CDE #73788

PHISHING

THE REEL THREAT TO EMERGENCY COMMUNICATIONS

A primer for understanding and guarding against a pervasive online danger.

By Megan Bixler

The Cybersecurity and Infrastructure Security Agency (CISA) states that 90% of successful cyberattacks start with a phishing email.[1] But what exactly is phishing? According to the National Institute of Standards and Technology (NIST),[2] "Phishing is the use of convincing emails or other messages to trick us into opening harmful links or downloading malicious software. These messages are often disguised as a trusted source, such as your bank, credit card company or even a leader within your own business."

In the late 1960s, the first concept for what is now known as the internet was made, called the Advanced Research Projects Agency Network (ARPANET), a technology developed by the U.S. government. Fast forward to the 1990s, the internet is becoming commercially available mostly through internet access providers. The number one internet access provider at the time was America Online (AOL). AOL mailed free software (via CDs), and users paid per hour for internet usage. The first major phishing attack happened in the 1990s initiated by hackers stealing user credentials and creating fake credit card numbers. The fake credit card numbers were used to create other AOL accounts that were used to scam AOL users through AOL Instant Messenger and email systems. This became such a big problem that AOL warned users against providing sensitive information in the AOL Instant Messenger and email. Since this initial campaign, phishing has become a major threat to any user on the internet. The word "phishing" is a homophone of "fishing," indicating the idea of luring victims with bait. The use of "ph" instead of "f" is thought to be influenced by the term "phreaking," which described the practice of proto hackers obtaining free long-distance phone calls.

In 2025, phishing is still deemed a successful cyberattack technique. It is estimated that 90% of all successful cyberattacks start with a phishing email.[3] It is also estimated that 1-4% of all global email traffic is considered phishing.[4] There is no arguing that phishing is successful, which provides positive feedback for cyber threat actors to continue to try to gain access to emergency communications center (ECC) systems through this method. To guard against a phishing attack, ECC employees should understand the various types of attacks and the best ways to mitigate the effect on 9-1-1 operations.

TYPES OF PHISHING ATTACKS

Since the initial AOL phishing campaign, the practice has become more sophisticated. With this sophistication, various phishing attack methods have been categorized:[5]

- Email phishing: The most common type of phishing, where attackers send fraudulent emails that appear to be from reputable sources. These emails often contain malicious links or attachments.
- Spear phishing: A targeted form of phishing where attackers customize their messages to a specific individual or organization. Spear phishing emails are often more convincing because they use personal information to appear legitimate.
- Whaling: A type of spear phishing that targets high-profile individuals, such as executives or senior officials. Whaling attacks often involve more sophisticated tactics and higher stakes.
- Smishing (SMS phishing): Phishing attacks conducted via SMS text messages. These messages typically contain a link or phone number that directs the recipient to a fraudulent website or prompts them to provide personal information.
- Vishing (voice phishing): Attacks conducted by phone, using social engineering techniques to trick victims into revealing personal information or transferring money.
- Clone phishing: Attackers create a nearly identical copy of a legitimate email that the victim has previously received but replace the links or attachments with malicious ones. The cloned email appears to come from a trusted source.
- Pharming: Attackers redirect users from legitimate websites to fraudulent ones without their knowledge. This is often achieved through DNS poisoning or other methods.

- Angler phishing: Attacks conducted via social media platforms. Attackers create fake profiles or hijack existing ones to lure victims into clicking malicious links or providing personal information.
- QR code phishing: Fraudulent QR codes direct victims to malicious websites. Attackers place the fraudulent QR codes in public places or send them via email or text messages.
- Pop-up phishing: Pop-up windows appear on legitimate websites that are designed to trick users into entering personal information or downloading malware.
- Search engine phishing: Attackers create malicious websites that appear in search engine results. These sites are designed to look like legitimate businesses or services.
- Watering hole phishing: Attackers compromise websites that are frequently visited by a specific group of users. When users visit these sites, they are redirected to malicious sites or prompted to download malware.
- Tabnabbing: Attackers manipulate inactive browser tabs to redirect users to phishing sites when they return to the tab.

