Vishing and Deepfakes: The New Frontier of Cyber Threats

October 2025

Ilaria Sangalli, *Index Research Lead*

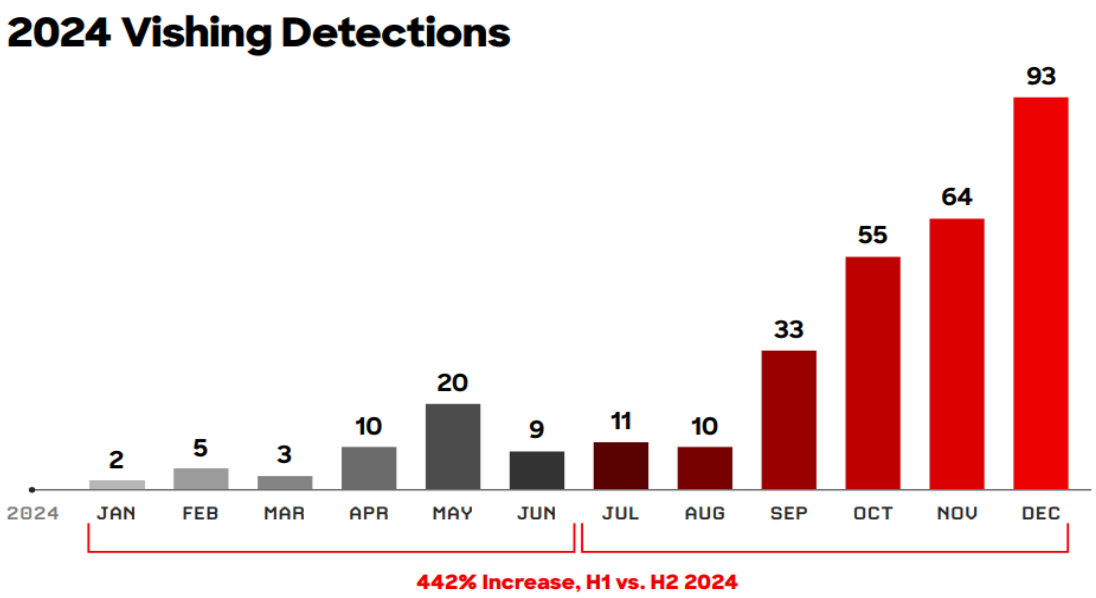
In today's digital landscape, the sophistication of cyber attackers is rapidly increasing, due in part to powerful tools like AI. However, it's not just their technical skills that are evolving. Cyber criminals are also becoming more theatrical and creative in their infiltration methods. This blend of technical and creative strategies makes cybersecurity a dynamic and ever-evolving field. Far from being boring, it requires a keen understanding of both technology and human behavior to stay one step ahead of the threats.

Why are cybercriminals becoming more creative? As cybersecurity defenses grow more sophisticated, especially with AI now forming the backbone of many systems, traditional system vulnerabilities are becoming harder to exploit. In response, cybercriminals are shifting their tactics by becoming more creative. Rather than targeting tightly secured systems, they are increasingly focusing on human vulnerabilities, which often remain the weakest aspect of security defenses.

One prevalent method cybercriminals are increasingly adopting is vishing, or voice phishing, which involves scammers making fraudulent phone calls to trick individuals into revealing sensitive information, downloading malware, or sending money.[1] What makes these scams even more dangerous is the use of AI technology, particularly deepfakes. Deepfake technology allows scammers to create realistic, but fake, audio and video, making their calls appear to come from trusted individuals or authorities. This added layer of realism can make it incredibly difficult for victims to detect the fraud.

According to CrowdStrike, vishing incidents surged by 442% between the first and second half of 2024.[2] A notable example of this trend is the recent AI-driven phone scam targeting prominent Italian business leaders, including Giorgio Armani and Patrizio Bertelli, Chair of Prada. Fraudsters impersonated Italy's Defence Minister, Guido Crosetto, to trick victims into transferring money for a fake ransom. The scammers claimed the funds were needed to release kidnapped journalists in the Middle East, and demanded €1 million to be sent to a Hong Kong bank account. Despite the warning, one entrepreneur had already transferred the money, believing he had spoken to Crosetto directly.[3]

[1] https://www.ibm.com/think/insights/rise-of-vishing
[2] https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0
[3] https://www.theguardian.com/world/2025/feb/10/ai-phone-scam-targets-italian-business-leaders-including-giorgio-armani



Source: Crodwstrike 2025 Global Threat Report. Vishing instructions detected by Crowdstrike OverWatch per month, 2024

As another real example, in 2024, Europol successfully dismantled a sophisticated phone phishing gang operating across multiple countries. The operation, which began in 2022, culminated in a series of coordinated arrests and raids in Belgium and the Netherlands. The gang employed phone-based phishing techniques, impersonating banking officials and police officers to deceive victims, primarily targeting the elderly. According to Europol, the gang defrauded victims in at least 10 European countries, stealing millions of euros.[4]

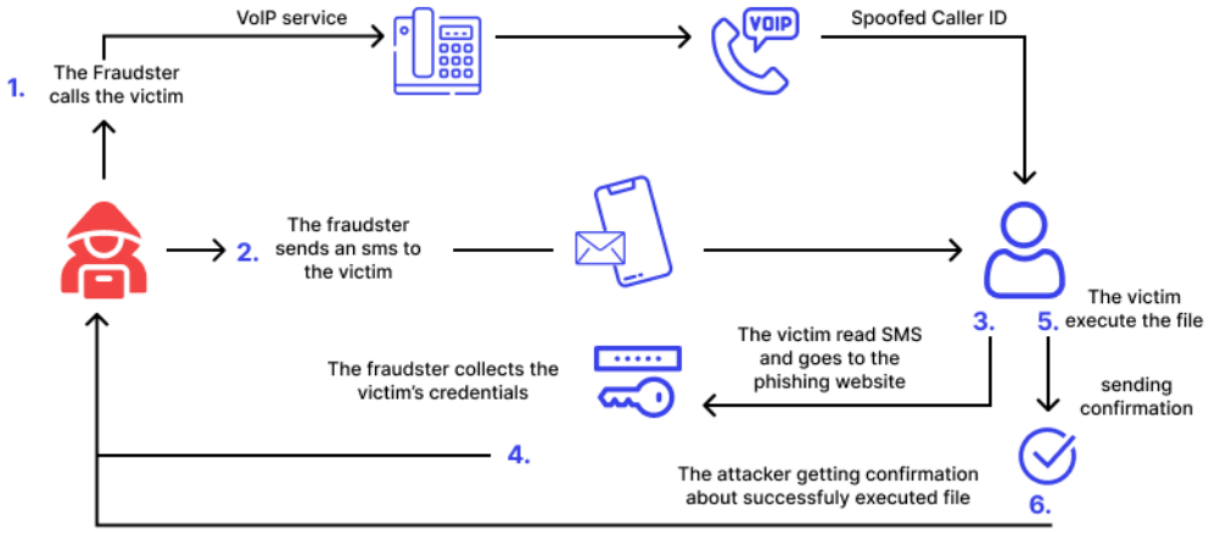
To better understand how these scams unfold, it is helpful to look at the typical process behind a vishing attack. The first step involves bulk dialing, where attackers use automated systems to call large volumes of phone numbers simultaneously, hoping to connect with a few potential victims. A VoIP (Voice over Internet Protocol) service is typically used, and the caller ID is spoofed to make it appear as if the call is coming from a legitimate source. Once connected, the attacker pretends to be an authorized representative from a reputable organization. They then create a scenario that requires immediate action, such as claiming the victim is eligible for a tax return or will face penalties if they don't comply. In this way, victims are pressured into providing sensitive information like account details, passwords, or PINs.

In other cases, vishing attacks may incorporate elements of smishing (SMS phishing) and phishing (web-based phishing). The attacker starts by calling the victim using a VoIP service. They then send an SMS to the victim, directing them to a phishing website. The victim visits the site and enters their credentials, which the attacker collects. Finally, the victim may be tricked into executing a file, granting the attacker further access.[5]

In March 2024, the Federal Trade Commission (FTC) issued a warning about a widespread scam involving fraudulent calls and text messages claiming to be from Amazon. Scammers used caller ID spoofing to make it appear as though the messages were legitimate. They often told convincing stories about suspicious

[4] https://www.infosecurity-magazine.com/news/european-police-phone-phishing/
[5] https://www.wallarm.com/what/vishing-attack

purchases or identity theft linked to the recipient's Amazon account. These narratives typically escalated to claims of compromised Social Security numbers or imminent legal action, ultimately pressuring victims into draining their bank or retirement accounts. The FTC advised not to trust caller ID, not to call back numbers provided in voicemails or texts, and to verify any suspicious activity directly through the Amazon website or app.[6]



Vishing attack in action

Source: Wallarm

All of these cases and trends show that the financial impact of vishing is substantial and growing. According to Keepnet, the median financial loss per victim in the U.S. was around $1,400 in 2022, contributing to a total loss of $1.2 billion.[7] In their 2024 Vishing Response Report, Keepnet reported vishing incidents costing organizations an average of $14 million annually.[8]

Given the significant financial impact, organizations should implement comprehensive and continuous training programs to mitigate the risks associated with vishing. It's crucial to understand that vishing can affect anyone, regardless of their background or experience. Both businesses and individuals are vulnerable, with retail organizations being particularly at risk due to the large amounts of personally identifiable information and financial data they hold, making them prime targets for cybercriminals.

To combat these threats, following best practices is essential. Effective measures include on-camera and in-person verification, out-of-band verification[9], and the use of authenticator apps with features like number matching and geo-verification. Additionally, asking questions that only the legitimate person would know can be a simple yet effective strategy. This approach has proven successful for companies like

[6] https://consumer.ftc.gov/consumer-alerts/2024/03/did-you-get-call-or-text-about-suspicious-purchase-amazon-its-scam
[7] https://keepnetlabs.com/blog/step-by-step-voice-phishing-how-ai-voice-cloning-and-caller-id-spoofing-works
[8] https://www.cyberdefensemagazine.com/exploring-the-vishing-threat-landscape/
[9] This is a security process that uses two separate communication channels to verify a user's identity. For example, if you are logging into a website, you might receive a verification code via SMS or a phone call. In the case of vishing, even if the attacker has compromised the phone call, they would still need access to the separate channel to succeed.

Ferrari. Last year, Ferrari avoided a sophisticated deepfake scam where an impersonator used AI to mimic CEO Benedetto Vigna. The scammer contacted a Ferrari executive via WhatsApp, pretending to discuss a confidential acquisition.[10] Despite the convincing imitation, the executive grew suspicious and asked a personal question only the real Vigna would know. When the scammer couldn't answer, the call ended abruptly.[11]

[10] The messages claimed there was a classified acquisition underway and urged the executive to sign a non-disclosure agreement and assist with a currency hedge transaction

[11] https://www.bloomberg.com/news/articles/2024-07-26/ferrari-narrowly-dodges-deepfake-scam-simulating-deal-hungry-ceo

Disclaimer:

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.