keepnet

2024
VOICE PHISHING (VISHING)
RESPONSE REPORT

www.keepnetlabs.com

2024
VOICE PHISHING (VISHING)
RESPONSE REPORT

Table of Content

1. Executive Summary 1
 1.1. Key Findings: 1
2. Introduction 2
3. Methodology 2
 3.1. Consent and Compliance 2
 3.2. Data Anonymization 2
 3.3. Security Measures 2
 3.4. Selection of Companies and Departments 2
 3.5. Criteria for "Vished" and "Vishing Aware" 2
4. Overall Findings 3
5. Industry Analysis 4
 5.1. Breakdown and Percentages of Industries: 5
6. Department Analysis 6
 6.1. Breakdown and Percentages of Departments: 7
7. Comparative Analysis 8
 7.1. Cross-Sector vs. Intra-Organizational Dynamics 8
 7.2. Tailored Cybersecurity Measures 8
8. Best Practices and Recommendations 9
9. A Case Study: Teknosa's Success Against Vishing 10

About Keepnet: A Unified Human Risk Management Platform 11
 Keepnet's Uniqueness: Advanced AI to Simulate and Educate 11
 Best Phishing Simulators 11
 Behavior-Based Security Awareness Training 11

Appendices 12
 Glossary of Terms: 12
 Methodology of Vishing Simulations 12
 The Importance of Vishing Simulation in Security Awareness Training 17
Keepnet's Managed Vishing Test Service 17
Legal Notice 18

1. Executive Summary

Vishing (voice phishing or voice scam) is a social engineering attack where hackers manipulate your employees into revealing confidential information over phone calls.

The 2024 Voice Phishing Response Report shows how businesses are at risk from voice phishing attacks. This report presents findings from our AI-based voice phishing simulations, which identify risky behaviors across industries and departments when faced with vishing threats:

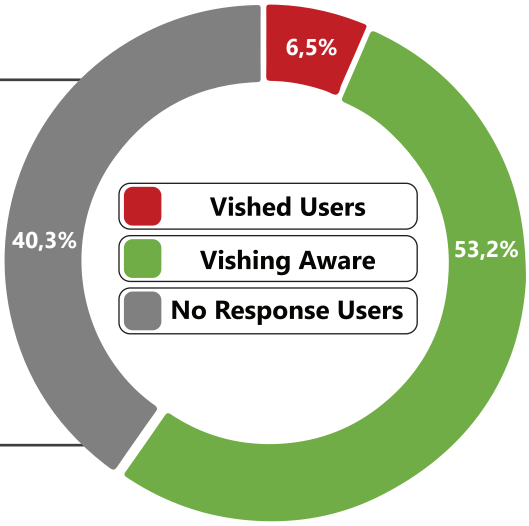
- **70% of businesses share sensitive information during fake calls.** Utilizing vishing simulation tools allows employees to learn from mistakes in real-time.
- Companies with the lowest rates of being vished often use sophisticated vishing simulation software. Adding regular vishing simulations to cybersecurity training helps **employees recognize and respond to voice phishing attacks with up to 90% success.**

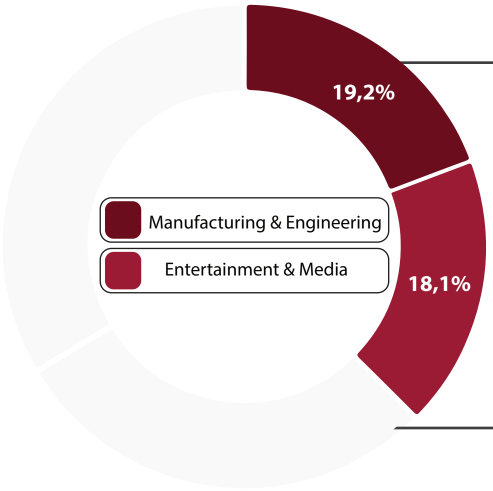
1.1. Key Findings:

Overview of Vulnerability Across Companies:

- Total users called: **3.279**
- Users who fell for Vishing: **6,5%**
- Users aware of Vishing: **53,2%**
- Users with No Response: **40,3%**

1





Most Vulnerable Industries:

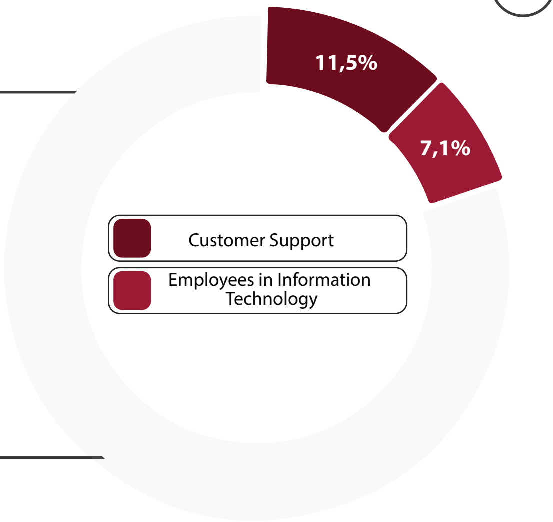
- Employees in the Manufacturing & Engineering industries are most vulnerable, with a 19,2 % fall for vishing.
- Employees in the Entertainment & Media industries follow closely, with vished rates of 18,1%.

2

Most Vulnerable Departments:

- Employees in Customer Support are most at risk, with an 11,5% vished rate.
- Employees in Information Technology departments are also highly vulnerable, with a 7,1% vished rate.

3



2. Introduction

The 2024 Voice Phishing Response Report highlights the rising threat of vishing. It analyzes how it affects different industries and departments. The urgency of addressing voice phishing issues has never been clearer. In 2023, vishing attacks led to losses topping $10 billion in the United States, costing businesses an average of over $14 million yearly globally.

Vishing can harm businesses, like the MGM Resort hack. In this attack, criminals used voice phishing to break into the company's protected networks. This attack caused a huge loss of about $100 million. The MGM Resort hack shows the need for organizations to prevent vishing threats and improve cybersecurity to protect themselves.[1]

Our research showed that **6,5% of employees gave away sensitive data during fake vishing calls.**

40,3% of calls went unanswered. This could mean that employees are avoiding or missing threats. Risks include employees accidentally calling attackers, criminals following up, or not recognizing and reporting vishing attempts.

3. Methodology

To understand the vulnerability of various industries and departments to voice phishing attacks, we conducted a comprehensive analysis within a defined timeline and under strict ethical and legal guidelines. This study includes simulated vishing campaigns between January 15, 2023, and January 15, 2024. A total of 82 companies generously consented to participate, providing data under conditions of anonymity and confidentiality.

3.1. Consent and Compliance

Participating companies explicitly consented to use their data, fully informed of the study's purpose and methodologies. Our analysis follows relevant data protection laws, including CCPA and GDPR, ensuring the highest legal compliance and privacy standards.

3.2. Data Anonymization

Data anonymization techniques were used to protect individual privacy. These methods guarantee that no individual can be identified directly or indirectly from the data used in our study.

3.3. Security Measures

Data security protocols, including encryption and secure storage, were implemented to secure the data throughout the analysis. Anonymized data used in this study will be retained only as long as necessary before secure deletion under our data retention policy.

3.4. Selection of Companies and Departments

We merged similar companies and departments from the dataset's broad range of industries to streamline the analyzing process. This allowed us to enhance the clarity and relevance of our findings. For instances where customers did not specify their industry or department, we categorized these as "Others." This grouping ensured we didn't miss any data, making a complete and fair analysis possible.

3.5. Criteria for "Vished" and "Vishing Aware"

- **Vished Employees:** Defined by their action of sharing sensitive information during a voice phishing test. The vished employees need additional security awareness training to identify and prevent voice phishing attacks.

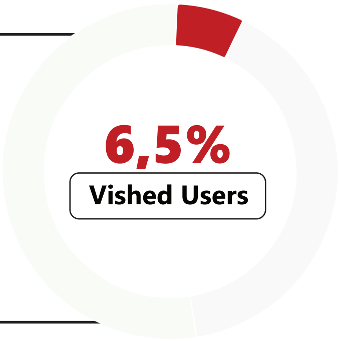
- **Vishing Aware Employees:** Recognize a vishing attempt and respond appropriately. They either refrain from giving information or end the call to protect security.

