What Is Vishing? Voice Phishing Definition | Proofpoint US

Published: 2021-02-27 · Archived: 2026-04-05 22:25:00 UTC

Vishing has become a mounting cybersecurity threat that leverages phone calls and voice communication to deceive individuals into revealing sensitive information. In recent years, attackers have increasingly used sophisticated tactics, including AI-driven voice impersonation, to exploit trust and urgency in business environments.

According to a 2024 report, vishing attacks surged by 442% in the latter half of the year, underscoring the sheer scale of this threat and its impact on organizations worldwide. As businesses rely more heavily on voice-based communication platforms, understanding and mitigating vishing risks has become a critical component of modern cybersecurity strategies.

Table of Contents

Definition

Most people have heard of phishing—vishing is a different attack under the general phishing umbrella that shares the same goals. Vishers use fraudulent phone numbers, voice-altering software, text messages, and social engineering to trick users into divulging sensitive information.

“Short for ‘voice phishing,’ vishing involves the attacker calling the victim and posing as a representative from a trusted organization, like a bank or government agency. The malicious actor may use social engineering techniques to trick the victim into revealing sensitive information over the phone,” explains Dave Cook, Cybersecurity Analyst and frequent author at Proofpoint.

Unlike other forms of phishing, vishing uses a voice to trick users. (Smishing, yet another form of phishing that uses SMS text messages to trick users, is often used in tandem with voice calls, depending on the attacker’s methods.) By exploiting urgency, fear, or authority in their tone, these threat actors aim to bypass organizational security standards, resulting in financial fraud, identity theft, or unauthorized access to corporate systems.

- Experience our technology in action!
- Receive report outlining your security vulnerabilities to help you take immediate action against cybersecurity attacks

Fill out this form to request a meeting with our cybersecurity experts.

Thank you for your submission.

Types of Vishing

Vishing attacks come in various forms, each tailored to exploit trust, urgency, or fear to extract sensitive information from individuals or businesses. Below are some of the most common types of vishing methods used by cyber criminals:

- **Wardialing**: Attackers use automated systems to call large volumes of numbers within specific area codes, often pretending to be local banks or law enforcement. These calls typically contain pre-recorded messages designed to instill fear and prompt victims to share personal information like Social Security numbers or banking details.
- **VoIP (Voice over Internet Protocol)**: Cyber criminals leverage VoIP technology to mask their identities and scale attacks by generating thousands of fake phone numbers. These calls often appear as legitimate local or toll-free numbers, making them harder to detect.
- **Caller ID spoofing**: Scammers manipulate caller ID systems to display trusted names like “IRS” or “Police Department.” This tactic creates a sense of legitimacy and urgency, increasing the likelihood that victims will comply with requests for sensitive information.
- **Tech support scams**: Fraudsters impersonate representatives from well-known companies like Microsoft or Apple, claiming there’s an issue with the victim’s device. They may request remote access or personal credentials under the guise of resolving the problem.
- **Voicemail phishing**: In this method, attackers leave urgent voicemails impersonating banks or government agencies, asking victims to call back. When victims return the call, they’re connected with scammers who attempt to extract sensitive data.
- **Dumpster diving**: This unconventional approach involves searching through physical trash from businesses to obtain documents containing personal data, such as employee names or account details. The gathered information is then used to craft persuasive vishing attacks.

Each type of vishing underscores the importance of vigilance and verification when responding to phone calls or voicemails requesting sensitive information.

Vishing vs. Phishing vs. Smishing?

Phishing, vishing, and smishing all have the same goal: to obtain sensitive data from users that could be used for identity theft, monetary gain, or account takeover.

The main difference between them is the medium used to target potential victims. Whereas phishing is primarily an email-based scam, vishing uses voice, typically calls to a user’s cell phone number. Smishing, on the other

hand, uses SMS or text messages to deceive victims, often exploiting the higher open rates and immediacy of mobile messaging.

Both vishers and phishers send messages to potential victims, usually in high volumes. Phishing attackers send a large number of email messages to a list of potential targets. If the attacker targets a specific organization, only a list of high-privileged user email addresses from the targeted business might be used. Vishing and smishing attacks often involve urgent messages purportedly from banks or delivery services, aiming to create a sense of urgency that prompts victims to act quickly.

Phishers generally use compelling email messages to trick users into replying with sensitive information or convince the user to click a link where malware is hosted. Malicious attachments are also used in some phishing attacks. Smishers use similar tactics via text messages, often including links to fake websites or prompts to download malicious apps.

