. Fake account names and handles may be just a few letters off from authentic ones. Using fake accounts, cyber criminals can capitalize on users' tendencies to make customer complaints via social media. In pretending to respond to a complaint, cyber criminals can ask individuals to provide personal information. Alternatively, angler phishers may point people to malicious customer support pages.

- **Catfishing:** This involves the use of a fraudulently established personal profile on a social networking site, designed to help hackers achieve criminal gains.

- **Pharming attacks:** In a pharming attack, a fake website masquerades as a legitimate one. Users are then asked to enter personal details into forms or pop-ups on the fake website, or a URL may force a user to download malicious code. There are assorted variations on these types of attacks. The bottom line is that all are duplicitous.

> Phishing attacks prey on personal judgement, insecurities, and in some cases, negligence or incompetence.

## CEOS: COMMON PHISHING HOOKS

Understanding advanced phishing techniques can enable you to identify threats before they inflict harm. Many of the most effective phishing attacks lure victims by creating a false sense of urgency.

For example, an email may suggest an account's expiration, a potentially missed deal, or an email may state that recipients only have a certain amount of time in which to accomplish an activity, such as a wire transfer.

In the past, phishing emails were poorly worded and low-effort initiatives. In the age of advanced phishing threats, cyber criminals no longer trip over bad grammar. Amidst the wave of advanced baiting techniques, here's what to look for in emails:

- Take notice of words such as "update", "verify", "validate" and "click here". This language is designed to coax you into sharing personal details.
- Beware of attachments, especially those that end in .exe.
- Learn how to discern a legitimate URL from a specious one.
  - A legitimate URL should not begin with an IP address, which might look like 143.578.20. In addition, a legitimate URL typically ends in an organization's name (example: checkpoint.com), not checkpoint.com.securitysoftware.net.
  - Legitimate and secure URLs also begin with HTTPS at the beginning, not HTTP.
  - If in doubt, reach out to a colleague who may be able to assist you with an assessment.
- Closely observe emails pertaining to wire transfers.
  - Ensure that wire transfer numbers do indeed match those of an authentic supplier's account.
  - In the event that a wire transfer amount seems beyond the norm, pause ahead of taking further administrative action. Phone a friend, so to speak.
  - Is the individual asking you to download a document or upload personal information in connection with the wire transfer?

## C-SUITE EXECUTIVES: COMMON PHISHING HOOKS

Non-CEO C-suite leaders should keep an eye out for cyber criminal attempts to leverage the CEO's name for internal deception purposes. An email that looks as though it emanates from the CEO may attempt to coerce the COO into transferring funds. This type of fraud has affected over 12,000 victims across the world.[5] According to the FBI, the average company transfers and loses $120,000 this way. In the UK, this type of fraud (BBC) has been labeled a national security issue.[6]

## DEFENSE-IN-DEPTH:

Short of shrugging off email and social media use altogether, businesses cannot guarantee phishing-proof environments. The next best options? Read on to learn more.

Organizations should pursue defense-in-depth strategies. Defense-in-depth refers to the implementation and ownership of multiple layers of security to prevent attacks. The idea is that if one of the layers fails, another layer can help an organization avoid a full-scale breach. A strategic combination of user awareness initiatives, smaller safeguards and technical infrastructure can thwart phishers.

**User awareness:**

Train all staff regarding discernment of phishing, spear phishing and whaling attempts. In particular, organizations should train financial administrators not to pander to demands purely because they appear to emerge from the CEO's desk. This helps to avoid business compromise. "It is…unrealistic to expect every employee to spot a scam or make the right cybersecurity decision 100 percent of the time, especially during these uncertain times," says one CEO, but cyber awareness training can serve as a first-line defense.[7]

Research shows that cyber security awareness training for the entirety of an organization's employees easily justifies the investment. In many cases, online training costs are nearly nil; just a few dollars per participant.[8]

[5] What is the Cost of 'CEO Fraud' and Why has it Cost Companies $2B in 2 years?
https://www.beckershospitalreview.com/hospital-management-administration/what-is-ceo-fraud-and-why-has-it-cost-companies-2b-in-2-years.html?oly_enc_id=6844A7823212C7A

[6] Gordon Corera, Fraud Epidemic 'Is Now National Security Threat'
https://www.bbc.com/news/business-55769991

[7] The Most Dangerous Cyber Security Mistakes
https://www.hcamag.com/us/specialization/hr-technology/the-most-dangerous-cyber-security-mistakes/229498

[8] Laurence Pitt, Defending Your Budget: How to Show ROI of Cybersecurity Investments
https://www.securityweek.com/defending-your-budget-how-show-roi-cybersecurity-investments

### Simple safeguards with an outsized impact:

- **Multi-factor authentication.** Multi-factor authentication can guard against fraudulent application access. In the event that an employee experiences a cyber security compromise at the application layer, the multi-factor authentication can prevent total account compromise and/or takeover.
- **Password management.** After implementing multi-factor authentication, organizations may want to implement and enforce password management policies. You may want to have leaders and employees change passwords every 6 months, and you may want to consider prohibiting password reuse.
- **Wire transfer safeguards.** Consider requiring secondary and/or tertiary signatures on wire transfers. You may also want to implement phone-based verification for transactions over a certain amount, such as $10,000. While these process-adds can prove inconvenient, they're preferable alternatives to substantial monetary loss.
- **Domain name purchases.** Consider buying up domain names that represent variations on that of your organization's name. For example, if your domain name has the word "for" in its title, (ex. Charityforthechildren.org) seek out domain name variations that involve use of the number 4 (ex. Charity4thechildren.org or Charity4thechildren.net). Your IT team should be able to provide information about available domain names and associated fees.

### Technical infrastructure:

Despite their genuine utility, awareness training and simple safeguards are not enough alone to prevent phishing. Consider technical solutions that can block phishing websites and social engineering attacks before they reach users. A solution that protects users from all kinds of phishing attacks across all vectors is the ideal choice. Look for a solution that is supported by a robust threat intelligence network and artificial intelligence.

Solutions like Check Point's Harmony Browse offer secure, fast and private web browsing. Harmony Browse inspects all SSL traffic at the endpoint location without adding latency on re-routing traffic through a secure-web service. It also blocks access to phishing websites and prevents the reuse of corporate passwords.

For comprehensive mobile phone protection, consider Check Point Harmony Mobile, the market-leading threat defense solution for mobile devices. By securing devices across every vector, Harmony Mobile keeps data safe. Advanced capabilities can even prevent of never-before-seen phishing threats.

## In Conclusion:

CEO, COO, CRO, or server-room data center support? No matter who you are or where you work, advanced phishing threats can disrupt your workflow, damaging your organization's reputation and potentially costing millions in lost revenue and clean-up costs. Mitigate the threat through awareness and action.

Educate yourself, share insights with colleagues, start with simple phishing safeguards and ultimately implement powerful protection via technical anti-phishing infrastructure. For more information about the latest anti-phishing tools, reach out to your local Check Point Software sales representative.

For additional cyber security thought leadership insights, visit CyberTalk.org.

**Worldwide Headquarters**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

**www.checkpoint.com**