Social Engineering Attacks Targeting the HPH Sector

April 11, 2024

TLP:CLEAR, ID# *202404111300*

Agenda

- Background on Social Engineering
- Targeted Campaign in the Health Sector
- Case Study Outside the Health Sector
- Role of Artificial Intelligence (AI)
- Mitigations

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Bottom Line Up Front

- Phishing remains one of the most effective social engineering attacks used against healthcare organizations.
- Advancements in technology and AI are lowering the barrier to entry for cybercriminals and increasing the sophistication of social engineering attacks.
- A combination of technical and non-technical mitigations are essential in defending against social engineering attacks.

What is Social Engineering?

- Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.
- There are various techniques used to conduct social engineering, and attackers continuously evolve these techniques to improve their successfulness.
- There are various types of targets of social engineering, such as employees, customers, and vendors.
- The goals of social engineering are broad, and may include obtaining sensitive information, gaining unauthorized access, disrupting operations, or committing fraud.

Image source: Tripwire

Types of Social Engineering Attacks

- **Phishing** leverages email, phone, SMS, social media or other forms of personal communication to entice users to click a malicious link, download infected files, or reveal personal information, such as passwords and account numbers. Note: Phishing attempts may also occur via physical postal mail.
- **Whaling** is a highly targeted phishing attack aimed at senior executives. Whaling often encourages victims to perform a secondary action, such as initiating a wire transfer of funds.
- **Baiting** is when scammers make false promises to users to lure them into revealing personal information or installing malware. Example: North Korean Operation Dream Job.

Example of Baiting

Early 2020: Operation Dream Job
(North Korean Cyber Espionage)

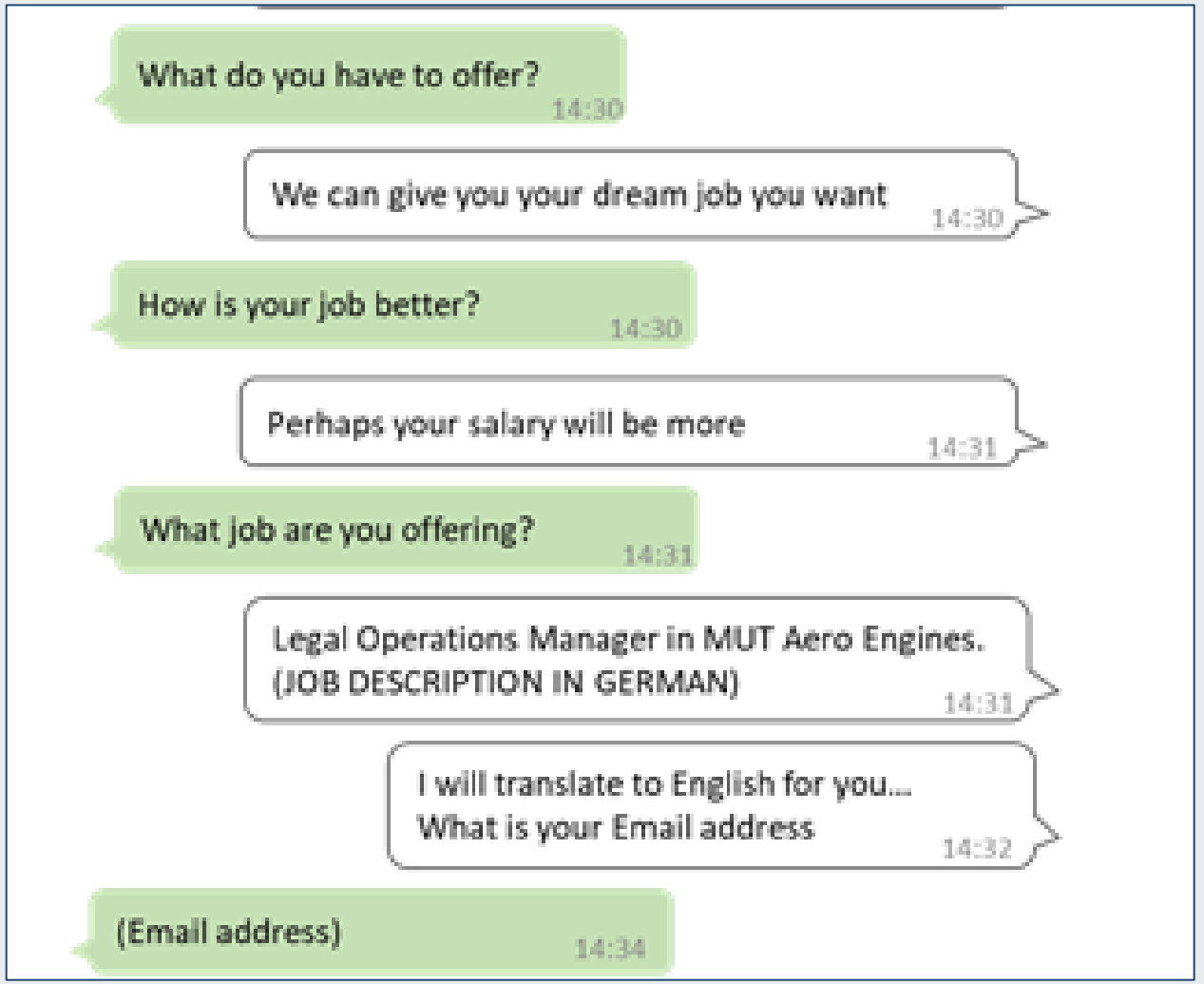


Image source: ClearSky Cyber Security

Types of Social Engineering Attacks, cont.