The visher might first send a text message to potential victims in high volumes from a long list of phone numbers. The message might ask users to make a phone call to the attacker's number. Another vishing method creates an automated message and robo-dials potential victims. It uses computer-generated voice messages to remove accents and build trust. The voice message then tricks the user into connecting to a human agent who continues the scam, or it might ask users to open an attacker-controlled website.

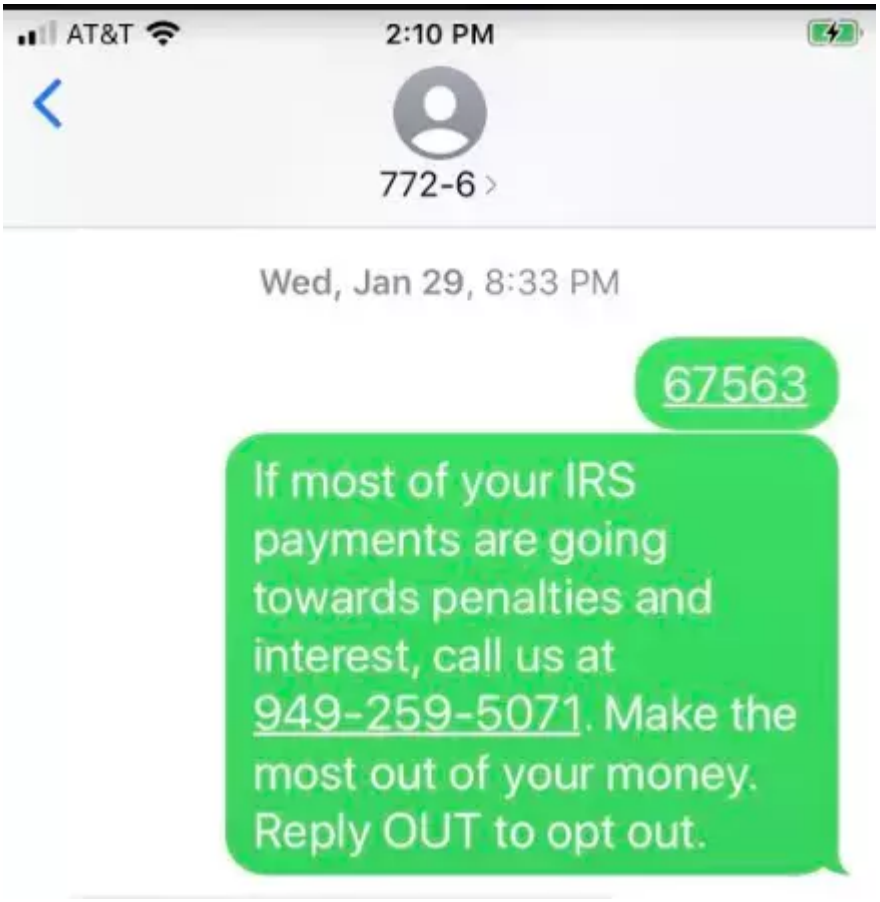
Although there are minor differences between vishing, phishing, and smishing, the end goal is always the same: obtaining credentials, personal identifiable data, and financial information. Users familiar with phishing might not be familiar with vishing, so attackers increase their chances of success.

Vishing Techniques

Identifying a vishing attack is more challenging than a phishing and smishing attack. Vishing attacks start with a text message and usually contain a phone number.

"Fraudsters can rather easily manipulate standard caller ID services," warns Gretel Egan, Security Awareness Training Strategist at Proofpoint. "They can even make it look like your own phone number is calling you (a simple trick to get you to pick up the phone and engage with the caller)."

The following image is an example of a vishing attack:



Scammers use scare tactics to convince users to make a phone call. In this message, the attacker pretends to be with the IRS. Most users fear penalties and fees from the IRS, so users calling this number will be told they owe money. The attacker convinces the targeted user to charge their credit card or to transfer money directly from the targeted user's account. IRS scams are one of the more common attacks targeting users in the U.S.

The following image is another example of a vishing attack starting with a text message:

In the above picture, the same threats and scare tactics are used to convince users to call. If the targeted user responds with STOP, the messages will continue. By replying to the attacker, the targeted user verifies that the phone number is valid and will continue to be a target.

Notice in both images that the caller ID number is an invalid, 6-digit invalid contact number. These numbers are used by telecoms to send users messages, indicating the message was sent from an auto-dialer API or an email account. If a message comes from one of these numbers, always be suspicious that it could be a smishing or vishing scam.

Not every message with an invalid caller ID number is malicious. These numbers are also used in multi-factor authentication requests when the user is sent a PIN to complete the authentication process. Social engineering attackers trick users into sending the PIN by contacting them to divulge the PIN. Vishing, phishing, and smishing can be combined with social engineering for more large-scale attacks on high-privilege accounts.

More and more vishing attackers are using computer programs to mask voices and geographical accents. Attackers can even use a different gendered voice to launch an attack. Often, these voices are audibly computer-generated and obvious vishing attempts. But always be aware of phone calls asking for private information.

Technology Advancements Combating Vishing

Advancements in technology have become a cornerstone in the fight against vishing, enabling real-time detection and prevention of fraudulent calls. These tools are designed to outpace increasingly sophisticated scams.

AI-Driven Anomaly Detection Systems

Artificial intelligence (AI) plays a pivotal role in identifying and mitigating vishing attempts. AI-powered fraud detection systems analyze vast datasets of call patterns, voice characteristics, and contextual information to detect anomalies indicative of fraudulent activity. For example, machine learning models—like deep neural networks and anomaly detection algorithms—can flag suspicious behaviors, such as unusual pauses or scripted speech patterns, in real time.

Natural Language Processing (NLP) further enhances these systems by analyzing call transcripts for coercive language or scam-related phrases, enabling swift identification of threats. Google's recent rollout of on-device AI scam detection for Android devices is a prime example, offering real-time alerts for suspicious calls while preserving user privacy.

Voice Biometrics and Deepfake Detection

Voice biometrics technology leverages unique vocal characteristics such as pitch, timbre, and speech patterns to authenticate callers and detect synthetic voice manipulations. This is especially critical as attackers increasingly use deepfake audio to impersonate trusted individuals.

AI-based systems can identify inconsistencies in speech patterns or mismatched audio features, effectively countering deepfake-enabled vishing campaigns. These technologies not only prevent fraud but also restore trust in voice-based communications.

Telecommunications Advancements

The telecommunications industry has made significant strides in combating vishing through innovations like SHAKEN/STIR protocols. This caller ID authentication framework ensures that calls are verified as legitimate by originating carriers before reaching consumers, reducing the success rate of spoofed calls.

Additionally, real-time fraud management systems integrated into telecom networks can block suspicious calls during the setup phase—before the recipient's phone even rings—by analyzing metadata and historical fraud patterns. These systems offer predictive capabilities, enabling proactive defenses against emerging scam tactics.

How to Prevent Vishing

Avoiding vishing attacks requires a combination of awareness, technology, and proactive measures. Users must take additional precautions to protect themselves. Here are key strategies to prevent vishing:

- **Stay informed and educated**: Regular training and awareness programs are crucial for both individuals and organizations. Educating employees helps them recognize and report vishing attempts, reducing the risk of successful attacks.
- **Verify caller identities**: If a caller requests sensitive information, hang up and contact the institution directly using a verified number. Verify the caller's position, purpose, and organization to ensure legitimacy.

- **Use multifactor authentication (MFA)**: Implement MFA on all sensitive systems to add an extra layer of security, making it harder for attackers to bypass security measures.
- **Be cautious with unsolicited calls**: Ignore calls from unknown numbers and let them go to voicemail. If necessary, call back using a verified number from the organization's official website.
- **Watch for pressure tactics**: Scammers typically use urgency and fear to manipulate victims. Be wary of requests for immediate financial transactions or sensitive information.
- **Protect against SIM swapping**: Be vigilant about messages related to multi-factor PINs or account changes. Contact your telecom provider immediately if you suspect SIM swapping.
- **Register with do not call lists**: Enroll in the National Do Not Call Registry to reduce unsolicited calls, making it easier to identify potential scams.

While telecoms have systems in place to flag suspicious calls, relying solely on these systems is insufficient. By strategically adopting these tactics, individuals and organizations can significantly reduce their vulnerability to vishing attacks.

Get Ahead of Tomorrow's Threats with Proofpoint

Anticipating the nature of certain cyber threats helps organizations identify where their defenses are weak and which protective measures to prioritize. Most organizations are more resilient through layered strategies that leverage detection and prevention technologies, real-time threat intelligence, and user-focused training programs to reduce the risk of attacks via email and cloud environments. As threats like phishing, BEC, ransomware, and credential theft evolve, it's important to have the right mix of tools and processes to keep your data and your people protected. Take ownership to protect against threats and make strides to improve your cybersecurity effectiveness.

Leverage the capabilities trusted by 83 of the Fortune 100 companies. Contact Proofpoint to learn more.

Related Resources