PHISHING MITIGATION STRATEGIES

In 2023, CISA collaborated with the National Security Agency (NSA), the FBI, and the Multi-State Information Sharing and Analysis Center (MS ISAC) to develop "Phishing Guidance: Stopping the Attack Cycle at Phase One."[6] This guide outlines mitigation techniques to help organizations prevent and respond to phishing attacks. The key recommendations are:

1. **Technical mitigations.** To effectively combat phishing threats, CISA recommends a range of technical mitigations that organizations should implement as part of a layered defense strategy. One of the foundational steps is deploying robust email filtering systems that can detect and block messages from known malicious domains and IP addresses. These filters help prevent phishing emails from ever reaching users' inboxes. Complementing this, firewall rules should be configured to restrict outbound connections to suspicious or known malicious infrastructure, thereby limiting the ability of malware to communicate with command-and-control servers. Multi-factor authentication (MFA) is another critical control, as it significantly reduces the risk posed by compromised credentials by requiring an additional verification step beyond just a password. Organizations are encouraged to use endpoint detection and response (EDR) tools, which provide real-time monitoring and automated responses to suspicious activity on user devices. Uniform resource locator (URL) filtering should be employed to block access to phishing websites and other harmful online destinations, further reducing the likelihood of successful attacks. Together these technical measures form a strong defense against the initial stages of phishing campaigns.
2. **Secure-by-design and secure-by-default practices.** CISA recommends adopting secure-by-design and secure-by-default principles to reduce the risk of phishing and other cyber threats at the source. Secure-by-design means that software manufacturers should integrate security features and considerations into the earliest stages of product development rather than treating them as optional add-ons. This approach ensures that security is a foundational element of the product, not an afterthought. Secure-by-default refers to configuring products to prioritize safety and minimize risk right out of the box. This includes enabling strong security settings by default, reducing unnecessary features that could introduce vulnerabilities and simplifying secure configurations for users. By embracing these principles, ECCs can help create a safer digital ecosystem where ECC employees are less exposed to threats like phishing, even if they lack advanced cybersecurity expertise.
3. **User education.** Educating users is a critical component of any phishing defense strategy. CISA recommends ongoing awareness programs that help individuals recognize and respond appropriately to phishing attempts. Training should focus on teaching users how to identify common signs of phishing, such as emails that impersonate trusted contacts, contain suspicious links or attachments, or use urgent or manipulative language to provoke a quick response. It's also important to foster a culture where users feel comfortable reporting suspicious messages without fear of reprimand. Regular phishing simulations can reinforce these lessons by providing practical, hands-on experience in spotting and avoiding phishing attempts. By equipping users with the knowledge and confidence to act as the first line of defense, organizations can significantly reduce the likelihood of successful phishing attacks.

   The educational requirements for ECCs emphasize cybersecurity awareness and preparedness. According to APCO's ANSI-accredited standard, Cybersecurity Training for Public Safety Communications Personnel (APCO ANS 3.110.1-2019), ECCs should dedicate four to eight hours annually to training employees on cybersecurity policies and procedures. This training should ensure that public safety telecommunicators understand the significance of cybersecurity awareness, can recognize the signs of a cyberattack and know the appropriate actions to take in response. APCO also offers specialized courses tailored to public safety professionals, including "Cybersecurity Fundamentals for the ECC," which covers the anatomy of cyberattacks and mitigation strategies, and "Intermediate Cybersecurity Principles for the ECC," designed for IT and supervisory staff to deepen their understanding of hacker tactics and network vulnerabilities.[7]
4. **Cyber incident response plan.** Having a well-developed and regularly tested cyber incident response plan is essential for minimizing the impact of phishing attacks. CISA advises that ECCs create detailed procedures that outline how to detect, contain and recover from phishing incidents. This includes clearly defining roles and responsibilities, establishing communication protocols and ensuring that all ECC employees understand the steps to take when a phishing attempt is suspected or confirmed. The plan should also include mechanisms for reporting incidents internally and externally, such as to cybersecurity authorities or affected stakeholders. Regular exercises and simulations help ensure the response team can act swiftly and effectively under pressure. By preparing in advance and practicing

their response, organizations can reduce downtime, limit data loss, and maintain trust with customers and partners in the event of a phishing-related breach. ●

***Megan Bixler, RPL, CPE**, is the Senior Technology Strategist for APCO International.*

REFERENCES

1. Cybersecurity & Infrastructure Security Agency. "Shields Up: Guidance for Families" www.cisa.gov/shields-guidance-families
2. National Institute of Standards and Technology. (n.d.). "Phishing." Retrieved April 28, 2025, from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing
3. Cybersecurity and Infrastructure Security Agency. "4 things you can do to keep yourself cyber safe." December 18, 2022. www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe
4. Proofpoint. "2024 State of the Phish Report: Phishing Statistics & Trends." 2024 www.proofpoint.com/us/resources/threat-reports/state-of-phish
5. U.S. Department of State. (n.d.). "Understanding and Preventing Phishing Attacks." www.state.gov/understanding-and-preventing-phishing-attacks
6. Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, Multi-State Information Sharing and Analysis Center. "Phishing Guidance: Stopping the Attack Cycle at Phase One." October 2023. www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf
7. Bixler, Megan. "Cyber Threat Prep." Public Safety Communications Magazine. September/October 2023. www.pscmagazine-digital.com/pscs/0523_september_october_2023/MobilePagedArticle.action?articleId=1914949

CDE EXAM #73788

1. Phishing is so obvious that less than 10% of cyberattacks are successful.
   a. True
   b. False

2. The most common type of phishing is:
   a. Watering hole phishing
   b. Email phishing
   c. Whaling
   d. Clone phishing

3. Smishing occurs via:
   a. Social media
   b. SMS messages
   c. Phone calls
   d. QR codes

4. Multi-factor authentication (MFA) is important because:
   a. It significantly reduces the risk posed by compromised credentials by requiring an additional verification step beyond just a password.
   b. Your agency can restrict you from logging in outside of your normal work hours.
   c. It timestamps when you log in.
   d. It's required to always carry your phone with you so your agency can get ahold of you when they need to.

5. By equipping users with the knowledge and confidence to act as the first line of defense, organizations can significantly _____ the likelihood of successful phishing attacks.
   a. Increase
   b. Maintain
   c. Reduce
   d. Eliminate

6. What does NIST stand for?
   a. No Incoming Smishing Threats
   b. Never Include Secure Technology
   c. National Incoming Service Telecommunications
   d. National Institute of Standards and Technology

7. The forerunner of the internet, the Advanced Research Projects Agency Network (ARPANET), was conceived in _____.
   a. The 1980s
   b. The late 1960s
   c. 2023
   d. 2001

8. The word "phishing" is a homophone of "fishing," indicating the idea of luring victims with _____.
   a. Free stuff
   b. Shiny pictures
   c. Bait
   d. Tangled lines

9. AOL was the most sophisticated phishing campaign.
   a. True
   b. False

10. Tabnabbing is when:
   a. Attackers manipulate inactive browser tabs to redirect users to phishing sites when they return to the tab.
   b. You leave your phone or laptop unattended and someone hacks in.
   c. You leave a restaurant without paying the tab.
   d. Cybercriminals keep tabs on which websites you're visiting.

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online! To receive a complimentary certificate of completion, you may take the CDE exam online. Go to https://www.training-apcointl.org/ to create your username and password. Enter CDE in the search box, and click on **"Phishing,"** then click on "enroll me" and choose **"Phishing (73788)"** to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.