

# **Social Engineering Assessment**

Prepared for: Sample Company

**COMPLETE REPORT**

January 1st, 2026

## Sanitized Sample Report

All names, domains, phone numbers, scenarios, and results in this document are fictional and provided for sample purposes only.

## Red Sentry

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations resulting from the assessment are provided in the attached report.

Given the time-boxed scope of this assessment and its focus on client-provided Objectives only, the findings in this report should not be taken as a comprehensive listing of all security issues.

### Contact Information

+1 (888) 337-0467

[hello@redsentry.com](mailto:hello@redsentry.com)



# TABLE OF CONTENTS

---

|                                                             |    |
|-------------------------------------------------------------|----|
| TABLE OF CONTENTS                                           | 3  |
| SUMMARY                                                     | 5  |
| Project Overview                                            | 5  |
| Goals                                                       | 5  |
| Dates                                                       | 5  |
| Result                                                      | 6  |
| Assessment Scope                                            | 6  |
| Objectives                                                  | 6  |
| Out-of-Scope Activities                                     | 7  |
| Rules of Engagement & Assumptions                           | 7  |
| Authorized Testing Model                                    | 7  |
| Notification and Awareness Level                            | 7  |
| Data Handling                                               | 7  |
| Deconfliction Process                                       | 7  |
| Success Criteria                                            | 8  |
| Executive Summary                                           | 8  |
| Critical Attack Chain Demonstration                         | 9  |
| Risk Overview                                               | 9  |
| Campaign Results Overview                                   | 10 |
| Outcome by Vector                                           | 11 |
| High-Level Recommendations                                  | 11 |
| Attack Storylines                                           | 12 |
| Storyline 1: Identity Platform Migration                    | 12 |
| Storyline 2: Secure Message Notification                    | 13 |
| Storyline 3: Limited Phishing Support                       | 15 |
| Detailed Observations                                       | 16 |
| High - Vishing Pretext Led to Sensitive Process Disclosure  | 16 |
| High - Simulated Credential and MFA Prompt Interaction      | 16 |
| Medium - SMS Lures Produced Higher Engagement Than Expected | 16 |
| Medium - Reporting Channels Were Not Used Consistently      | 17 |



|                                                  |    |
|--------------------------------------------------|----|
| Low - Some Users Correctly Challenged the Caller | 17 |
| Recommendations                                  | 18 |
| Management Summary                               | 18 |
| Appendix A: Outcome Definitions                  | 19 |
| Appendix B: Sample Evidence Handling             | 19 |

# SUMMARY

---

## Project Overview

Sample Company engaged Red Sentry to assess employee susceptibility and organizational response to virtual social engineering attacks. The assessment used approved phishing, smishing, and vishing scenarios to evaluate how users respond to identity-focused lures, unsolicited phone calls, and credential or MFA simulation workflows.

The following report summarizes the scenarios executed, outcomes observed, user response patterns, reporting behavior, and recommendations for reducing social engineering risk.

## Goals

- Evaluate whether users recognize and report suspicious phone, SMS, and email-based social engineering attempts.
- Measure whether users disclose sensitive information, interact with suspicious links, or submit credentials during approved simulations.
- Assess whether escalation paths, help desk processes, and security reporting channels effectively interrupt the attack chain.
- Provide actionable recommendations for user awareness, identity protection, and process hardening.

