Vishing Attacks on the Rise

Executive Summary
Voice phishing, also known as vishing, is the practice of eliciting information or attempting to influence action via the telephone. Over the past year, HC3 has noted a marked increase in these attacks across all sectors. Social engineering techniques continue to remain successful in providing initial access to target organizations, and the HPH sector should remain alert to this evolving threat landscape with an emphasis on user awareness training. Recently, a large U.S. company fell victim to a cyber attack that leveraged sophisticated phishing techniques involving phone calls to gain access to the victim organization.

Report
Phishing campaigns continue to be an effective way to gain unauthorized access to target networks by both cybercriminal and state-sponsored threat actors. According to security vendor Agari, the use of 'hybrid vishing' saw a massive 625% growth in Q2 2022. Hybrid vishing threats, also referred to as “callback phishing,” are multi-stage attacks that differ from traditional vishing by first interacting with the victim via email. The objectives of these attacks are usually to obtain sensitive information or distribute malware. Callback phishing attacks were first introduced by the 'BazarCall/BazaCall' campaigns that appeared in March 2021 to gain initial access to corporate networks for ransomware attacks.

In May 2022, a major U.S.-based telecommunications company suffered a cyber incident that relied on a series of sophisticated vishing attacks against an employee. The threat actor— which was identified as an initial access broker (IAB) with ties to the UNC2447 cybercrime gang (the Lapsus$ threat actor group) and the Yanluowang ransomware operators— gained access from a user that had enabled password syncing via Google Chrome and had stored their work credentials in their browser, enabling that information to synchronize to their Google account. After obtaining the user’s credentials, the attacker attempted to bypass multifactor authentication (MFA) using a variety of techniques, including vishing and MFA fatigue, which is the process of sending a high volume of push requests to the target’s mobile device until the user accepts, either accidentally or simply to attempt to silence the repeated push notifications they are receiving.

HC3 has previously observed numerous phishing campaigns in the HPH sector that leverage vishing techniques. For instance, in September 2020, threat actors posing as employees of a Michigan, U.S.-based health system carried out a vishing campaign that involved calling patients to steal their member numbers and protected health information (PHI). These fake phone calls even “spoofed” caller ID and appeared to be originating from a legitimate phone number belonging to the healthcare entity. Advanced Persistent Threat (APT) groups, or state-sponsored threat actors, are even known to use voice-changing software to successfully trick targets into installing malware.

Analyst Comment
HC3 assesses with high confidence that threat actors will continue to evolve their tactics, techniques, and procedures (TTPs) when conducting phishing attacks due to prior success in gaining initial access. Security researchers recently found a way to use just a series of emojis to deliver an exploit to a target. While this method requires specific circumstances to occur for the emoji exploit to work, this demonstrates the constantly evolving threat landscape and difficulty in detecting malware.
How to Identify Vishing/Phishing

- Suspicious emails claiming a free trial has ended for a service for which the recipient never signed.
- Unexpected emails containing only the name, address, and phone number of an unrecognized organization.
- Individuals asking callers to navigate to a website to cancel a subscription they did not sign up for.
- Emails from a Gmail account with the name of a high-level individual in medical research.
- Phone calls or emails pretending to be from a government entity, such as a Department of Health or major technology company.

Below is an example of a vishing campaign email. It includes email before the call, typically presenting the victim with a fake subscription/invoice notice. The recipient is advised to call the phone number listed to resolve any issues with the charge, but instead of a real customer support agent, the call is answered by phishing actors who then offer to resolve the problem by tricking the victim into disclosing sensitive information or installing remote desktop tools on their system. The threat actors may then install further backdoors or spread to other machines.

![Figure 1. Example of Email](image)

Mitigations

- User training and awareness of new phishing campaigns targeting the HPH sector.
- Confirm receipt of an email from a known sender via a trusted communication method or contact.
- Secure VoIP servers and look for evidence of existing compromise (such as web shells for persistence).
- Block malicious domains and other indicators associated with campaigns, such as those mentioned above.
- Stay up-to-date with the latest health-themed scams and fraud schemes i.e. COVID-19 and Monkeypox.
- Consider switching your organization’s MFA setting or configuration to require a one-time password (OTP) versus a push notification to mitigate MFA fatigue.
References


CyberArk Blog Team, “Don’t Fall for MFA Fatigue or Next-Level Phishing Attacks,” August 18, 2022. https://www.cyberark.com/resources/blog/don-t-fall-for-mfa-fatigue-or-next-level-phishing-attacks


Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback