Vishing Attack Prevention and Response

WHAT IS THE DIFFERENCE BETWEEN PHISHING, SMISHING, AND VISHING? While each type of attack attempts to steal personal information, each takes a different approach to accomplish the goal. Phishing uses emails and links, smishing uses text messages or common messaging apps, and vishing uses voice calls and voicemails to obtain sensitive information. Let's take a closer look at vishing and how Cofense can help you prepare your employees to identify and report malicious vishing campaigns.

OVERVIEW

Vishing is a prevalent and serious threat that lets adversaries gain access to your company's enterprise and direct access to your most critical data. Today's sophisticated vishing techniques easily bypass many organizations' prevention tactics, making vishing a rewarding option for attackers. As a result, security teams must understand how vishing targets their organization, the potential impacts on the business, and how to update their anti-phishing strategies.

According to the FBI, vishing has seen a significant increase since the beginning of the COVID-19 pandemic and employees, both in the office and working in other locations, are at a higher risk of a vishing attack than they were two years ago.

ANATOMY OF A VISHING ATTACK

Vishing attacks usually start with contact by phone, email, and/or text message and request an employee to reach out via a voice call to request personal or financial information. Often, callers pretend to be from the company's IT or finance department; impersonate an executive in their respective company, business partner, or federal agency; and/or claim to be from a software vendor used by employees at your organization. The caller attempts to convince the employee to provide private information or take action that will be used to compromise the company's networks, gain access, or steal data or funds.

Users should be suspicious of anyone who calls with a request that includes:

- Account issues demanding urgency or immediate resolution of a problem that is difficult to verify (IT access/failure, financial accounts, locked-out logins, etc.).
- Requests for information like full name, birth date, social security number, etc.

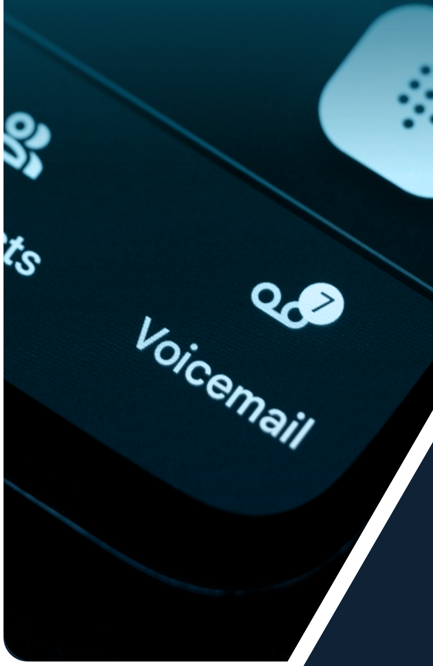
Threat actors may even provide partial information on coworkers or vendors to convince victims to release the information they need.

RESPOND AND RECOVER FROM VISHING ATTACKS

Vishing sets the groundwork to launch more in-depth attacks which can lead to more substantial crimes, including malware, ransomware, data and financial theft, malicious data deletion, and general business disruption. Through vishing, hackers can even gain unrestricted access to your entire network, placing all the organization's data at risk. Vishing and related phishing incidents must be reported when recognized so security teams can move quickly to respond.

According to surveys of working adults and IT professionals conducted in 2022, almost 7 in 10 (70%) respondents reported having encountered vishing attacks. This represents an increase from 54% in 2020.

Source: Statista March 2023



cofense.com/vishing

MINIMIZE THE IMPACT OF VISHING ATTACKS

A solid security response plan that minimizes the potential impact of a vishing attack on your business must include:

- An easy, non-punitive, and efficient way for users to immediately report incidents that include the information disclosed, to determine potential damage of the attack.
- Documented procedures to quickly alert financial institutions, vendors, and federal agencies, along with any partners or branches of the business that may be affected.
- A way to communicate the security threat so your enterprise is aware and can recognize other potential risks.

STRENGTHEN YOUR SECURITY POSTURE WITH CUSTOMIZED VISHING ENGAGEMENT

With Cofense, you can take your program even further to help maximize your return on investment. Our professional services team can develop and execute a customized vishing program specifically tailored to your organization's needs on top of what you get through our vishing learning modules. Let’s take a closer look at the Vishing Simulation program.

PhishMe and Reporter are required for Cofense's Vishing Simulation program. The program includes:

- A vishing outreach program layered on top of the annual phishing program.
- Quarterly vishing simulations conducted on employees.
- Upon reaching the interactive voice response (IVR), employees will be informed that the simulation is part of a larger company-sanctioned security awareness training program.
- Susceptible employees receive additional training content to reinforce preferred behavior/action.
- Localized program execution by region.
- Robust post-simulation reporting provided regarding employees who fell susceptible to the training.

THE COFENSE WAY TO PREVENT VISHING ATTACKS

Vishing can often go undetected, and security awareness is critical because untrained employees may not recognize and report suspicious phone calls. Vishing attacks focus on high-value business targets, such as call centers, IT administrators, accounts payable, HR, and more. Security teams should implement the following vishing prevention measures to protect their organization:

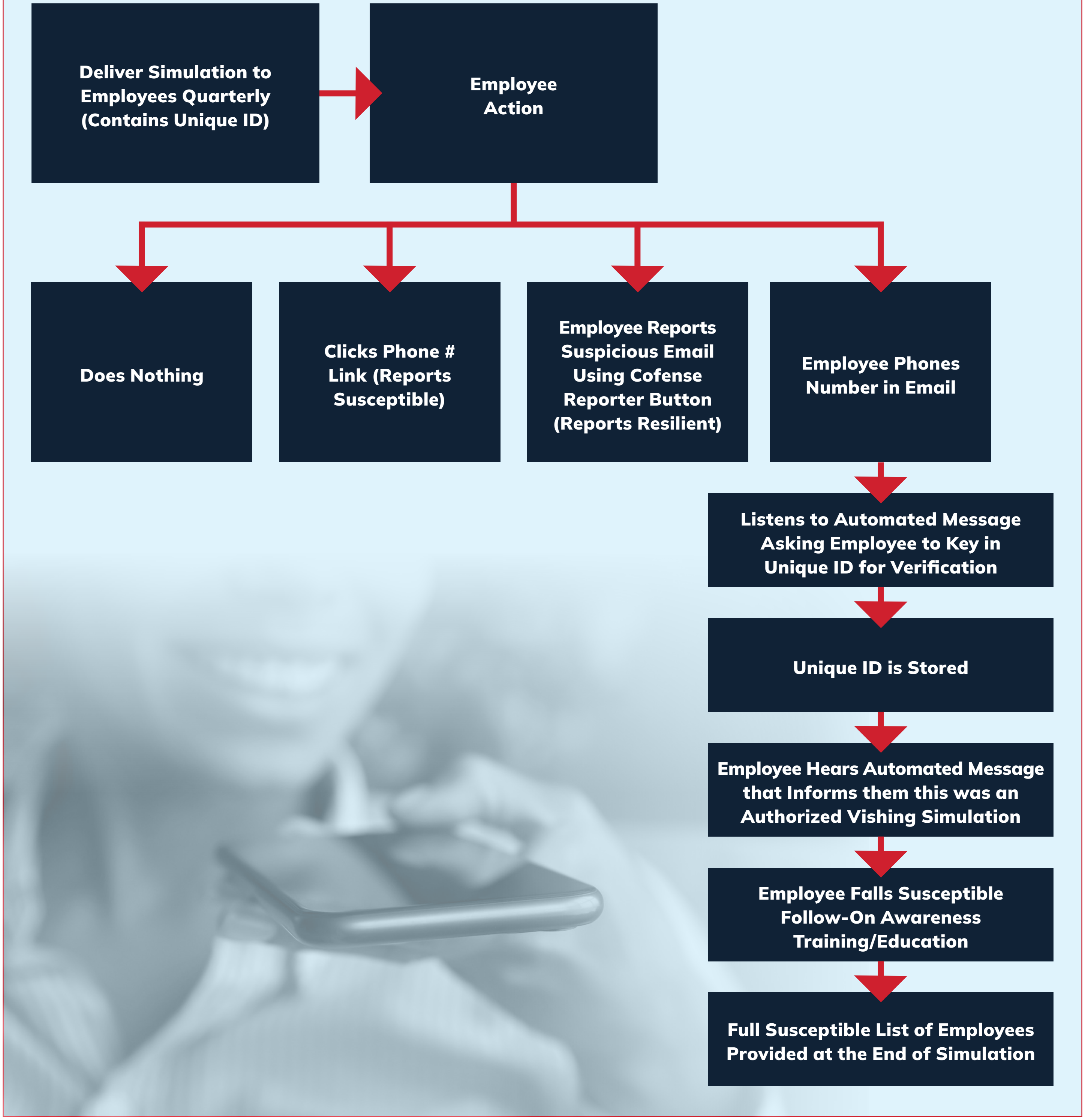
- Update security awareness programs with Cofense’ s vishing LMS modules to train employees to recognize and report vishing attempts.
- Add Cofense Reporter to your email task bar for easy and efficient reporting.
- Vish your employees at a regular cadence using vishing simulations
- Train employees at all levels to verify caller identity and the authenticity of email links.
- Advise all employees to refrain from texting sensitive information in social and messaging apps other than official company platforms.
- Use your enterprise technology stack to block unknown numbers and add mobile apps to route calls to your company’s VoIP.
- Make sure anti-spam and anti-phishing solutions are current.
- Augment native email security with Cofense threat detection and leverage auto-quarantine to remediate suspicious emails.

COFENSE LMS VISHING MODULES INCLUDE:

- **Micro Vishing** – An overview of vishing including pretexting, emotional appeals, priming the recipient, and what to do to avoid the traps.
- **Vishing Simulators** – Our latest vishing simulation includes new threats to detect, updated phone choices, and customization options to improve immersion.
- **Vishing Comprehensive Simulator** – Helps the user apply critical thinking to voice mail messages.

HOW IT WORKS

VISHING SIMULATION WORKFLOW


Deliver Simulation to Employees Quarterly (Contains Unique ID)
Employee Action
Does Nothing
Clicks Phone # Link (Reports Susceptible)
Employee Reports Suspicious Email Using Cofense Reporter Button (Reports Resilient)
Employee Phones Number in Email
Listens to Automated Message Asking Employee to Key in Unique ID for Verification
Unique ID is Stored
Employee Hears Automated Message that Informs them this was an Authorized Vishing Simulation
Employee Falls Susceptible Follow-On Awareness Training/Education
Full Susceptible List of Employees Provided at the End of Simulation

About Cofense

Cofense® is the original and leading provider of security awareness training and phishing simulation, offering global enterprise-level advanced email threat detection and remediation solutions. Cofense PhishMe® and Cofense Phishing Detection and Response (PDR) offer the world's only platforms to leverage over 35 million Cofense-trained employees who actively report suspected phishing and other dangerous email threats in real-time. Exclusive only to Cofense, this reporting system ingests and catalogs thousands of threats per day that are missed by current email gateway technologies and then eradicates those threats from customer inboxes. In short, Cofense sees and stops threats other email security systems miss. Please visit www.cofense.com or connect with us on X and LinkedIn for additional information.

COFENSE
EMAIL SECURITY

W: cofense.com/contact T: 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175