[1] For further details on the MGM Resort hack and insights into how vishing attacks can compromise business cybersecurity, leading to significant financial losses, refer to our in-depth coverage: https://keepnetlabs.com/blog/cybersecurity-in-the-spotlight-unraveling-the-mgm-resort-breach

4. Overall Findings

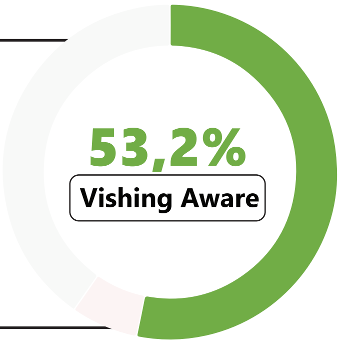
1

Vished Users:
6,5% of the calls resulted in employees being vished. This indicates a vulnerability where individuals hand over information or take actions that could lead to a security breach.



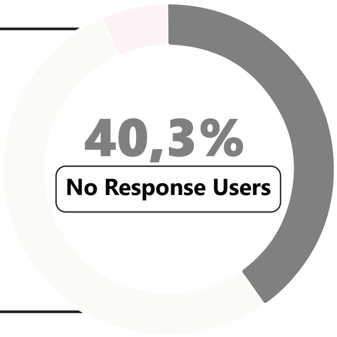
2

Vishing-Aware Users:
Most of the calls, 53,2%, were handled by vishing-aware employees. These people either hung up the call quickly or said no when asked to share sensitive data.



3

No Response Users:
40,3% of all calls received no response. This significant portion of non-engagements is concerning because it leaves open the question of vulnerability among these employees.[2]

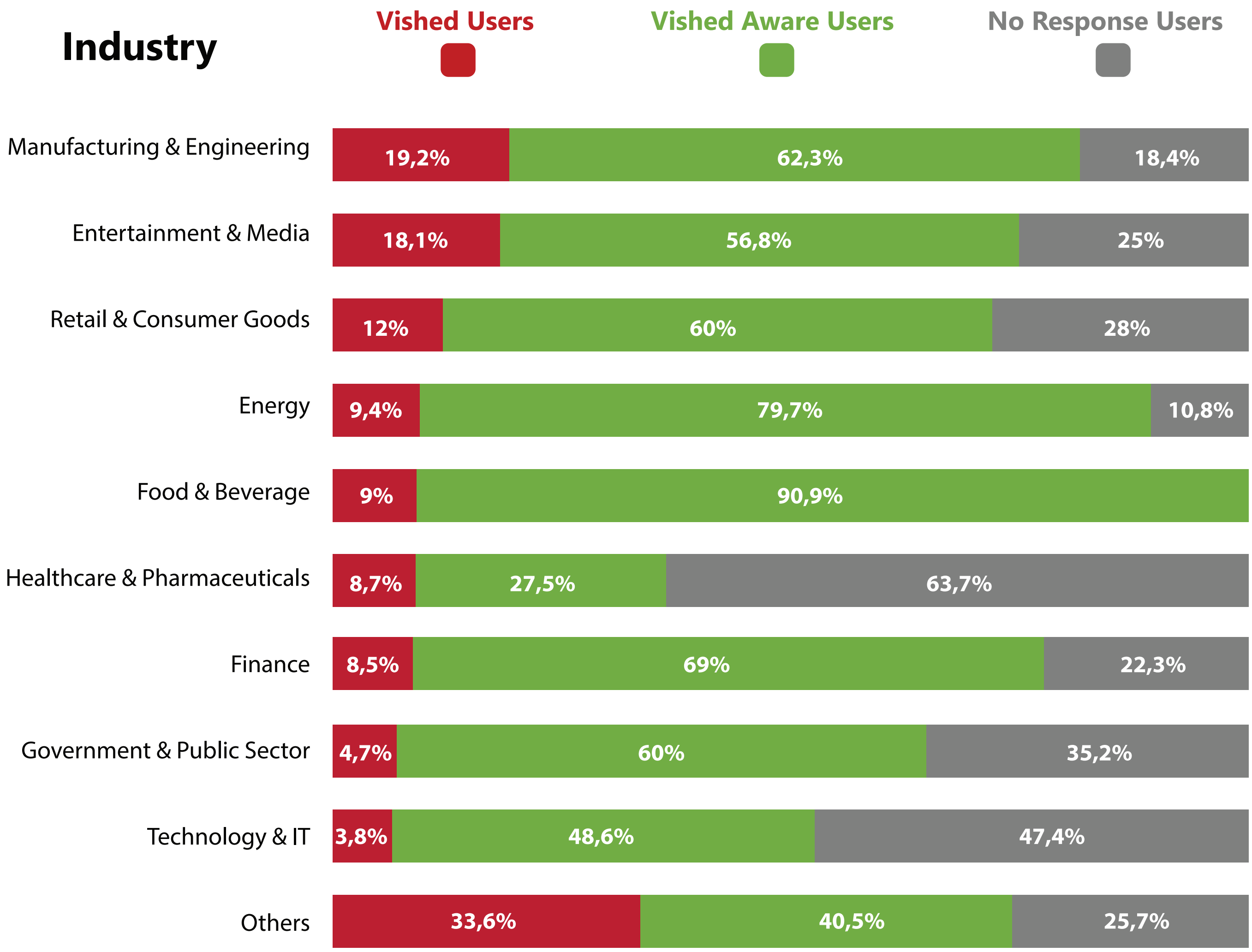


> *"The insights from this report shed light on a critical issue at a time when social engineering attacks continue to evolve at an alarming pace. The vulnerabilities revealed through this comprehensive analysis highlight the pressing need for industries to adopt a more proactive approach to cybersecurity. It's clear from the data that investing in advanced, behavior-based security training is not just a good practice—it's essential for protecting against sophisticated voice phishing attacks."*
>
> **Joe Busto, VP of Sales, North America**

[2] The term "No Response Users" describes employees who fail to answer 40% of incoming calls. This significant figure is alarming and prompts critical questions about the nature of these missed calls. Are these employees actively identifying and avoiding dangerous calls, or are they simply unavailable or not paying attention? The high rate of no responses may introduce a significant vulnerability in security measures, potentially leaving us exposed to undetected criminal activities. Also, this oversight not only represents a serious blind spot in the defensive operations but also poses a real threat, as it could allow criminals to exploit these gaps to their advantage.

5. Industry Analysis

The table[3] below shows how vulnerable test users were in various industries:



- Employees in Manufacturing & Engineering show higher vulnerability, possibly due to factors including less focused cybersecurity training and resources. To protect against vishing scams better, focused education and training programs are important, especially for at-risk industries.

- In contrast, employees in the Technology & IT industries have the lowest vishing rates, likely due to a stronger focus on technology and strict regulations.

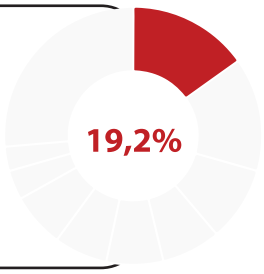
[3] Vulnerability of test users are ranked by the "vished percentage".

5.1. Breakdown and Percentages of Industries:

Highest Vulnerability: Manufacturing & Engineering

- Employees in the Manufacturing & Engineering industry show the highest vulnerability, with a vished percentage of 19,2%.
- This could be due to various factors, including potentially less focus on cybersecurity training tailored to vishing threats.

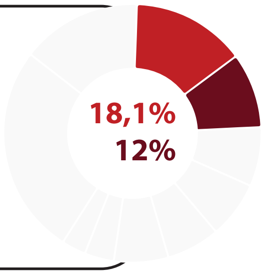
1



Entertainment & Media and Retail & Consumer Goods

- Both sectors show a higher vished percentage than others, at 18,1% and 12% respectively.
- This could reflect the public-facing nature of these industries, which regularly engage in external communications.

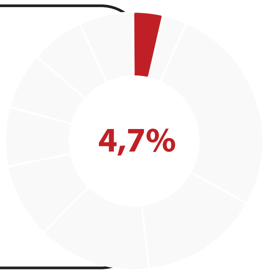
2



Government & Public Sector Resilience

- Despite having many total users, the Government & Public Sector show a low vishing percentage of 4,7%.
- This could indicate effective training programs or a more cautious approach by users when handling voice communications.