- **Quid pro quo**: The attacker requests sensitive information from the victim in exchange for a desirable service, i.e. fake tech support.
- **Pretexting**: A form of social engineering that involves composing plausible scenarios, or pretext, that are likely to convince victims to share valuable and sensitive data. Examples include romance or pig-butchering scams (obtaining fraudulent funds through manipulative means).
- **Smishing / SMS-phishing**: A social engineering attack conducted specifically through SMS messages where scammers attempt to lure the user into clicking on a link, which directs them to a malicious site and downloads malicious software and content.
- **Vishing**: Short for voice phishing, uses phone calls to trick victims into providing sensitive information.

Example of Vishing

March 2024: Phone Refund Scam

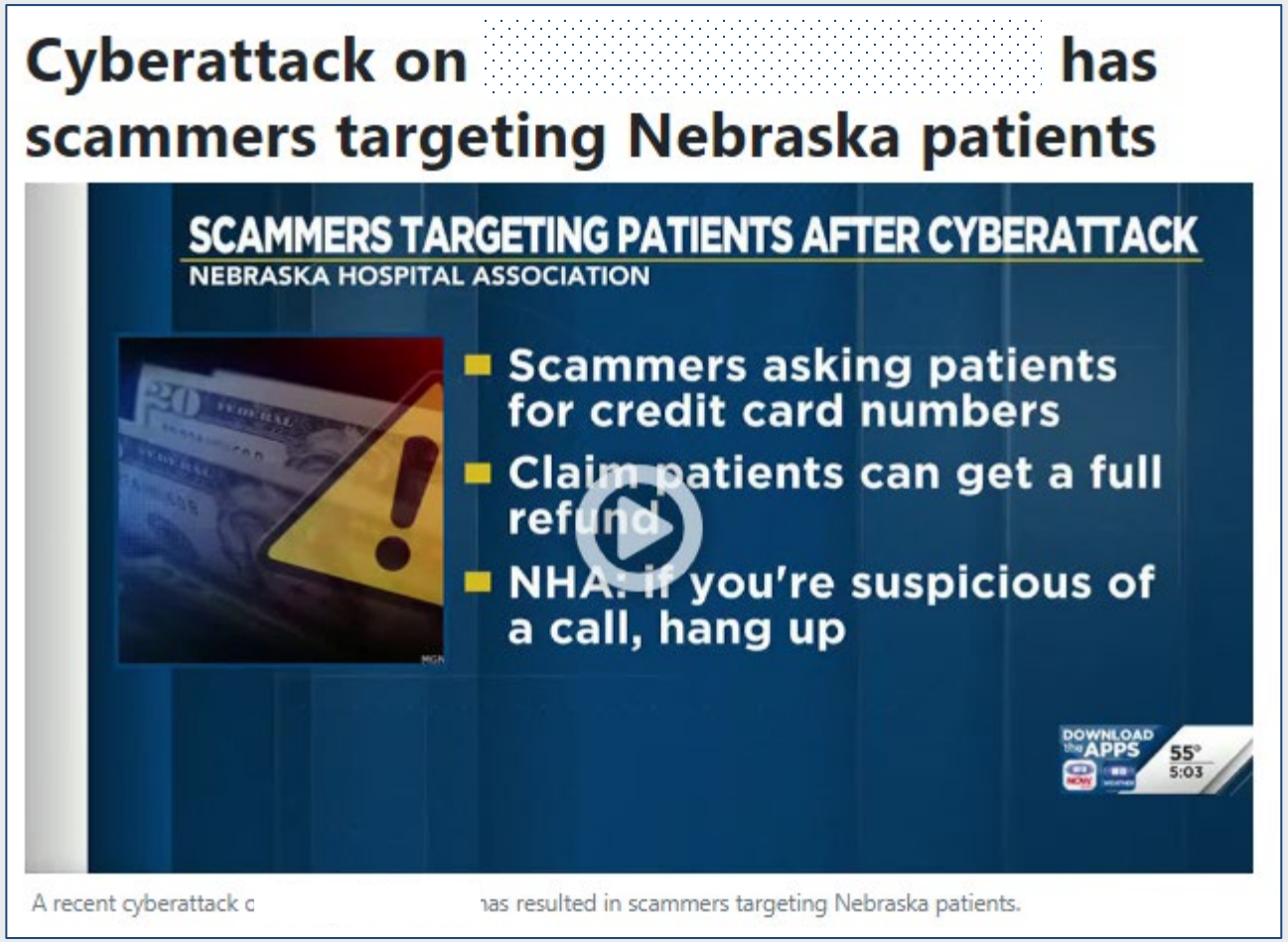


Image source: 10/11 NOW local news

Telephone-Oriented Attack Delivery (TOAD)

- Telephone-Oriented Attack Delivery (TOAD) lures potential victims to contact fraudulent call centers managed by threat actors in attempts to steal credentials or install malware onto their systems.
- TOAD moves the attack channel from an initial email to the telephone. Emails initiating TOAD attacks often do not contain URLs or attachments, which makes them difficult to detect.
- Often leverage a Norton, Paypal, or McAfee subscription themed lure with details of supposed bill (call to cancel).
- BazaCall campaigns tricking users into downloading BazaLoader malware were observed leveraging a new technique with Google Forms in December 2023 to bypass secure email gateways.

Example of TOAD Phishing Email

August 2023

[EXT] Payment for order no. 63014611 is approved

Customer Care Team <customercaretea... Monday, August 28, 2023 at 7:09 AM

To:

CAUTION: This email is external. Do not click links or attachments that are unexpected or from unknown senders. If unsure, click the Report Phishing Button in Outlook.

2023-08-28
Order Number:- 597G24SZ
Support:- +1(888) 864-1634

Order Summary

Dear Valid User,
Thank you for using Membership & Webroot Advanced Threat Protection. Tonight, your purchase details are set to renew automatically, and the corresponding amount will be deducted from your account. This email is in regards that you have an reactive membership with us, which is going to be renewed on 2023-08-28.

ITEM DESCRIPTION:
Client UID:- G24SZ597
Item:- AntiVirus Tech Support
Quantity: - 1
Tenure: - 5 Years
Payment Mode: - Confirmed
Charged Amount:- $424.24

To avoid future charges, reach out to us at our customer care before today to cancel our services. Alternatively, we encourage you to consider renewing your membership and remain a valued member of our community. Your satisfaction is our utmost priority, and we're here to assist you in any way we can.

+1(888) 864-1634

Image source: Proofpoint

TOAD Attack Sequence

Overview of a typical TOAD attack sequence for malware

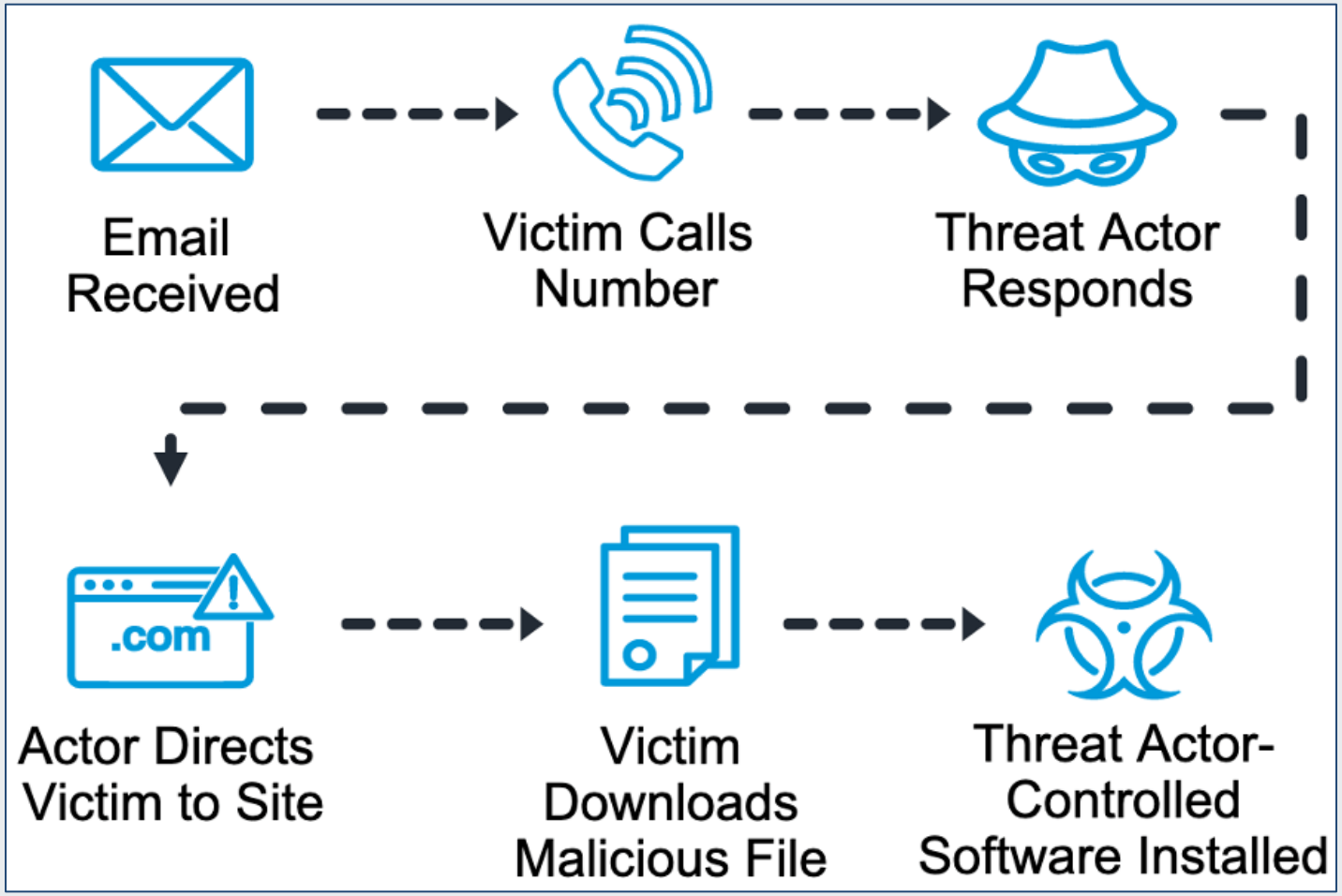
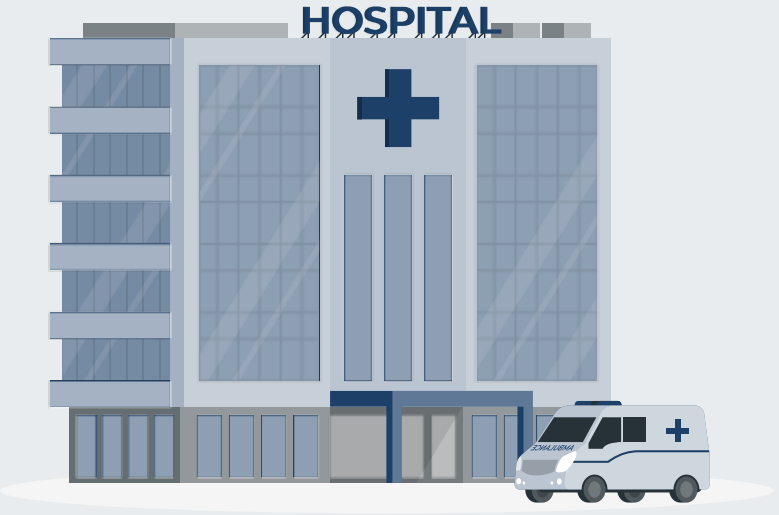


Image source: Proofpoint

State of Phishing in Healthcare

- In 2023, an average of 1.99 healthcare data breaches of 500 or more records were reported each day, and an average of 364,571 healthcare records were breached every day.
- In 2023, Cofense saw an increase in tactics like vishing, smishing, brand impersonation, and QR code phishing that bypass Secure Email Gateways (SEGs).
- Healthcare and finance remained the top targeted industries, with increases in malicious emails bypassing SEGs in those industries at 84.5% and 118%, respectively.
- In 2023, OCR announced its first-ever settlement resulting from an investigation of a phishing attack at a medical group, following a response to a phishing email that spoofed one of the medical group's owners.



Targeted Campaign in the Health Sector

Late Q3 2023

Social Engineering IT Help Desks

- Multiple sophisticated social engineering attacks by financially-motivated threat actors in the late third quarter of 2023 targeted IT help desk employees via phone calls originating from an area code local to the targeted healthcare organizations, with an end goal of conducting payment fraud scams.
- The threat actor (TA) claimed that their phone was broken and could not log in to receive MFA tokens, convincing IT help desks to enroll a new device to gain access to corporate resources.
- After gaining access, the TA targeted login information related to payer websites, where they then submitted a form to make ACH changes for payer accounts and divert legitimate payments to attacker-controlled U.S. bank accounts, which were then transferred to overseas accounts.

Spear Phishing Voice (T1566.004)

Key MITRE ATT&CK Technique

- Spearphishing voice (T1566.004) is a specific variant of spear phishing. It is different from other forms of spear phishing in that it manipulates a user into providing access to systems through a phone call or other forms of voice communications.
- Spear phishing frequently involves social engineering techniques, such as posing as a trusted source (ex: impersonation) and/or creating a sense of urgency or alarm for the recipient.
- May also combine voice phishing with MFA Request Generation.

Phone Call Spoofing

How are attackers spoofing phone calls to appear to originate from a trusted or local caller?

- Voice over Internet Protocol (VoIP)
- Spoofing services
- Orange boxing
- SIM swapping

MFA Bypass Techniques

How are attackers bypassing MFA?

- SIM swapping
- Adversary-in-the-middle (AITM)
- MFA prompt bombing
- Token theft
- Vishing/smishing

Social Engineering IT Help Desks, cont.

- During the malicious campaign that social engineered the healthcare organization's IT help desk, the threat actor also registered a domain with a single letter variation of the target organization, a technique known as typosquatting.
- Typosquatting involves deliberately registering domains with misspelled names of well-known websites to lure unsuspecting visitors to alternative websites, typically for malicious purposes.
- Organizations may intentionally register similar domains to their own to deter adversaries from creating typosquatting domains. (T1583.001)

Typosquatting Techniques

Typosquatting involves registering domains with deliberately misspelled names of well-known websites. Hackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes.

Common typosquatting techniques include:

- Dropping the dot after ‘www’. (Example: wwwaa.com)
- Dropping one letter. (Example: apple.om)
- Switching two letters. (Example: faecbook.com)
- Doubling characters. (Example: twiiter.com)
- Using similar-looking characters. (Example: google.com, with a capital ‘i’ instead of a lowercase ‘l’)
- Pressing a wrong key. (Example: costko.com)

Relevant Case Study from the Gambling Industry

September 2023

Scattered Spider, AKA UNC3944

- UNC3944 is a financially motivated threat cluster that has persistently used phone-based social engineering and SMS phishing campaigns (smishing) to obtain credentials to gain and escalate access to victim organizations.
- The group has targeted large companies and their contracted information technology (IT) help desks.
- Scattered Spider threat actors have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs.
- According to CISA, ALPHV Blackcat affiliates use advanced social engineering techniques and open-source research on a company to gain initial access. Actors pose as company IT and/or help desk staff and use phone calls or SMS messages to obtain credentials from employees to access the target network.

Scattered Spider, AKA UNC3944, cont.

- Previously performed social engineering by impersonating an employee from information found during reconnaissance on LinkedIn and calling the victim help desk to attempt to obtain password resets or multifactor bypass codes.
- During these calls, the threat actor provided verification information requested by the help desk employees, including usernames, employee IDs, and other types of personally identifiable information (PII) associated with employees.
- Notably, the threat actors often asked the service desk support to repeat the question and paused for significant lengths before answering, likely due to the threat actor looking through notes or attempting to search for the answer to the question posed.