## Dates

| Phase           | Date                             |
|-----------------|----------------------------------|
| Kickoff         | January 1st, 2026                |
| Testing Period  | January 1st to January 5th, 2026 |
| Report Delivery | January 5th, 2026                |



## Result

| Overall Rating | Summary                                                                                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Moderate Risk  | Users demonstrated strong reporting behavior in several cases, but approved scenarios also resulted in credential submission, MFA prompt interaction, and disclosure of business process details. |

## Assessment Scope

| Scope Area         | Included                                                                     |
|--------------------|------------------------------------------------------------------------------|
| Target Population  | 20 approved Sample Company personnel                                         |
| Primary Vectors    | Vishing and smishing                                                         |
| Supporting Vector  | Limited phishing support used to complete approved scenario flows            |
| Credential Capture | Simulated credential capture and MFA prompt interaction                      |
| Environment        | Remote / virtual only                                                        |
| Reporting          | Executive summary, scenario narratives, outcome metrics, and recommendations |

## Objectives

- Use an approved vishing pretext to determine whether users disclose internal process details or follow risky instructions.
- Use an approved smishing scenario to determine whether users interact with SMS-based lures.
- Use limited phishing support to simulate credential or MFA/session capture where authorized.
- Evaluate reporting behavior, including whether suspicious communications are escalated to Security or the Help Desk.
- Identify process gaps that could be abused by a real adversary.



## Out-of-Scope Activities

- Physical facility access attempts, tailgating, badge activity, or device drops.
- Malware deployment, payload execution, or destructive activity.
- Contact with anyone outside the approved target list.
- Attempts to access real production systems using captured credentials.
- Testing of emergency, legal, medical, layoff, or family-crisis pretexts unless explicitly approved.
- Repeated harassment, coercive pressure, or calls outside approved testing windows.

## Rules of Engagement & Assumptions

---

### Authorized Testing Model

Testing was conducted against an approved list of target users. The assessment team used only non-destructive techniques and avoided any contact, pretext, or data handling activity not authorized in the Rules of Engagement.

### Notification and Awareness Level

The assessment proceeded under the assumption that most targeted users were unaware of the campaign. A limited number of sponsor contacts were aware of the engagement for deconfliction and safety purposes.

### Data Handling

- No real passwords are displayed in this report.
- Simulated credential capture was configured to prevent unnecessary retention of sensitive values.
- Screenshots, call notes, and SMS evidence were sanitized before inclusion.
- Only approved campaign data was collected and used for reporting.

### Deconfliction Process

If users, Help Desk staff, Security, or other stakeholders escalated the campaign during testing, the assessment team followed the approved deconfliction process through the designated client contact. Testing could be paused if there was risk of business disruption or user distress.



# Success Criteria

| Outcome    | Definition                                                                                     |
|------------|------------------------------------------------------------------------------------------------|
| Reported   | User identified the activity as suspicious and reported it through an approved channel.        |
| Interacted | User clicked a link, replied to SMS, engaged with the caller, or followed a risky instruction. |
| Submitted  | User submitted simulated credentials, MFA code, or other sensitive information.                |
| Blocked    | Control, process, or user behavior prevented meaningful progress.                              |

## Executive Summary

Red Sentry conducted a virtual social engineering assessment to simulate identity-focused threat actor behavior using vishing, smishing, and limited phishing support. The assessment was designed to evaluate whether employees would recognize and report suspicious communication, disclose sensitive operational details, interact with SMS-based lures, or complete credential and MFA simulation workflows.

The campaign demonstrated that Sample Company has a meaningful foundation of user awareness, with several targets correctly identifying and reporting suspicious communications. However, the assessment also showed that phone-based pretexting and SMS-based lures created a higher-risk interaction pattern than email-only phishing. Multiple users engaged with the pretext, one user submitted simulated credentials, and one user interacted with a simulated MFA prompt after receiving a vishing call.

The most significant risk identified was not a single user action, but the combined attack path: a phone call created trust, a text message delivered a convincing link, and a login page simulated identity verification. This sequence mirrors modern identity-driven intrusion techniques where adversaries rely on urgency, helpful employees, and MFA fatigue rather than technical exploitation.

No destructive activity was performed, no real credentials were used to access production systems, and no physical testing was included. The assessment team recommends targeted improvements to user reporting workflows, help desk verification procedures, MFA challenge handling, and awareness training focused on phone and SMS-based attacks.



