CS-037 · Email Security

Vishing

Voice-based social engineering that uses phone calls to deceive people into giving up access.

Executive Summary

Vishing is social engineering conducted over the phone, in which an attacker uses a voice call to impersonate a trusted party and manipulate the target into revealing credentials, sharing a one-time passcode, approving a login prompt, or granting remote access. Because a live conversation lets the attacker adapt in real time and apply personal pressure, vishing can be highly persuasive. It is often combined with phishing or smishing to increase credibility.

What It Is

Vishing, short for voice phishing, uses a telephone call rather than a written message to deceive a target. The caller commonly poses as technical support, a bank, a vendor, a government official, or an internal colleague, and constructs a scenario that justifies an urgent request. The goal may be to extract a password or one-time passcode, to have the target approve a push notification, to persuade them to install remote-access software, or to authorize a payment. What makes voice powerful is interactivity: the attacker can respond to hesitation, build rapport, invent reassurances, and escalate pressure in ways a static message cannot. Vishing frequently targets help desks and support staff, whose job is to be helpful, and it pairs naturally with other channels in blended attacks.

Why It Matters

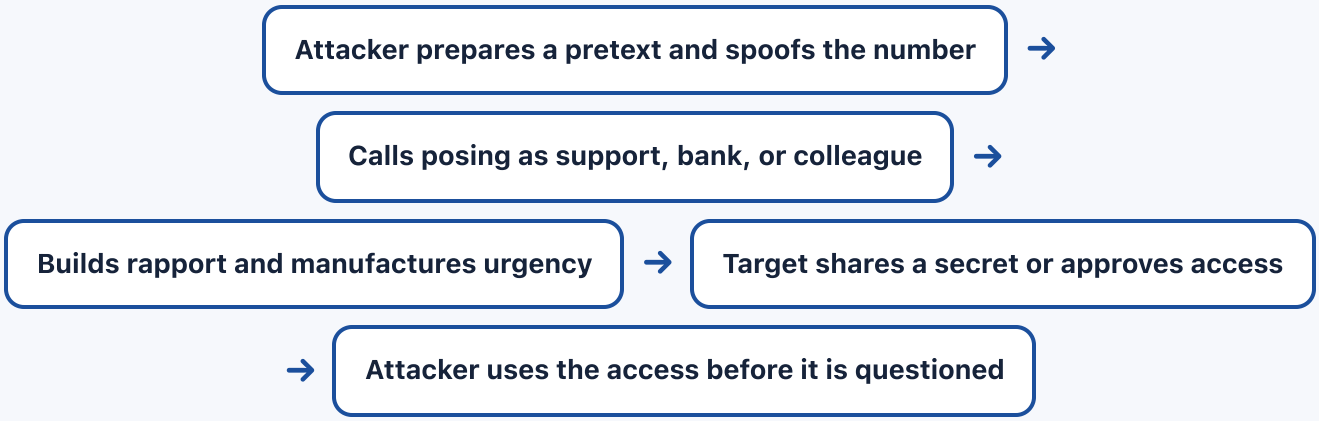
A live human voice carries authority and urgency that text often lacks, and people are conditioned to be cooperative and polite on the phone. This makes vishing effective at extracting exactly the secrets that protect accounts, including the one-time passcodes and push approvals meant to stop attackers who already have a password. Help desks are a favored

target because resetting credentials and granting access is their normal function, and a convincing caller can turn that helpfulness into a breach. Vishing has grown more dangerous as attackers use caller-ID spoofing and, increasingly, synthetic voice tools to impersonate specific people. For professionals, this makes strong identity verification procedures and skepticism toward unsolicited calls essential parts of defense.

How It Works

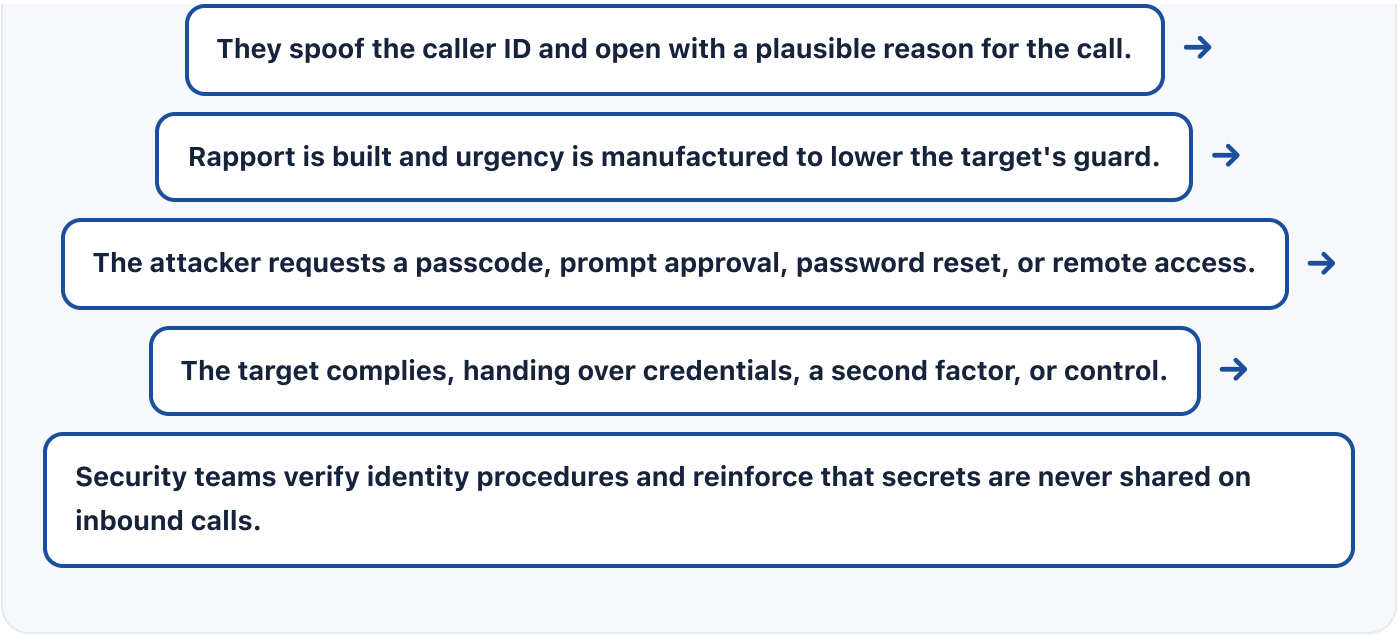
The attacker prepares a pretext and often gathers details in advance so the call sounds informed. They spoof or disguise the calling number to appear trustworthy and open with a believable reason for the call, such as suspicious activity, a required update, or a routine verification. Through conversation they build rapport and manufacture urgency, then make the real request: read back a code, approve a prompt, reset a password, or install a tool that gives them control. If the target hesitates, the attacker adapts, offering reassurance or invoking authority. Success gives them credentials, a bypassed second factor, or direct access, which they use immediately before the ruse is discovered. Defenses center on verifying the caller through independent means and never sharing secrets or approving prompts on an inbound call.

Architecture Diagram



Vishing uses a live call and adaptive persuasion to extract secrets or access the attacker needs.

Visual Workflow



Common Attacks

- Impersonating technical support to obtain a password or install remote-access software
- Posing as a bank or agency to extract account details or a one-time passcode
- Calling a help desk to trick staff into resetting an account or bypassing verification
- Prompting repeated push approvals until a tired user finally accepts (MFA fatigue)
- Using caller-ID spoofing or synthetic voice to impersonate a specific trusted person

Common Mistakes

- Trusting a caller because the number on the display looks official
- Sharing a one-time passcode or approving a prompt during an inbound call
- Help desks resetting access without strong, independent identity verification
- Assuming a confident, friendly caller must be legitimate
- Having no clear procedure for staff to pause and verify an unexpected call

Best Practices

- Verify unexpected callers by hanging up and calling back a known official number
- Never share passwords or one-time passcodes over the phone
- Use phishing-resistant authentication that cannot be read out or approved blindly

- Enforce strong, scripted identity verification at help desks
- Train staff and support teams specifically on voice pretexts and pressure tactics
- Establish a safe way to decline or pause a suspicious call without penalty

Quick Checklist

- [x] Callback verification policy for unexpected or sensitive calls
- [x] Clear rule that passcodes and passwords are never shared by phone
- [x] Phishing-resistant multi-factor authentication in use where possible
- [x] Scripted, strong identity checks required for help-desk resets
- [x] Voice-specific awareness training for staff and support teams
- [x] Incident path to lock accounts quickly after a suspected vishing compromise

Recommended Tools

Phishing-resistant MFA
Uses factors that cannot be read aloud or approved without intent

Help-desk identity verification
Enforces strong, scripted checks before any reset or access grant

Caller authentication and screening
Reduces spoofed and fraudulent inbound calls reaching staff

Security awareness platform
Trains staff on voice pretexts, pressure, and safe callback habits

Industry Standards

NIST SP 800-63
Digital identity and authentication assurance, including account recovery

NIST SP 800-61
Incident handling for a compromise that follows a vishing call

CIS Critical Security Controls
Authentication and awareness safeguards

that reduce vishing success

Career Relevance

Vishing defense spans identity verification, help-desk operations, and awareness. SOC analysts and incident responders handle account takeovers that begin with a phone call, and security awareness leads train staff and support teams on voice pretexts. Security engineers deploy phishing-resistant authentication that resists coaxed approvals, while GRC analysts assess help-desk verification and account-recovery controls. For the AI-Governance-Jobs.com audience, vishing is a key social engineering topic across security and governance work.

Interview Questions

- What is vishing, and why can a live call be more persuasive than an email?
- How does MFA fatigue work, and how do you defend against it?
- Why are help desks a favored target, and how would you harden them?
- What identity verification steps should precede any account reset?
- How do synthetic voice tools change the risk from vishing?

Related Certifications

CompTIA Security+ | **ISC2 Certified in Cybersecurity (CC)** | **GIAC Security Essentials (GSEC)**

Further Reading

- CISA: Avoiding Social Engineering and Phishing Attacks
- FTC: Phone Scams
- NIST: Digital Identity Guidelines

Key Takeaways

- Vishing is social engineering conducted over the phone.
- A live conversation lets attackers adapt, build rapport, and apply pressure.
- Help desks and one-time passcodes are frequent targets.

- Never share secrets or approve prompts on an inbound call.
- Callback verification and phishing-resistant authentication are core defenses.

FAQ

▶ **How is vishing different from phishing?**

▶ **What is MFA fatigue?**

▶ **How can I verify an unexpected caller?**

Related Careers

RELATED ROLES

Soc Analyst

Security Awareness Lead

Incident Responder

Grc Analyst

RELATED CERTIFICATIONS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

GIAC Security Essentials (GSEC)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides

Role roadmaps

Salary data

Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Vishing**
3. Go deeper: Smishing
4. Go deeper: Phishing
5. Validate it: work toward **CompTIA Security+**

6. Find the role: browse current openings

RELATED SHEETS

CS-036 Smishing | CS-032 Phishing | CS-033 Spear Phishing | CS-025 Multi-Factor Authentication (MFA) | CS-010 Cyber Hygiene