Scattered Spider, AKA UNC3944 TTPs

Below are the MITRE ATT&CK techniques associated with social engineering for the threat actors Scattered Spider/UNC3944 and ALPHV Blackcat affiliates:

- **Phishing for Information, T1598:** ALPHV Blackcat affiliates pose as company IT and/or help desk staff using phone calls or SMS messages to obtain credentials from employees to access the target network.
- **Phishing, T1566:** Scattered Spider threat actors use broad phishing attempts against a target to obtain information used to gain initial access. Scattered Spider threat actors have posed as help desk personnel to direct employees to install commercial remote access tools.
- **Phishing (Mobile), T1660:** Scattered Spider threat actors send SMS messages, known as smishing, when targeting a victim.
- **Vishing, T1566.004:** Scattered Spider threat actors use voice communications to convince IT help desk personnel to reset passwords and/or MFA tokens.
- **Trusted Relationship, T1199:** Scattered Spider threat actors abuse trusted relationships of contracted IT help desks to gain access to targeted organizations.

Comparative Case Study

How do TTPs observed in targeted campaigns in the health sector compare to an incident in the gambling industry (UNC3944)?

- Credential theft malware leveraged by UNC3944
- Both employed phone-based social engineering for initial access
- Both impersonated employees after conducting reconnaissance
- At least one spoofed a local phone area code when calling the target
- At least one threat actor claimed phone was broken to bypass authentication
- Both leveraged typosquatting domains in phishing campaigns
- One involved ransomware deployment
- Use of AI tools remains unknown

Role of Artificial Intelligence (AI)

Vishing Skyrockets Post-ChatGPT

- Since the launch of ChatGPT in November 2022, vishing, smishing, and phishing attacks have increased by a staggering 1,265%.
- Research from Enea reveals that 76% of enterprises lack sufficient voice and messaging fraud protection, as AI-powered vishing and smishing skyrocket following the launch of ChatGPT.
- Advancements in technology and AI are lowering the barrier to entry for cybercriminals and increasing the sophistication of attacks.
- Generative AI tools like ChatGPT are predicted to play a role in crafting more effective cyberattacks in 2024, especially in the area of social engineering.

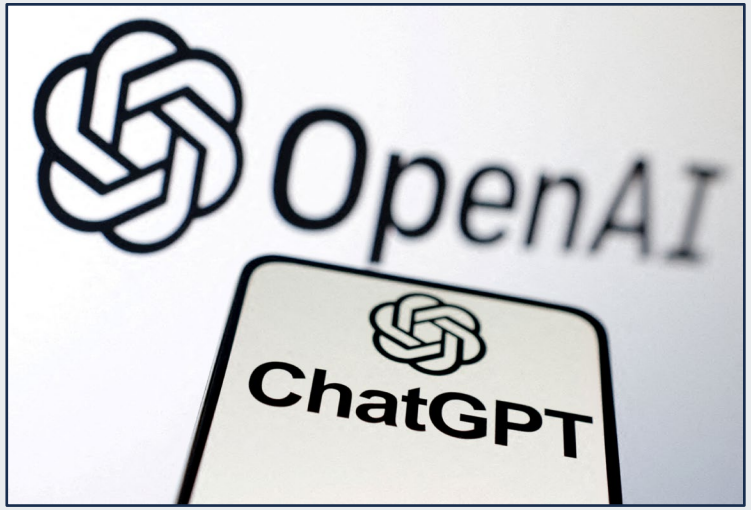


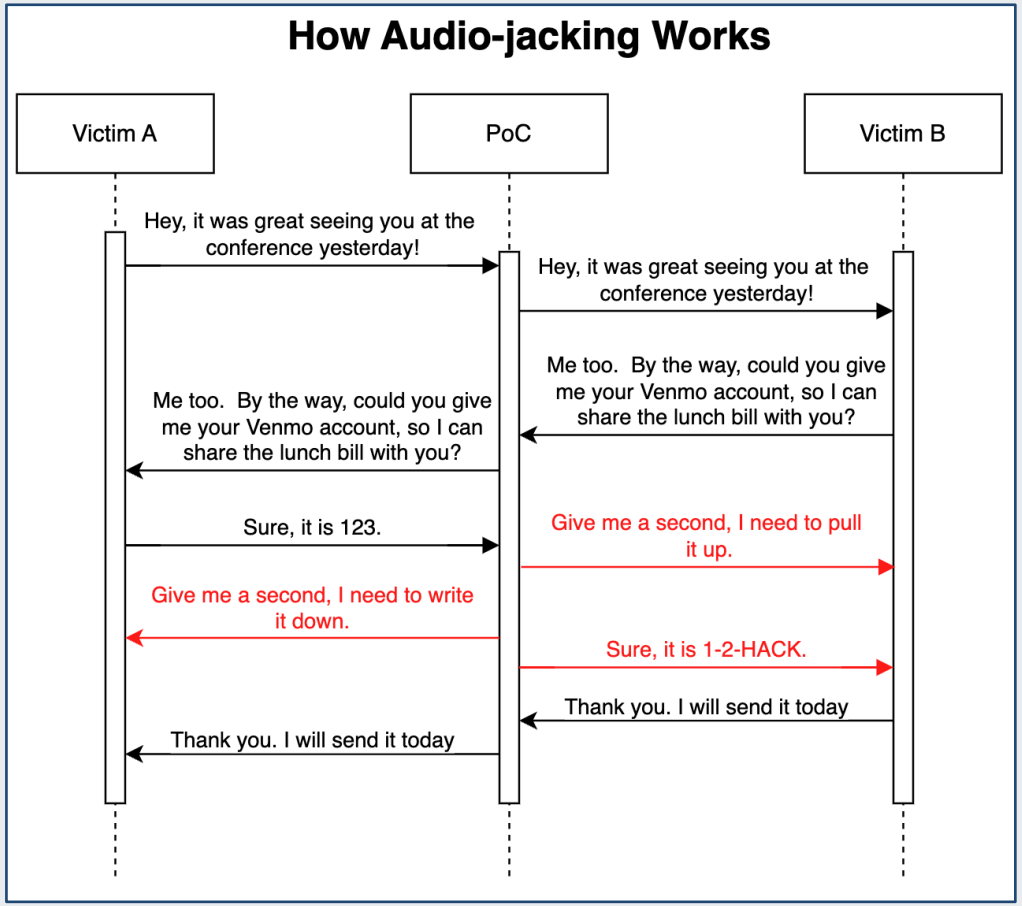
Image source: Reuters

AI Deepfake Video Call Scams

- In early 2024, scammers used artificial intelligence-powered “deepfakes” to pose as a multinational company’s chief financial officer in a video call and were able to trick an employee into sending them more than $25 million, CNN reported.
- The scam began with a phishing email that was initially deemed somewhat suspicious, but the deepfake video call bolstered the threat actors’ credibility and convinced the finance employee to transfer money to an offshore account.
- Likely sophisticated organized criminal organizations consisting of multiple individuals, supporting various roles throughout the duration of the scam.

Malicious LLMs for Social Engineering

- February 2024 saw research published by IBM on using generative AI to distort live audio transactions.
- Successful attempts to intercept and “hijack” a live conversation, using Live Language Models (LLM) to understand the conversation and manipulate the audio output unbeknownst to the speakers for a malicious purpose.
- The attack would require malware installed on the victims’ phones, or a malicious or compromised Voice over IP (VoIP) service.
- Presents the possibility of modifying medical information in phone conversations.



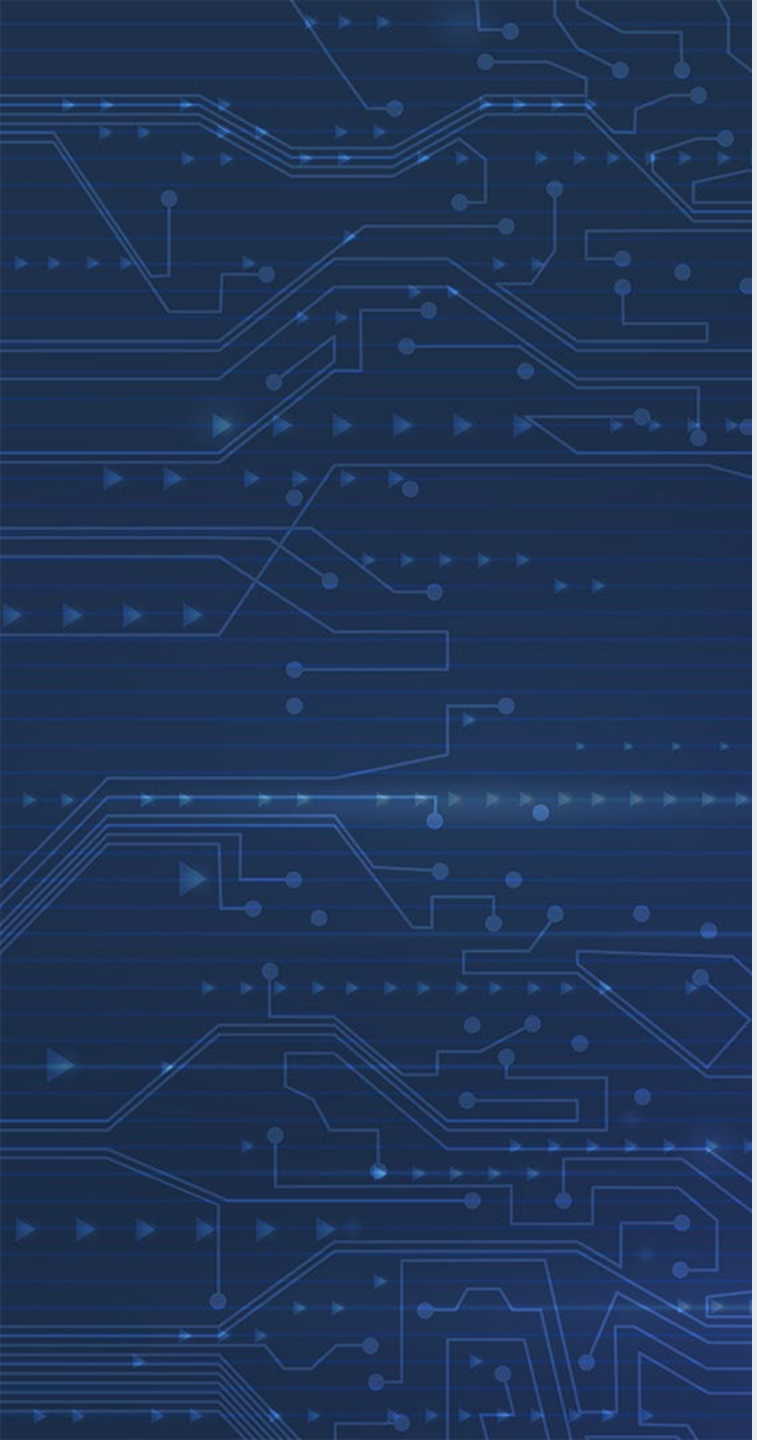
Source: IBM X-Force

Malicious LLMs for Social Engineering, cont.