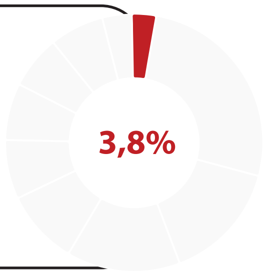
3



Lowest Vishing Vulnerability: Technology & IT Sectors

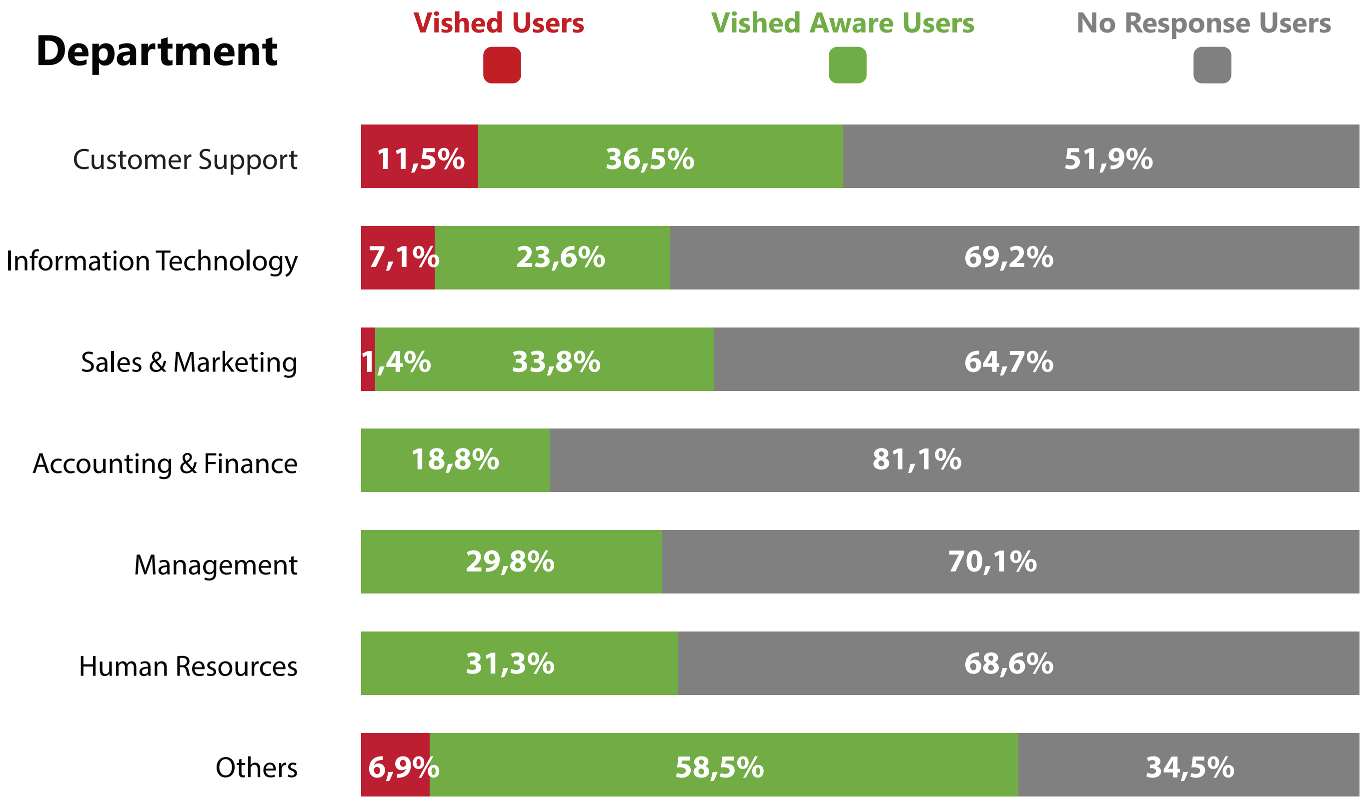
- Employees in the Technology & IT sector have the lowest vished percentage at 3,8%, which is not surprising considering the industry.
- Employees in this sector are likely more aware of cybersecurity threats and how to avoid them.

4



6. Department Analysis

The following table[4] reveals that vishing vulnerabilities and awareness levels differ significantly across organizational departments.



- Departments like Customer Support are at higher risk of vishing attacks. They need specific training and awareness programs to prevent them.
- Departments with no "vished" percentages may have good security or low exposure. However, they also have high no-response rates. This indicates they still need security awareness training since we do not know why they did not engage in the calls.

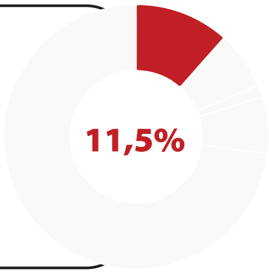
[4] Vulnerability of test users are ranked by the "vished percentage".

6.1. Breakdown and Percentages of Departments:

Highest Vishing Vulnerability: Customer Support

- The Customer Support department has the highest vishing percentage at 11,5%.
- Customer Support roles involve a lot of communication with outside parties. This can make them more vulnerable to vishing attacks.

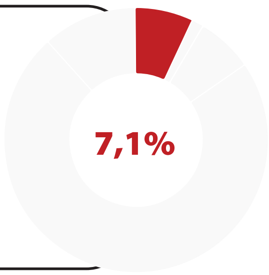
1



Moderate Vulnerability: Technology & IT

- The Technology & IT department, at 7,1%, has a relatively lower percentage of vishing than Customer Support, but still shows a notable number of vished users.
- This indicates that even departments with presumably higher awareness levels are not immune to vishing threats.

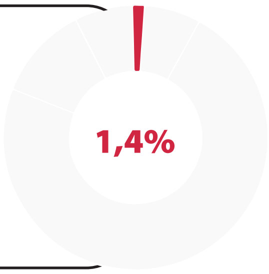
2



Low Vishing Vulnerability: Sales & Marketing

- The Sales & Marketing department has a low vished percentage of 1,4%, compared to other departments.
- This demonstrates their strength and ability to overcome challenges in their job. Their job requires them to be cautious and verify information when dealing with external messages.

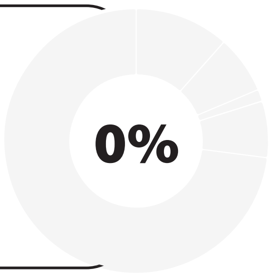
3



Zero Vishing Incidents: Accounting & Finance, HR, and Management

- The Vishing rate of the Accounting & Finance, Human Resources, and Management departments is 0%.
- This means that these departments' training and awareness programs work well. As a result, there may be fewer vishing attacks in these departments compared to others.