## Critical Attack Chain Demonstration

1. Vishing call established credibility using a believable IT support pretext.
2. Target confirmed internal identity process details and current MFA device type.
3. Smishing message delivered a simulated identity verification link.
4. Target interacted with the verification page and submitted simulated credentials.
5. A simulated MFA prompt was accepted, demonstrating a potential path to identity compromise.
6. The activity was not reported until after campaign completion.

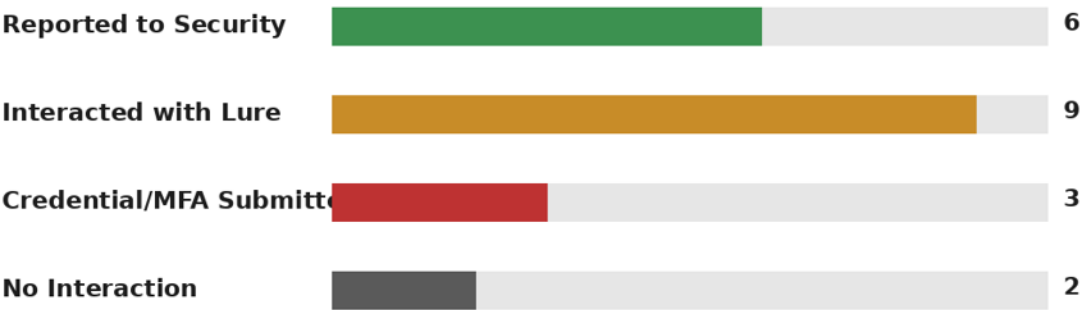
## Risk Overview

- Employees were more willing to trust phone calls than email messages.
- SMS-based follow-up increased the perceived legitimacy of the pretext.
- Some users disclosed operational details that could help an attacker refine follow-on attempts.
- Reporting behavior was inconsistent across departments.
- Existing email-awareness maturity did not fully translate to phone and SMS scenarios.

# Campaign Results Overview

The chart and tables below summarize the fictional sample outcomes for this report. In a real engagement, this section would include approved metrics such as user interaction rates, credential submission rates, MFA simulation outcomes, reporting activity, and scenario-level conclusions.

## Social Engineering Results Overview



Sample totals based on a fictional 20-person engagement. Categories may overlap depending on campaign design

Figure 1: Sample Social Engineering Results Overview

| Metric               | Result | Interpretation                               |
|----------------------|--------|----------------------------------------------|
| Targets in Scope     | 20     | Approved sample population                   |
| Reported to Security | 6      | Positive user behavior observed              |
| Interacted with Lure | 9      | Moderate susceptibility to non-email vectors |
| Credential Submitted | 1      | High-impact identity exposure scenario       |
| MFA Prompt Accepted  | 1      | Potential account compromise path            |
| No Interaction       | 2      | No meaningful engagement with the campaign   |

## Outcome by Vector

| Vector                   | Targets | Primary Outcome                                              | Business Risk                                                                           |
|--------------------------|---------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Vishing                  | 12      | Users engaged with caller, several disclosed process details | Attackers may use phone-based trust to guide users into risky actions.                  |
| Smishing                 | 10      | Users interacted with SMS lures at a higher rate than email  | SMS lures may bypass user expectations and mobile email security controls.              |
| Limited Phishing Support | 6       | One credential submission occurred after phone and SMS setup | Email or web landing pages can become more effective when paired with voice pretexting. |

## High-Level Recommendations

- Expand awareness training beyond email phishing to include vishing, smishing, MFA fatigue, QR codes, and identity platform pretexts.
- Require users to report suspicious calls and text messages through a simple, well-known channel.
- Harden help desk identity verification procedures and document what support staff will never request from users.
- Configure MFA prompts to display clear context and require number matching or phishing-resistant authentication where feasible.
- Conduct recurring but varied social engineering assessments to avoid users learning only one specific campaign pattern.

# Attack Storylines

The assessment team developed scenario storylines based on approved business contexts and target roles. Each storyline was designed to evaluate a different part of the human and process control environment without using destructive techniques or unauthorized access attempts.

| Storyline           | Vector   |                  | Objective                                                                                     | Result               |
|---------------------|----------|------------------|-----------------------------------------------------------------------------------------------|----------------------|
| Identity Migration  | Platform | Vishing/Smishing | Determine whether users follow identity verification instructions from an unsolicited caller. | Partial Success      |
| Secure Notification | Message  | Smishing         | Determine whether users interact with SMS links related to a business workflow.               | Moderate Success     |
| Document Request    | Review   | Limited Phishing | Determine whether a user interacts with a web landing page after prior pretexting.            | Blocked by Reporting |

## Storyline 1: Identity Platform Migration

The team contacted selected users using a pretext related to an identity platform migration. The caller claimed to be validating MFA enrollment after a system update. The scenario was designed to test whether users would trust an unsolicited phone call and follow up through an SMS-delivered verification link.

| Phase                 | Action                                                                          | Observed Result                                                               |
|-----------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Reconnaissance        | Reviewed approved target metadata including role, department, and phone number. | Target-specific context supported a believable pretext.                       |
| Vishing               | Called selected users using the approved IT support scenario.                   | Several users engaged and attempted to help.                                  |
| Smishing              | Sent a simulated verification link after the phone call.                        | Multiple users opened the link.                                               |
| Credential Simulation | Displayed a sanitized identity verification page.                               | One user submitted simulated credentials and accepted a simulated MFA prompt. |



## Vishing Call Notes

|                         |                                                                   |
|-------------------------|-------------------------------------------------------------------|
| <b>Target Role</b>      | Claims Operations Specialist                                      |
| <b>Pretext</b>          | Identity platform migration support                               |
| <b>Call Status</b>      | Answered                                                          |
| <b>Outcome</b>          | Target confirmed MFA device type and followed verbal instructions |
| <b>Defensive Action</b> | No help desk escalation or security report observed               |
| <b>Tester Note</b>      | Target was helpful and attempted to resolve the issue quickly     |

Figure: Sanitized vishing evidence table for sample reporting only.

*Figure 2: Sanitized Vishing Call Notes*

## Storyline 2: Secure Message Notification

The smishing scenario used a short SMS notification that appeared to reference a secure business message. The goal was to evaluate whether users would interact with a text-message link and whether they would report suspicious mobile communication.

| Observation                                                    | Impact                                                                       |
|----------------------------------------------------------------|------------------------------------------------------------------------------|
| Users interacted with SMS links more quickly than email links. | Mobile urgency may reduce the time users spend evaluating sender legitimacy. |
| Some users replied to the message before reporting it.         | Attackers may obtain additional context through conversational engagement.   |
| Reporting was inconsistent.                                    | Security teams may not receive timely visibility into SMS-based attacks.     |

## Messages

**From: Sample Company IT Support**

Hi Alex, this is IT Support. We are validating MFA enrollment after today's identity platform update.

Please confirm whether your Okta Verify app is still showing as active. Reply YES or NO.

Thanks. We sent a secure validation link. It expires shortly: [sampleco-verify.example/check](https://sampleco-verify.example/check)

YES

Figure: Sanitized smishing scenario sample. Domain and target details are fictional.

*Figure 3: Sanitized Smishing Scenario Example*

# Storyline 3: Limited Phishing Support

The limited phishing component was used only to support the approved scenario flow. It was not designed to duplicate a traditional email-awareness program. The landing page simulated an identity verification experience and did not retain real credentials.

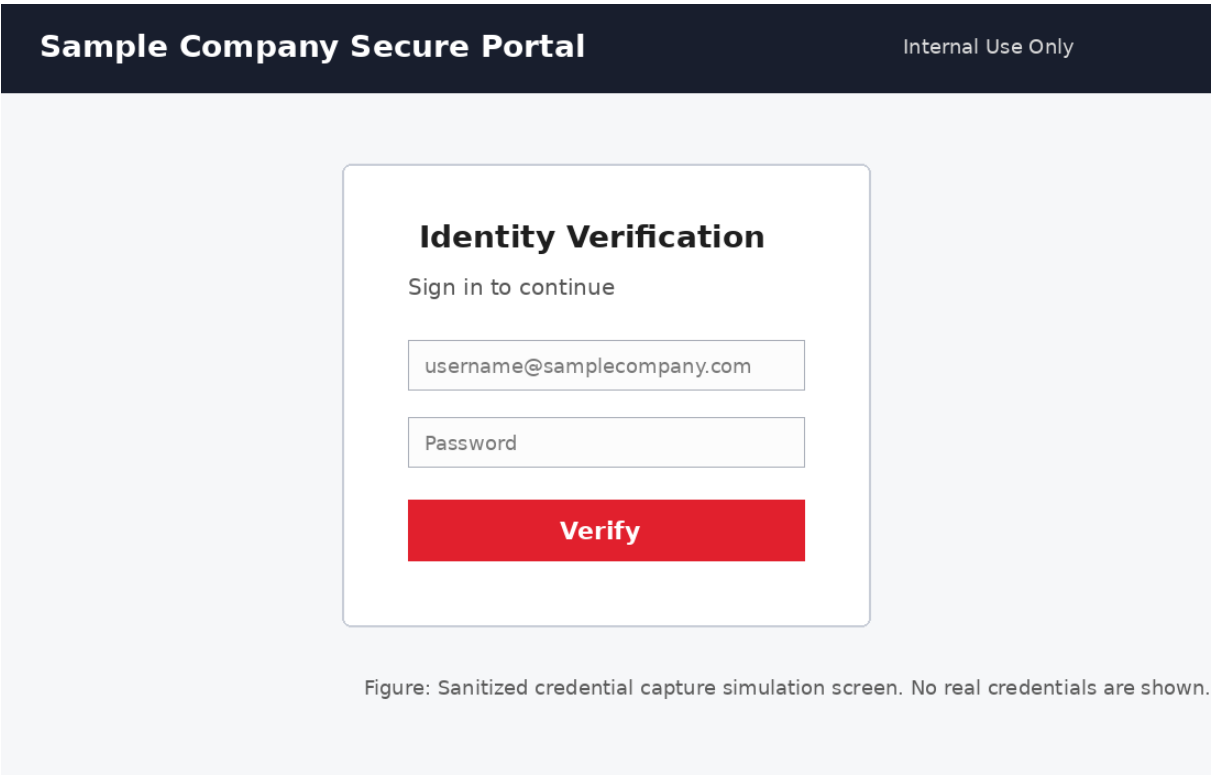


Figure 4: Sanitized Credential Capture Simulation Page

## Detailed Observations

---

### High - Vishing Pretext Led to Sensitive Process Disclosure

#### Description

Several users disclosed internal identity or support process details during phone-based pretexting. While no passwords were requested, the disclosed information could allow a real attacker to refine future social engineering attempts.

#### Business Impact

A real adversary could use this behavior to gain access to protected accounts, bypass identity controls, or gather information needed for follow-on attacks against high-value users or business processes.

#### Recommendation

Train users to treat unsolicited support calls as suspicious, publish clear verification procedures, and require callbacks through known internal numbers.

### High - Simulated Credential and MFA Prompt Interaction

#### Description

One user submitted simulated credentials after receiving a phone call and SMS verification link. The user also accepted a simulated MFA prompt, demonstrating a plausible identity compromise path.

#### Business Impact

A real adversary could use this behavior to gain access to protected accounts, bypass identity controls, or gather information needed for follow-on attacks against high-value users or business processes.

#### Recommendation

Adopt phishing-resistant MFA where possible, use number matching and context-rich prompts, and train users to deny unexpected MFA prompts.