- **WormGPT**: Launched in 2021 and has been used extensively in business email compromise (BEC) attacks; writes convincing phishing emails.
- **FraudGPT**: Active since July 2023, and can create phishing pages, phishing emails, and phishing SMSs, among other capabilities.
- **WolfGPT**: Active since July 2023 and primarily focuses on supporting code and exploit development but may also be used for advanced phishing attacks.

State-Sponsored Use of AI and LLMs

- In February 2024, Microsoft and OpenAI partnered to publish a report about nation-state threat actors linked with China, Iran, North Korea, and Russia experimenting with artificial intelligence (AI) and large language models (LLMs) to enhance their cyberattacks.
- Multiple state-sponsored threat actors have used OpenAI's services to generate content likely for use in phishing and spear phishing campaigns, including Charcoal Typhoon (China), Crimson Sandstorm (Iran), and Emerald Sleet (North Korea).
- They use LLM-supported social engineering tactics and use LLMs for assistance with drafting and generating content likely used in spear phishing campaigns. They generate various phishing emails, and leverage LLMs for assistance with translations and communication, likely to establish connections or manipulate targets.



Mitigations

Mitigations for AI-based Vishing

- Paraphrase and repeat the dialogue during a phone conversation where sensitive information is being discussed if suspicious, to ensure accuracy.
- Consider using a “code word” that only your family or organization knows to verify the identity of the caller, if there is a suspicion of impersonation.
- Regular vishing exercises to assess an organization’s defenses against voice phishing attacks that simulate realistic scenarios.

Mitigations

- **ID:** M1017
- **Mitigation:** User Training
- **Description:** Users can be trained to identify and report social engineering techniques and spear phishing attempts, while also being suspicious of and verifying the identify of callers.

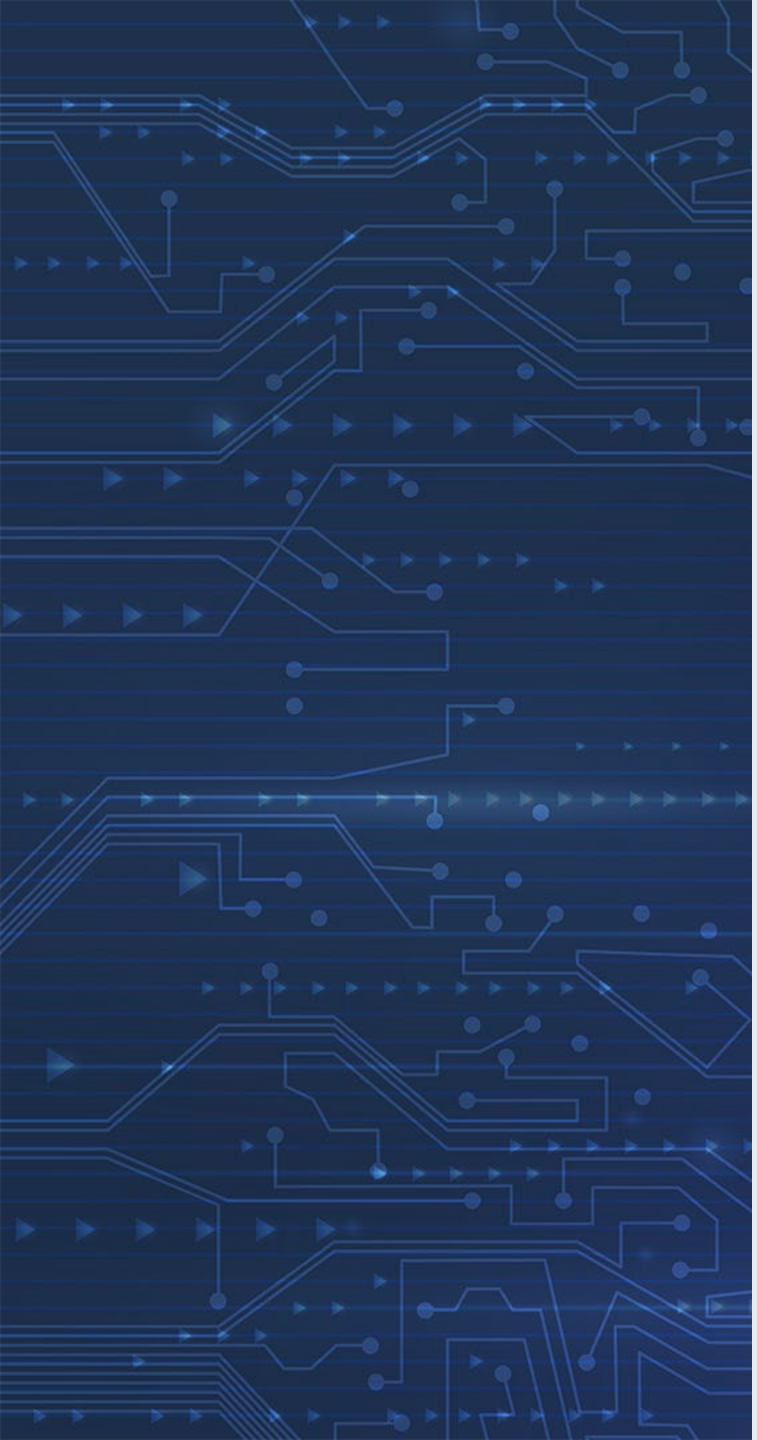
Detections

- **ID:** DS0015
- **Data Source:** Application Log
- **Data Component:** Application Log Content
- **Detects:** Monitor call logs from corporate devices to identify patterns of potential voice phishing, such as calls to/from known malicious phone numbers. Correlate these records with system events.

Relevant HC3 Products

Relevant HC3 Products

- April 3, 2024 - Social Engineering Attacks Targeting IT Help Desks in the Health Sector
- October 26, 2023 - AI and Phishing as a Threat to the HPH White Paper
- October 23, 2023 - QR Codes and Phishing as a Threat to the HPH White Paper
- July 13, 2023 - AI, Cybersecurity and the Health Sector
- January 17, 2023 - AI for Malware Development Analyst Note
- August 19, 2022 - Vishing Attacks on the HPH Sector Analyst Note
- August 18, 2022 - The Impact of Social Engineering On Healthcare



Conclusion

Major Takeaways

- Various threat actors, from low-level scammers to state-sponsored cyber actors, may conduct social engineering attacks to compromise individuals and organizations in the HPH sector.
- User awareness and cybersecurity policies remain some of the most important steps toward mitigating social engineering attacks.
- HC3 assesses with high confidence that threat actors will continue to exploit major events to tailor their social engineering campaigns to increase success rates.

Reference Materials

References

- Lenaerts-Bergmans, Bart. “10 Types of Social Engineering Attacks and How to Prevent Them,” CrowdStrike. November 8, 2023. https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/
- Tripwire. “Social Engineering: Definition & 6 Attack Types,” March 1, 2023. https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for
- KnowBe4. “What is Social Engineering?,” https://www.knowbe4.com/what-is-social-engineering/
- New Jersey Cybersecurity & Communications Integration Cell (NJCCIC). “Garden State Cyber Threat Highlight: Increase in TOAD Attacks,” NJCCIC. February 2, 2023. https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/increase-in-toad-attacks
- Kaspersky. “What is Typosquatting? – Definition and Explanation.” https://usa.kaspersky.com/resource-center/definitions/what-is-typosquatting

- UK National Cyber Security Centre. “Whaling: how it works, and what your organisation can do about it.” Published October 6, 2016. Reviewed August 22, 2020. https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it
- Smith, John. “8 Strategies for Defending Against Help Desk Attacks.” Dark Reading. December 21, 2023. https://www.darkreading.com/cyberattacks-data-breaches/8-strategies-defending-against-help-desk-attacks
- The Hacker News. “4 Ways Hackers use Social Engineering to Bypass MFA.” February 12, 2024. https://thehackernews.com/2024/02/4-ways-hackers-use-social-engineering.html
- Dave Cook and Tyler Johnson. “Cybersecurity Stop of the Month: Attack Sequence of TOAD Threats.” Proofpoint. November 1, 2023. https://www.proofpoint.com/us/blog/email-and-cloud-threats/cybersecurity-stop-month-attack-sequence-toad-threats

- Microsoft Threat Intelligence. “Staying ahead of threat actors in the age of AI,” February 14, 2024. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
- OpenAI. “Disrupting malicious uses of AI by state-affiliated threat actors.” February 14, 2024. https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors
- Cantos, Michelle, Sam Riddell, and Alice Revelli. “Threat Actors are Interested in Generative AI, but Use Remains Limited,” Mandiant Blog. August 17, 2023. https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited
- Heather Chen and Kathleen Magramo. “Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’” CNN. February 4, 2024. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
- Lee, Chenta. “Audio-jacking: Using generative AI to distort live audio transactions.” IBM. February 1, 2024. https://securityintelligence.com/posts/using-generative-ai-distort-live-audio-transactions/

- Erzberger, Arhur. “WormGPT and FraudGPT – The Rise of Malicious LLMs.” Trustwave. August 8, 2023. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/wormgpt-and-fraudgpt-the-rise-of-malicious-llms/
- ThriveDX. “Investigating the MGM Cyberattack – How social engineering and a help desk put the whole strip at risk.” October 6, 2023. https://thrivedx.com/resources/article/investigating-the-mgm-cyberattackhow-social-engineering-and-a-help-desk-put-the-whole-strip-at-risk
- Ragan, Steve. “Why help desk employees are a social engineer’s favorite target.” July 17, 2013. https://www.csoonline.com/article/539410/social-engineering-why-help-desk-employees-are-a-socialengineer-s-favorite-target.html
- Jones, David. “MGM, Caesars attacks raise new concerns about social engineering tactics.” September 18, 2023. https://www.cybersecuritydive.com/news/mgm-caesars-attacks-social-engineering/693956/

- American Hospital Association. “Hospital IT help desks targeted by sophisticated social engineering schemes.” January 12, 2024. https://www.aha.org/news/headline/2024-01-12-hospital-it-help-deskstargeted-sophisticated-social-engineering-schemes
- Service Desk Institute. “Protecting the IT Service Desk from Social Engineering Attacks.” February 27, 2023. https://www.servicedeskinstitute.com/protecting-the-it-service-desk-from-social-engineeringattacks/
- Mandiant Intelligence. “Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety.” September 15, 2023. https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware
- Alder, Steve. “Hospital IT Help Desks Targeted in Sophisticated Payment Fraud Scam.” https://www.hipaajournal.com/hospital-it-help-desk-scam/

Questions

FAQ

Upcoming Briefing

- May 16, 2024 – Business Email Compromises in the HPH Sector

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV