Help desk vishing

# One phone call can hand an attacker an employee's account.

Attackers no longer break authentication. They call the help desk, pose as an employee and ask for a password reset or a new MFA device. The agent decides on trust and on details anyone can look up. One successful call is a valid account with that employee's access.

**#1**

initial infection vector for cloud intrusions is now voice phishing (vishing)

Mandiant M-Trends 2026

**82%**

of detections were malware-free: attackers used valid credentials and trusted identity flows

CrowdStrike 2026 Global Threat Report

**$100M**

in losses at MGM Resorts after one help desk call led to a password reset

MGM Resorts SEC Form 8-K, Q3 2023

## How the attack works

- **Research:** names, roles and managers from LinkedIn and breached data.
- **The call:** an urgent story, such as a locked account or a new phone, sometimes in an AI-cloned voice.
- **Weak checks pass:** employee ID, manager name and security questions are all things an attacker can find.
- **Access re-issued:** the reset or MFA re-enrollment gives the attacker a working account, past MFA and SSO.

## Why it matters

- **It bypasses your identity stack:** MFA, SSO and PAM protect login. Recovery is where a human re-grants trust.
- **Proven, costly attacks:** Caesars paid a $15M ransom after an outsourced IT vendor handed over credentials; Marks & Spencer lost £300M in operating profit after IT support was socially engineered.
- **Outsourced help desks:** external agents have no familiarity with your workforce, and no reliable way to tell a real employee from an impostor.

> **The control gap:** help desks are built to help. Agents are measured on fast resolution and happy callers, not on catching impostors, so the default is to *trust* the person on the line.

## How imper.ai closes it, inside your existing help desk flow

01

### A link to a known recovery channel

The request starts as usual, in the ITSM portal, the IVR or a phone call. A browser link goes to the employee's registered recovery email or phone, as strong as an OTP. Nothing to install.

02

### Impersonation detection

Opening the link exposes the requester's infrastructure: VPNs and proxies, VoIP lines, remote control, virtual machines and location. Optional security questions or a document check can be added on top.

03

### Resolve or escalate

Verified employees unlock the account or reset the password themselves, directly in your directory. Risky requests go to an agent with a risk score and evidence, and an alert to the SOC.

Works with ServiceNow, IVR and phone, Entra ID, Okta, O365 and Google Workspace, for in-house or outsourced help desks. Sources: Mandiant M-Trends 2026. CrowdStrike 2026 Global Threat Report. MGM Resorts SEC Form 8-K (Q3 2023). Caesars Entertainment ransom disclosure (September 2023). Marks & Spencer FY 2025/26 results.