### Medium - SMS Lures Produced Higher Engagement Than Expected

#### Description

Users appeared less skeptical of SMS links than email links, especially when the SMS followed a phone call.

### **Business Impact**

A real adversary could use this weakness to increase campaign success rates or delay detection by exploiting channels that receive less scrutiny than email.

### **Recommendation**

Include smishing in awareness content and provide a simple reporting path for suspicious texts.

## **Medium - Reporting Channels Were Not Used Consistently**

### **Description**

Some users reported the activity immediately, while others interacted with the campaign without escalation.

### **Business Impact**

A real adversary could use this weakness to increase campaign success rates or delay detection by exploiting channels that receive less scrutiny than email.

### **Recommendation**

Standardize reporting instructions and reinforce that suspicious phone calls and texts should be reported just like phishing emails.

## **Low - Some Users Correctly Challenged the Caller**

### **Description**

Several users asked the caller to verify identity or stated that they would contact internal IT through normal channels.

### **Business Impact**

This behavior reduced campaign effectiveness and demonstrated positive user awareness. Continued reinforcement is recommended.

### **Recommendation**

Recognize and reinforce this behavior in training and internal communications.

The assessment team ascribes success or failure in objective completion to a scale of business impact relevant to the client's known environment. Below is a description of each of these outcomes which can be found.

# Recommendations

Red Sentry recommends prioritizing improvements that reduce identity-driven social engineering risk and improve reporting consistency across communication channels.

| Priority | Recommendation                                                                                     | Expected Benefit                                                                 |
|----------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 1        | Implement clear verification procedures for unsolicited IT or identity support calls.              | Reduces attacker ability to use phone calls to build trust.                      |
| 2        | Expand awareness training to include vishing, smishing, MFA fatigue, and QR or mobile-first lures. | Addresses vectors not covered by traditional email-only programs.                |
| 3        | Improve MFA prompt context and consider phishing-resistant MFA for high-risk users.                | Reduces risk from credential capture and MFA prompt manipulation.                |
| 4        | Create a simple reporting process for suspicious calls and texts.                                  | Improves security team visibility into non-email attacks.                        |
| 5        | Run periodic targeted scenarios against varied departments and business workflows.                 | Prevents users from becoming trained only on repeated email templates.           |
| 6        | Review help desk and identity recovery scripts for caller verification weaknesses.                 | Improves resistance to Scattered Spider-style identity and support desk attacks. |

## Management Summary

The assessment demonstrated that non-email social engineering remains a meaningful risk even in organizations with mature phishing awareness programs. The strongest improvements will come from expanding training beyond email, strengthening identity verification processes, and making it easy for users to report suspicious calls and text messages.

## Appendix A: Outcome Definitions

---

| Outcome                   | Definition                                                                                                                                              |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Success - High Impact     | The scenario achieved an objective that could enable credential compromise, MFA bypass, sensitive data disclosure, or other meaningful business impact. |
| Success - Moderate Impact | The scenario achieved partial attacker progress but did not result in simulated credential, MFA, or sensitive business process compromise.              |
| Partial Success           | The target engaged with the scenario, but controls, reporting, or user skepticism limited the impact.                                                   |
| Blocked                   | User behavior, process controls, or technical safeguards prevented meaningful attacker progress.                                                        |
| Reported                  | The user reported the communication through an approved channel before or after interacting with the scenario.                                          |
| Not Attempted             | The assessment team did not attempt the scenario due to scope, time, or safety constraints.                                                             |

## Appendix B: Sample Evidence Handling

---

- Evidence screenshots are sanitized before inclusion in client deliverables.
- Captured credentials are masked or omitted unless the client specifically requests a controlled demonstration value.
- Phone numbers, names, email addresses, and internal identifiers are redacted where not required for remediation.
- Per-user results may be summarized or pseudonymized depending on client preference and policy requirements.