4

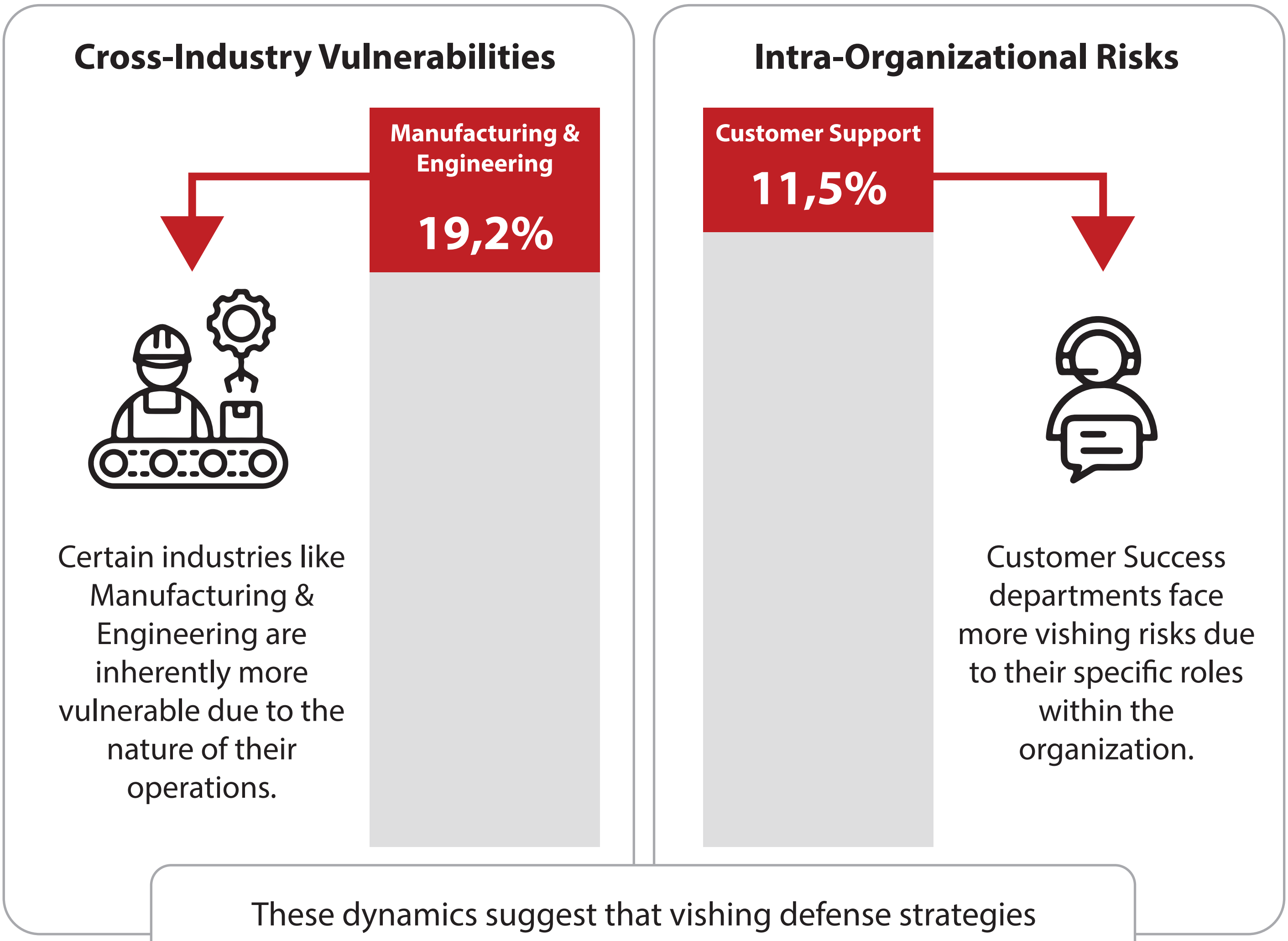


7. Comparative Analysis

Vishing scams are more likely to target certain industries and departments. Sales and Customer Support teams communicate with people outside the company and are at higher risk of vishing scams.

Departments such as Research & Development or Internet Technology focus on internal tasks. This means they may be less affected by outside influences. This is because they have fewer direct interactions with external sources.

7.1. Cross-Sector vs. Intra-Organizational Dynamics



Cross-Industry Vulnerabilities

Certain industries like Manufacturing & Engineering are inherently more vulnerable due to the nature of their operations.

Intra-Organizational Risks

Customer Success departments face more vishing risks due to their specific roles within the organization.

These dynamics suggest that vishing defense strategies must be broadly applicable across industries and tailored to address department-specific vulnerabilities.

7.2. Tailored Cybersecurity Measures

Organizations should tailor cybersecurity strategies to both the industry and the specific roles within it. Despite general strategies, departments like Customer Support or Internet Technology require specific training to address risks.

8. Best Practices and Recommendations

The analysis of vishing simulation results has revealed the critical role of proactive cybersecurity measures. This section outlines effective strategies and recommendations for enhancing vishing awareness and resilience:

Effective Strategies:

- **Vishing Simulation Software:** Companies with the lowest rates of being vished often employ sophisticated vishing simulation software. These tools simulate realistic vishing attempts and provide employees with immediate feedback. They help them learn from their mistakes in real-time. Adding regular vishing simulations into the cybersecurity training enables employees to recognize and respond to various tactics attackers employ.

- **Behavior-based Security Awareness Training:** Effective training programs go beyond generic advice. They have tailored content to the specific vulnerabilities and scenarios relevant to each department and industry. For example, customer-facing departments like Sales and Customer Support benefit from scenarios that mimic daily situations. This targeted approach ensures that training is relevant and engaging, increasing retention and applying best practices.

Recommendations:

- **Tailored Training for Vulnerable Departments:** Departments identified as most at risk should receive specialized training. This should focus on the vishing attacks they are most likely to encounter. Interactive workshops and role-playing exercises can enhance engagement and retention of key concepts.

- **Industry-Specific Modules:** Industries with higher vishing vulnerability should develop customized training modules that address their unique threats. By incorporating industry-specific examples and case studies, companies can provide more contextual and applicable guidance for their employees.

- **Continuous Learning and Nudges:** Implementing a continuous learning program can help maintain high levels of awareness. This can include periodic vishing simulations, security awareness courses, nudges, and updates on the latest vishing tactics. Encouraging employees to share and learn from each other helps create a culture of security awareness and vigilance.

- **Employee Awards Programs:** Recognizing and rewarding employees who successfully identify and report vishing attempts can motivate others to stay vigilant. These programs can also highlight the importance of cybersecurity awareness within the company culture.

- **Enhanced Reporting Mechanisms:** Simplifying the process for reporting suspected vishing attempts encourages employees to act without fear. Clear guidelines help address potential threats quickly and effectively.

"Our approach to mitigating vishing threats goes beyond conventional methods. Focusing on behavior-based security awareness training and voice phishing simulations, we empower employees to be the first line of defense against social engineering attacks."

Ozan UCAR, CEO of Keepnet

9. A Case Study: Teknosa's Success Against Vishing

211

Stores

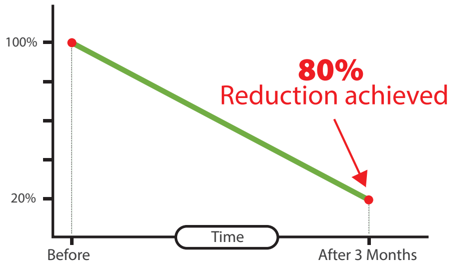
2500

Employees

"As a leading technology retailer with 211 stores and over 2.500 employees, we were experiencing significant losses due to vishing attacks."

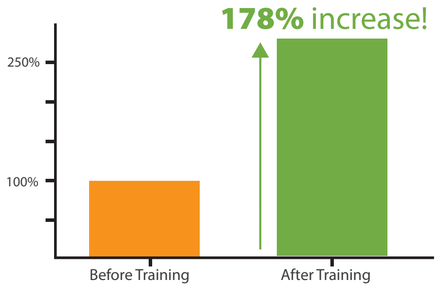
"Threat actors were stealing sensitive data from our sales representatives over the phone by impersonating C-level executives, causing monetary losses and stress to our business. To counter this, we implemented an AI-based voice phishing simulation in our security awareness program."

Vishing Risk Reduction Over Three Months



Within three months, our vishing risk score was reduced by 80%.

Increase in Reporting of Fake Calls



Employees reporting of real fake calls increased by 178%.

Potential Loss Avoided Per Year

Successfully avoided a potential annual loss of $439,250.

"This initiative has helped our employees understand the risks associated with phone communications, handle fake calls effectively, and follow procedures to secure our business."

Ulas Kaya
Information Security Manager at Teknosa

Read the full case study below:

Read Now

You'll learn how to:

- AI-powered simulation and training can reduce vishing risks by up to 80%.
- Implementing effective scam detection strategies can potentially save up to $439.250 annually.
- Increase employee reporting of fraudulent calls by as much as 178%.

About Keepnet: A Unified Human Risk Management Platform

Keepnet is a unified platform that addresses the human element of cybersecurity risks. Keepnet offers a holistic approach to strengthening the security culture using tools that simulate phishing attacks and deliver security awareness training. This equips employees with the knowledge and skills to identify and prevent potential threats of social engineering attacks.

Keepnet's Uniqueness : Advanced AI to Simulate and Educate

Our vishing defense strategy leverages the latest artificial intelligence (AI) to create and manage a series of dynamic vishing scenarios. This capability sets us apart from competitors who offer static, one-size-fits-all training modules.

Unlike platforms that offer fragmented solutions, Keepnet provides a full spectrum of products that work together to train, simulate and test employee readiness against sophisticated social engineering and phishing tactics. This includes:

Best Phishing Simulators

- **Email Phishing Simulation:** Trains employees to recognize and respond appropriately to phishing emails, a common vector for cyber attacks.

- **Smishing Simulation:** As SMS scams increase, Keepnet ‘s smishing simulator helps employees identify and avoid SMS phishing attempts.

- **Vishing Simulation:** The cutting-edge vishing (voice phishing) simulator teaches staff to be cautious of deceptive phone calls.

- **Quishing (QR Code Phishing) Simulation:** With the rising use of QR codes, the risk of QR code-based phishing grows. Keepnet's Quishing Simulator educates about this emerging threat.

- **MFA Phishing Simulation:** Multi-factor authentication is significant for security, but phishing attacks targeting MFA protocols are sophisticated. The MFA Phishing Simulator prepares employees for such attacks.

- **Callback Phishing Simulator:** This innovative tool trains employees to recognize and appropriately respond to callback phishing, where attackers manipulate victims into calling back on a malicious number.

Behavior-Based Security Awareness Training

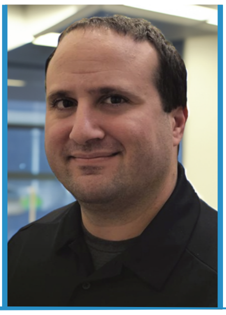
Besides these phishing simulations, Keepnet uses a behavior-based security awareness training method. This method not only educates employees about the different cyber threats but also automates the delivery of targeted security training in response to employees' incorrect actions.

Recognition by Gartner's Voice of the Customer

Keepnet’s commitment to cybersecurity excellence is further validated by their recognition in Gartner's “Voice of the Customer report. ”This acknowledgment highlights Keepnet’s role as a leader in the security awareness industry, committed to developing innovative, user-centric solutions to combat social engineering and enhance organizational security.

“We saved a huge amount of time with high quality output integrating the platform with our own custom servers and were able to produce 2400 social engineering activities, including vishing. We were able to scale and schedule out to run operations when needed with great reporting results.”

Jon Isaacson, JTI Cybersecurity



Appendices

Glossary of Terms:

- **Vishing:** A social engineering attack known as voice phishing, where attackers use telephone services to trick individuals into handing over sensitive information like passwords or credit card details.
- **Vished Users:** Individuals successfully deceived by a vishing simulation, leading them to provide sensitive information or perform actions that could compromise security.
- **Vishing Aware Users:** Individuals correctly identified and responded to vishing attempts by refusing to give information or ending the communication.
- **No Response Users:** Participants who did not respond to vishing attempts either successfully identified or avoided the threat. It could also be the lack of engagement with calls to unknown numbers.
- **Vishing Percentage:** The proportion of vished users relative to the total number of users subjected to the vishing simulation, indicating the success rate of vishing attempts.
- **Simulation Software:** Tools used to create realistic vishing (or other phishing) scenarios for training and assessing employee responsiveness to such threats.
- **Social Engineering:** Psychological manipulation techniques used by attackers to trick individuals into making security mistakes or giving away sensitive information.
- **Sensitive Information:** Data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization, such as passwords, financial records, or personal identification numbers.
- **Cybersecurity Training:** Programs designed to educate employees about various cybersecurity threats, including vishing, and best practices for preventing such attacks.

Methodology of Vishing Simulations

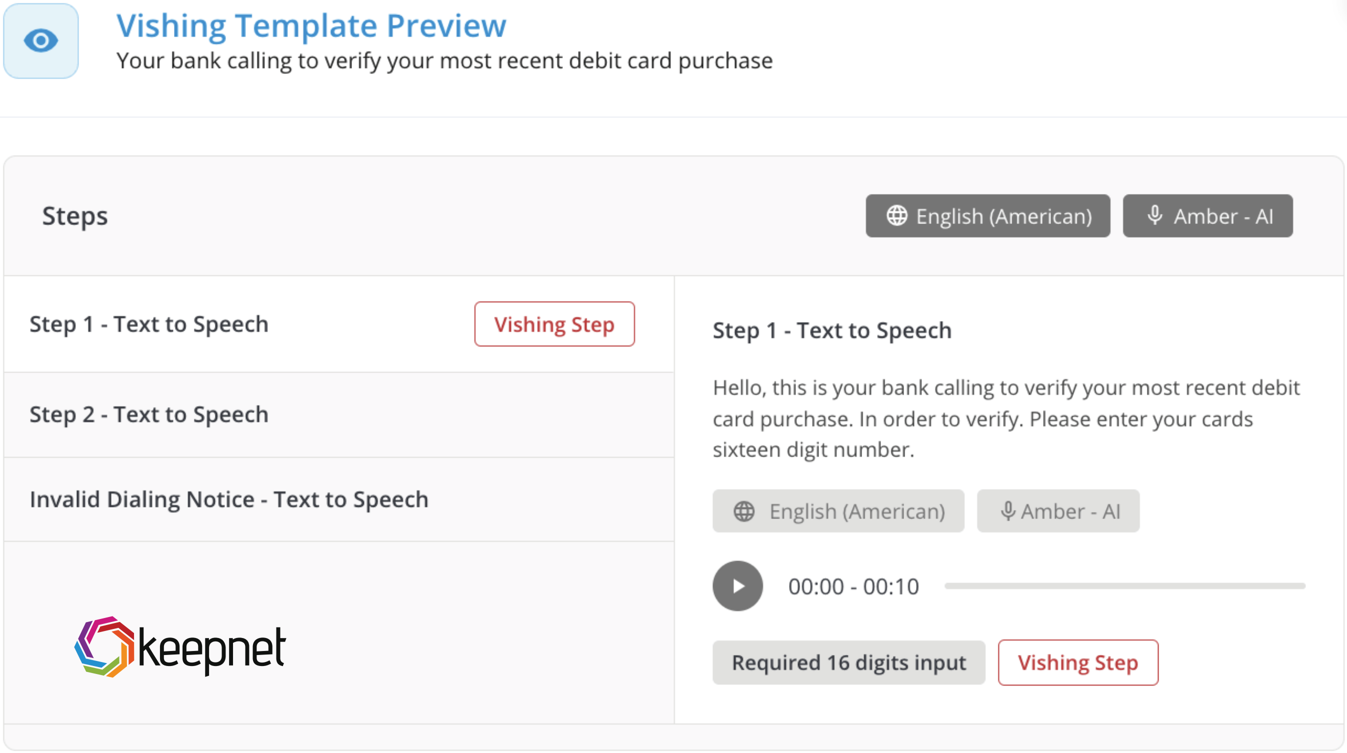
Vishing (voice phishing) simulations are integral to modern cybersecurity strategies. They aim to enhance employees' ability to recognize and respond to voice phishing attempts. Here's a closer look at how we have implemented voice phishing simulations for our clients.

Initial Setup on Our Platform

The process begins with administrators uploading their employee numbers onto our platform. This initial step is important, tailoring the simulation to the specific needs.

Designing the Vishing Scenario

After the initial setup, it is time to create the voice phishing scenario. Administrators can either craft these vishing templates or select pre-existing scenarios. This customization is key to creating a realistic and relevant test environment. See a sample scenario in the screenshot below:



Vishing Template Preview

Your bank calling to verify your most recent debit card purchase

Steps

English (American) | Amber - AI

Step 1 - Text to Speech — Vishing Step

Step 2 - Text to Speech

Invalid Dialing Notice - Text to Speech

Step 1 - Text to Speech

Hello, this is your bank calling to verify your most recent debit card purchase. In order to verify. Please enter your cards sixteen digit number.

English (American) | Amber - AI

00:00 - 00:10

Required 16 digits input — Vishing Step

In this example, the simulated phone call is set up to impersonate a bank. It informs the employees that the call is to confirm a recent transaction made with their debit card. The call then prompts the targets to enter their debit card's sixteen-digit number.

As you can see, the user interface has a text-to-speech component. An artificial intelligence named "Amber" is used to create a voice that will read the message aloud to the call employees.

The aim is to create an experience where employees can practice recognizing and responding to social engineering tactics without compromising their actual security or privacy.

Selecting Targets and Customizing Calls

Once the scenario is set, administrators can select the target users for the simulation. This ensures that the simulation reaches the intended participants.

Additionally, administrators can customize the call numbers. They can use a local number from their area. This makes the simulated vishing calls appear more realistic and effective.

Vishing Simulation Execution

The execution phase of the vishing simulation is where the action takes place. Our AI-powered system starts calling the employees using the pre-designed script. The call mimics real people to test the employee's ability to detect voice phishing. The scenarios require a prompt requiring them to press a button to proceed. This phase is safe and controlled, with no real-world risks, aiming to sharpen the employees' response to potential vishing attacks. It's important to note that although the AI system targets specific employee IDs for calls, it does not retain any employee ID information.

Analyzing the Result

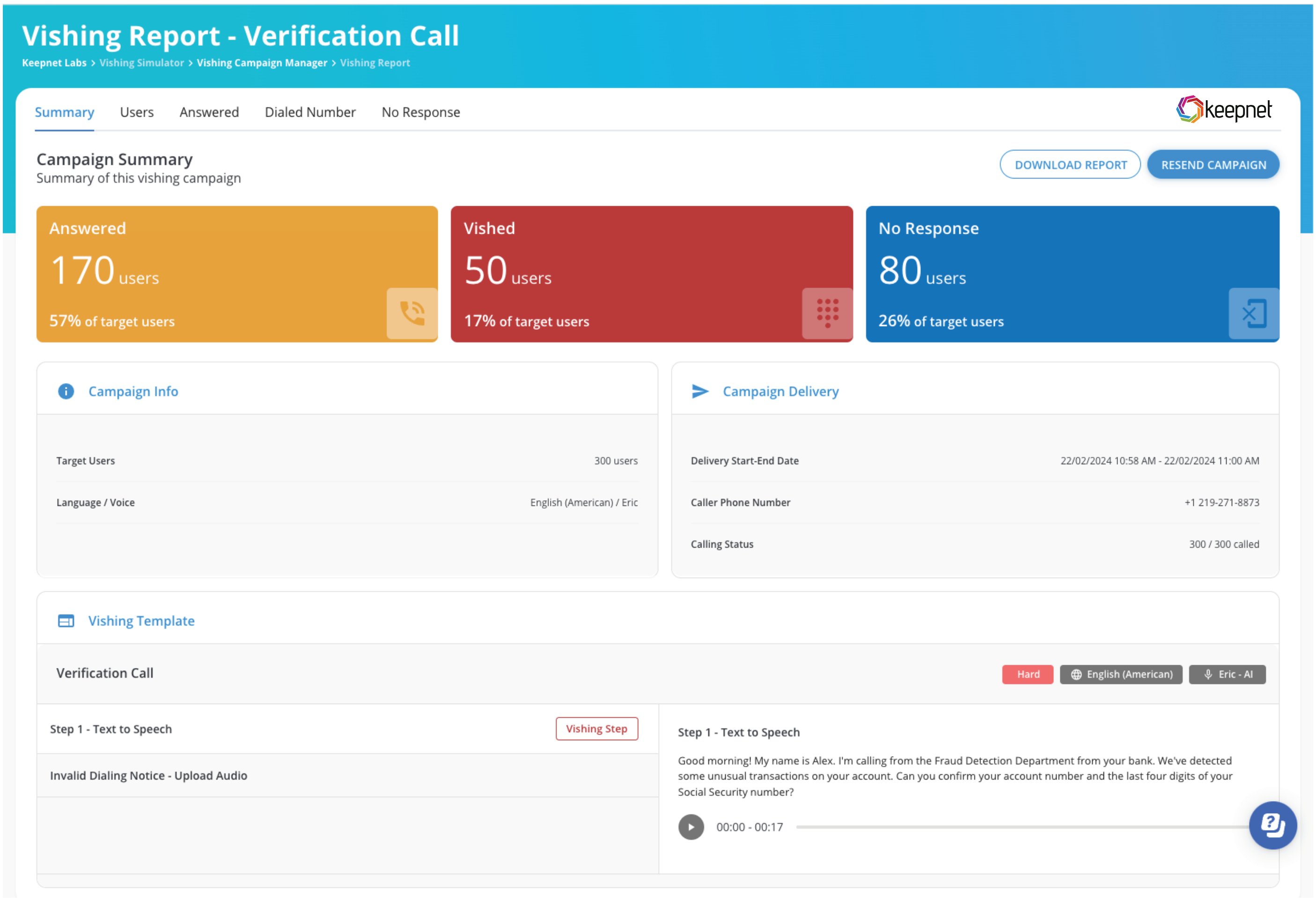
Following the simulation, a detailed Vishing Report is generated. This report shows the data from the vishing tests. This offers important insights into employee interactions with the simulated voice phishing campaigns. Key metrics analyzed include the number of employees that are vished, vished-aware or no response.

Our vishing report aims to provide actionable insights into how employees interact with potential phishing calls. This information is significant for identifying vulnerabilities and tailoring cybersecurity training programs.

The report is divided into several tabs, each offering a different perspective on the employees' reactions to the vishing calls.

Summary Tab:

This tab provides an overall view of the campaign results, summarizing the key metrics such as the number of calls made, vished, and the number no response.



Vishing Report - Verification Call

Keepnet Labs > Vishing Simulator > Vishing Campaign Manager > Vishing Report

Campaign Summary
Summary of this vishing campaign

Answered	Vished	No Response
170 users	50 users	80 users
57% of target users	17% of target users	26% of target users

Campaign Info

Target Users	300 users
Language / Voice	English (American) / Eric

Campaign Delivery

Delivery Start-End Date	22/02/2024 10:58 AM - 22/02/2024 11:00 AM
Caller Phone Number	+1 219-271-8873
Calling Status	300 / 300 called

Vishing Template

Verification Call — Hard · English (American) · Eric - AI

Step 1 - Text to Speech — Vishing Step

Invalid Dialing Notice - Upload Audio

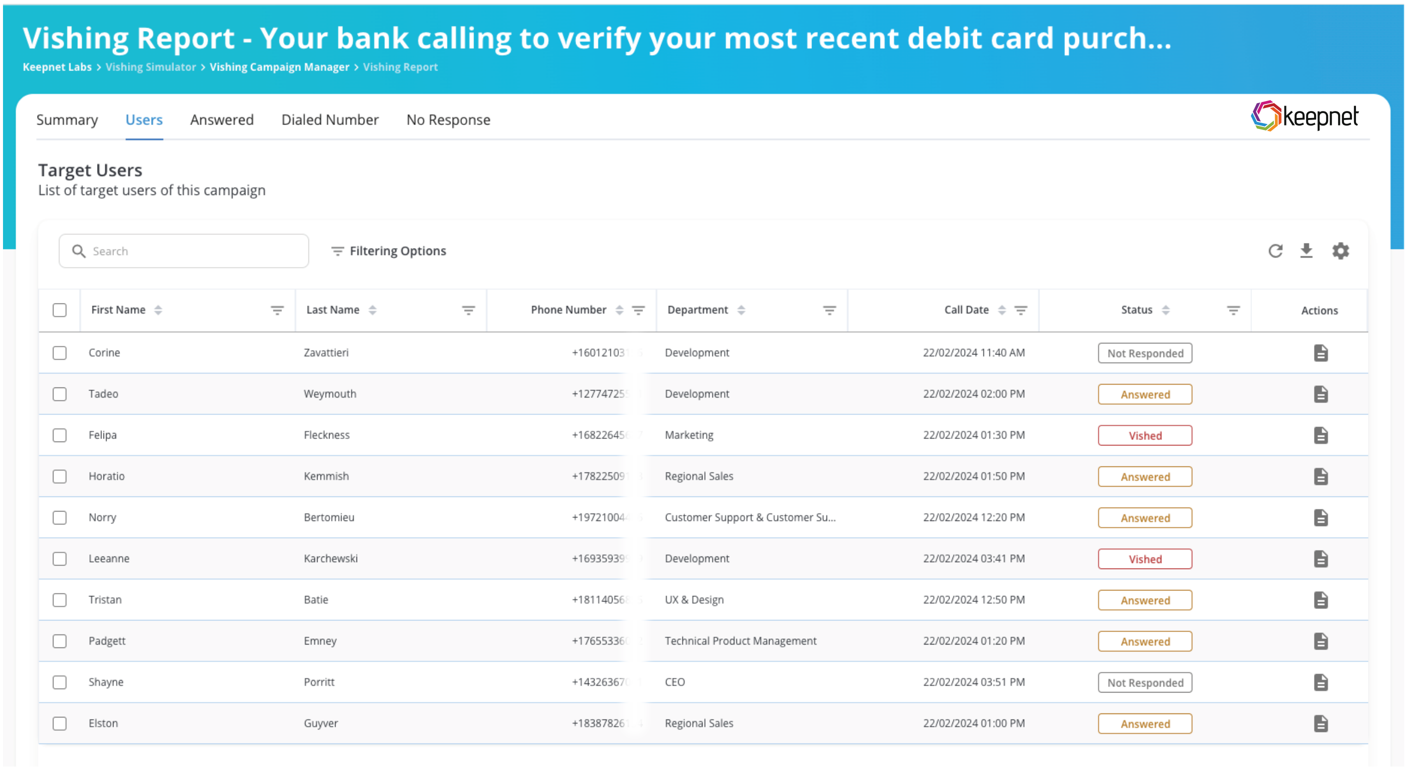
Step 1 - Text to Speech

Good morning! My name is Alex. I'm calling from the Fraud Detection Department from your bank. We've detected some unusual transactions on your account. Can you confirm your account number and the last four digits of your Social Security number?

00:00 - 00:17

Users Tab:

Here, all individuals targeted in the vishing campaign are listed. The report details whether they answered the call, ignored it, or were successfully "vished" (i.e., deceived into following the caller's requests).[5]



Vishing Report - Your bank calling to verify your most recent debit card purch...

Keepnet Labs > Vishing Simulator > Vishing Campaign Manager > Vishing Report

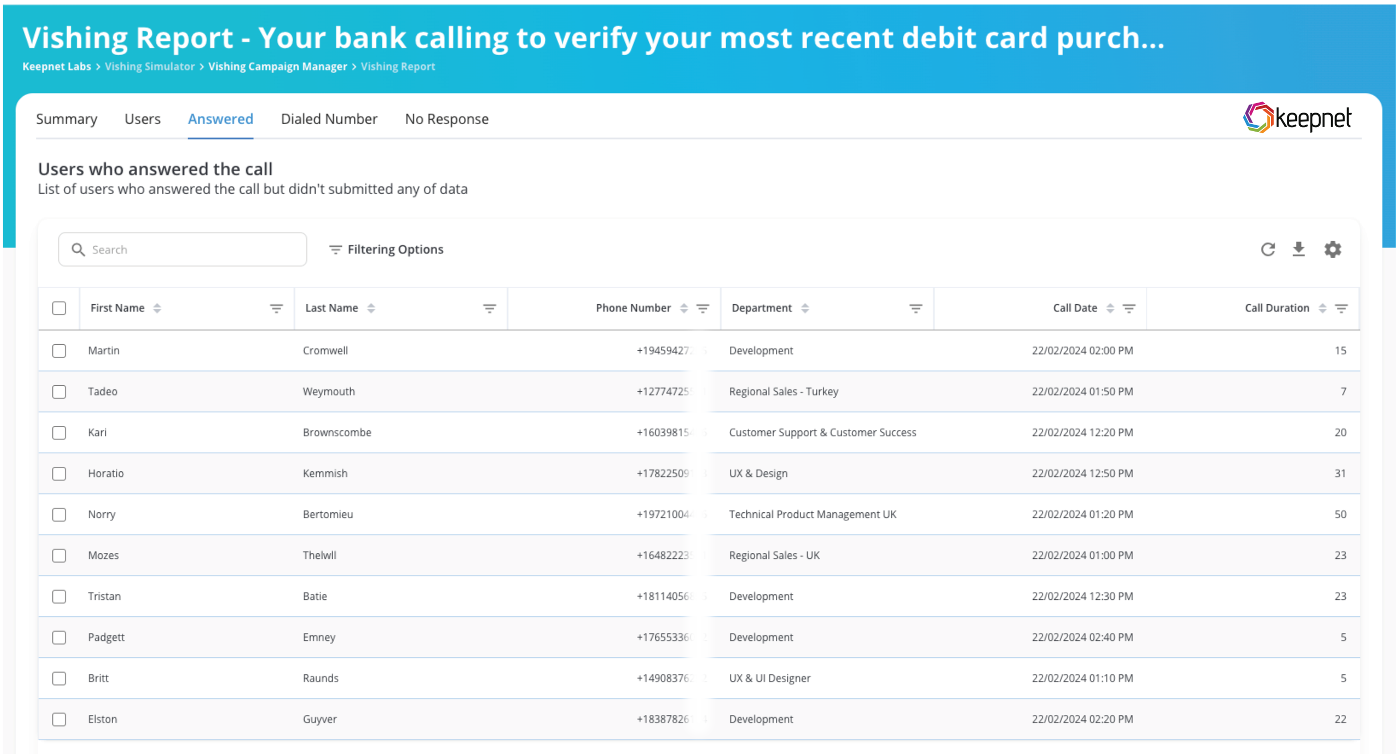
Target Users

List of target users of this campaign

☐	First Name	Last Name	Phone Number	Department	Call Date	Status	Actions
☐	Corine	Zavattieri	+16012103	Development	22/02/2024 11:40 AM	Not Responded	📄
☐	Tadeo	Weymouth	+12774725	Development	22/02/2024 02:00 PM	Answered	📄
☐	Felipa	Fleckness	+16822645	Marketing	22/02/2024 01:30 PM	Vished	📄
☐	Horatio	Kemmish	+17822509	Regional Sales	22/02/2024 01:50 PM	Answered	📄
☐	Norry	Bertomieu	+19721004	Customer Support & Customer Su...	22/02/2024 12:20 PM	Answered	📄
☐	Leeanne	Karchewski	+16935939	Development	22/02/2024 03:41 PM	Vished	📄
☐	Tristan	Batie	+18114056	UX & Design	22/02/2024 12:50 PM	Answered	📄
☐	Padgett	Emney	+17655336	Technical Product Management	22/02/2024 01:20 PM	Answered	📄
☐	Shayne	Porritt	+14326367	CEO	22/02/2024 03:51 PM	Not Responded	📄
☐	Elston	Guyver	+18387826	Regional Sales	22/02/2024 01:00 PM	Answered	📄

Answered Tab:

This section shows the list of users who answered the simulated vishing call. It includes information on the duration of the call, indicating how long the employee engaged with the potential threat.



Vishing Report - Your bank calling to verify your most recent debit card purch...

Keepnet Labs > Vishing Simulator > Vishing Campaign Manager > Vishing Report

Users who answered the call

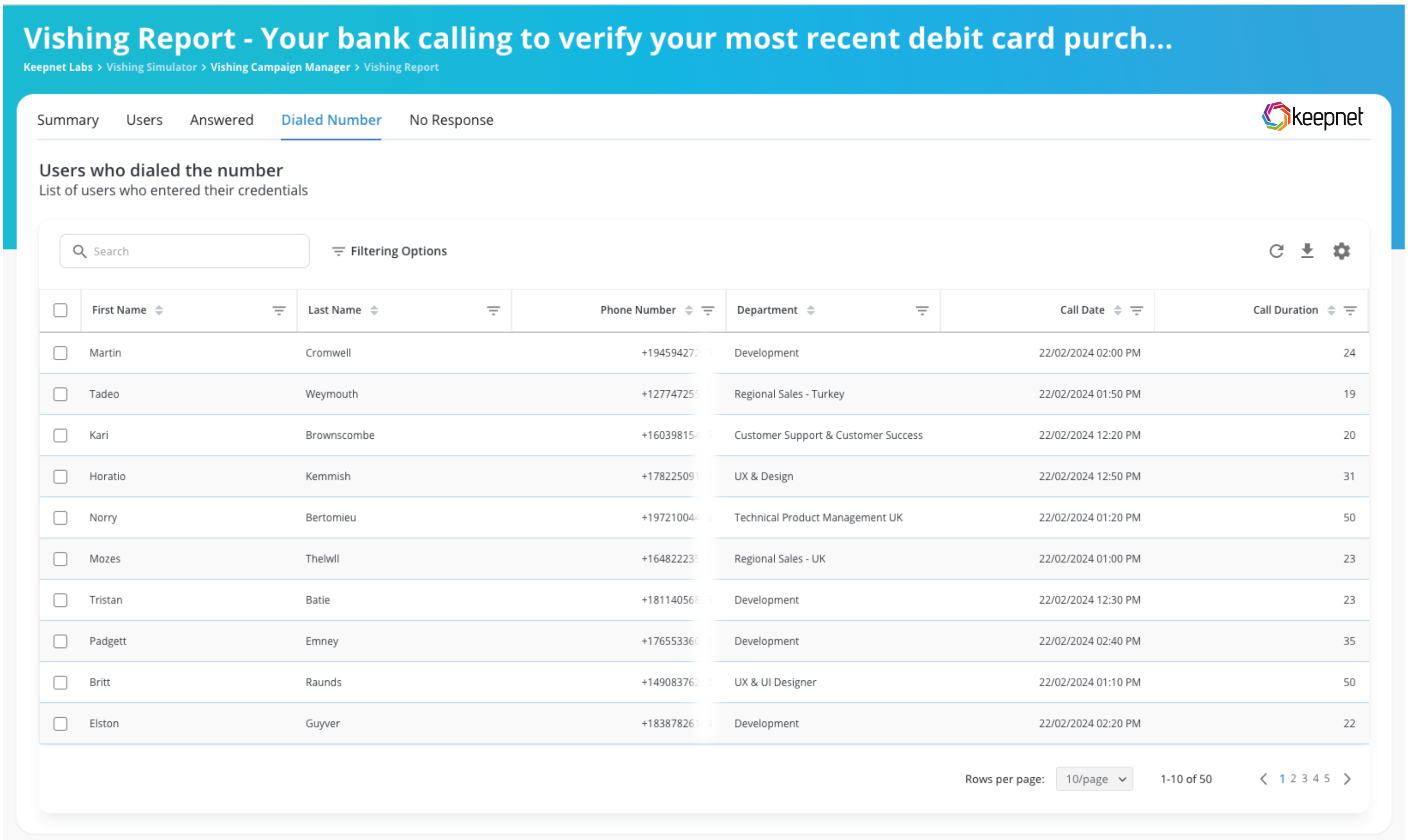
List of users who answered the call but didn't submitted any of data

☐	First Name	Last Name	Phone Number	Department	Call Date	Call Duration
☐	Martin	Cromwell	+19459427	Development	22/02/2024 02:00 PM	15
☐	Tadeo	Weymouth	+12774725	Regional Sales - Turkey	22/02/2024 01:50 PM	7
☐	Kari	Brownscombe	+16039815	Customer Support & Customer Success	22/02/2024 12:20 PM	20
☐	Horatio	Kemmish	+17822509	UX & Design	22/02/2024 12:50 PM	31
☐	Norry	Bertomieu	+19721004	Technical Product Management UK	22/02/2024 01:20 PM	50
☐	Mozes	Thelwll	+16482223	Regional Sales - UK	22/02/2024 01:00 PM	23
☐	Tristan	Batie	+18114056	Development	22/02/2024 12:30 PM	23
☐	Padgett	Emney	+17655336	Development	22/02/2024 02:40 PM	5
☐	Britt	Raunds	+14908376	UX & UI Designer	22/02/2024 01:10 PM	5
☐	Elston	Guyver	+18387826	Development	22/02/2024 02:20 PM	22

[5] The employee information displayed in this report is entirely fictional. It has been generated with a specialized tool utilizing free online software, designed to simulate a realistic user experience on our platform. This demonstration aims to provide our clients with an accurate preview of how their reports would appear when using our services. None of the names, numbers, or any personal details correspond to real individuals.

Dialed Number Tab:

It details instances where employees have been manipulated by our AI-powered vishing system to perform specific actions as instructed during the call. This may include providing sensitive information such as social security numbers, login credentials, or any other confidential data. Employees listed in this section are those who have been 'vished'.



Vishing Report - Your bank calling to verify your most recent debit card purch...

Keepnet Labs > Vishing Simulator > Vishing Campaign Manager > Vishing Report

Summary | Users | Answered | **Dialed Number** | No Response

Users who dialed the number
List of users who entered their credentials

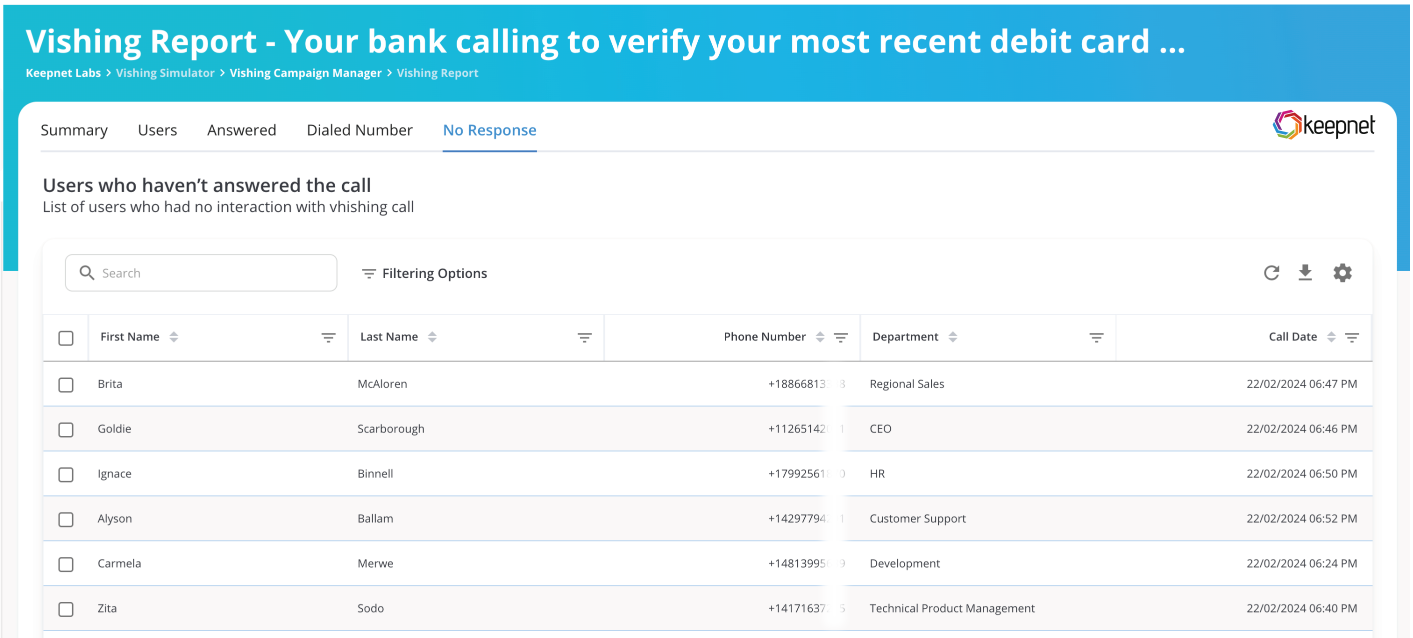
Search | Filtering Options

□	First Name	Last Name	Phone Number	Department	Call Date	Call Duration
□	Martin	Cromwell	+19459427[redacted]	Development	22/02/2024 02:00 PM	24
□	Tadeo	Weymouth	+12774725[redacted]	Regional Sales - Turkey	22/02/2024 01:50 PM	19
□	Kari	Brownscombe	+16039815[redacted]	Customer Support & Customer Success	22/02/2024 12:20 PM	20
□	Horatio	Kemmish	+17822509[redacted]	UX & Design	22/02/2024 12:50 PM	31
□	Norry	Bertomieu	+19721004[redacted]	Technical Product Management UK	22/02/2024 01:20 PM	50
□	Mozes	Thelwll	+16482223[redacted]	Regional Sales - UK	22/02/2024 01:00 PM	23
□	Tristan	Batie	+18114056[redacted]	Development	22/02/2024 12:30 PM	23
□	Padgett	Emney	+17655336[redacted]	Development	22/02/2024 02:40 PM	35
□	Britt	Raunds	+14908376[redacted]	UX & UI Designer	22/02/2024 01:10 PM	50
□	Elston	Guyver	+18387826[redacted]	Development	22/02/2024 02:20 PM	22

Rows per page: 10/page   1-10 of 50   < 1 2 3 4 5 >

No Response Tab:

This part lists employees who did not answer the call. Non-responsiveness could be due to various reasons and does not necessarily indicate awareness of the vishing attempt.



Vishing Report - Your bank calling to verify your most recent debit card ...

Keepnet Labs > Vishing Simulator > Vishing Campaign Manager > Vishing Report

Summary | Users | Answered | Dialed Number | **No Response**

Users who haven't answered the call
List of users who had no interaction with vhishing call

Search | Filtering Options

□	First Name	Last Name	Phone Number	Department	Call Date
□	Brita	McAloren	+18866813[redacted]	Regional Sales	22/02/2024 06:47 PM
□	Goldie	Scarborough	+11265142[redacted]	CEO	22/02/2024 06:46 PM
□	Ignace	Binnell	+17992561[redacted]	HR	22/02/2024 06:50 PM
□	Alyson	Ballam	+14297794[redacted]	Customer Support	22/02/2024 06:52 PM
□	Carmela	Merwe	+14813995[redacted]	Development	22/02/2024 06:24 PM
□	Zita	Sodo	+14171637[redacted]	Technical Product Management	22/02/2024 06:40 PM

The Importance of Vishing Simulation in Security Awareness Training

Keepnet's Vishing Simulator is important in understanding an organization's security awareness against social engineering attacks. It highlights the effectiveness of current training the need for more targeted education, and helps build a security culture and awareness.

Organizations can significantly increase their employees' preparedness against voice phishing attacks by implementing the vishing simulation.

Keepnet's Managed Vishing Test Service

Our managed Vishing Test Service offers vishing simulations to raise your team's awareness against voice phishing. Benefits include:

- **Tailored Scenarios:** Real-world challenges crafted by our experts.
- **Expert Analysis:** Detailed insights into vulnerabilities and strengths.
- **Adaptive Strategies:** Continuous updates to keep your defenses solid.

Visit our **Managed Vishing Service** page for more details.

Get Your Private Demo Session

Schedule your 30-minute private demo now!

Get Demo

You'll learn how to:

- Measure your team's awareness and preparedness against voice phishing threats.
- Identify specific areas of weakness within departments and tailor cybersecurity training accordingly.
- Create a detailed report for your management for further actions.

Legal Notice

This document, titled "2024 Voice Phishing (Vishing) Response Report," is the property of Keepnet. The information provided in this report is for general informational purposes only. All information in the report is provided in good faith. However, we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information in the report.

Authorized Use
This report is available for personal and professional use. Readers are allowed to cite, share, and reproduce the contents for educational and research purposes only, provided that Keepnet Labs is credited as the source.

Prohibited Use
You may not sell, license, rent, modify, distribute, copy, reproduce, transmit, publicly display, publicly perform, publish, adapt, edit, or create derivative works from any of the material contained in the report without prior explicit written permission from Keepnet.

Legal Action
Keepnet reserves the right to seek all remedies available by law and in equity for violations of these terms and conditions, including the right to block access from a particular Internet address to our site.

Questions and permissions requests should be addressed to:

Email: info@keepnetlabs.com