6300 Corporate Blvd. Suite 200  
Baton Rouge, LA 70809  
Phone: 225-612-2129  
[https://www.tracesecurity.com](https://www.tracesecurity.com/)

Remote Social Engineering Report

****

Client’s Name

Publish Date

TraceSecurity

## **Table of Contents**

**Table of Contents 2**

Executive Summary 3

Overview of Phone Engagement 4

Statistical Details of Phone Engagement 4

Phone Engagement Details 5

# Executive Summary

Client’s Name has just completed a Remote Social Engineering test of the operational implementation of its IT Policies and Procedures.

The key factor in a social engineering attack is confidence. If an attacker can gain an employee's confidence, then he or she has a much higher probability of success. There are two ways for an attacker to gain this confidence for a social engineering attack: by direct confrontation or by proxy. The size of your institution is best suited for a social engineering attack where employees are targeted by proxy.

TraceSecurity's social engineering engagement of Client’s Name consisted of phone calls placed to selected employees.

The phone calls are designed to try to entice employees of Client’s Name to access websites or run computer commands to simulate compromise of the network. Contact’s Name at Client’s Name, provided the TraceSecurity analyst a list of employees for testing. The analyst attempted to contact the employees, performing a total of total calls phone calls. Uncompromised employees followed company security policies and did not cooperate with the analyst. compromised employees cooperated with the analyst and followed instructions that could have led to the compromise of confidential information. unanswered phone calls were not answered. This is considered a successful vishing attack for the analyst.

During a vishing attack, remote attackers only need one employee to cooperate to achieve his or her goal. To prevent successful vishing attacks, user awareness training should be conducted on a regular basis. Employees are the first line-of-defense against these types of attacks and, as such, need to be well-trained in verifying the identity of the person calling. If an employee cannot verify the identity of a caller, the employee should ask for the caller's first and last name, a callback number, and document the caller's intentions. The employee should then provide the call information to the IT department or verify with IT that it is safe to speak with the caller.

# Overview of Phone Engagement

During the phone engagement, the TraceSecurity analyst contacted various employees of Client’s Name by phone. The phone extensions were provided by Contact’s Name and the analyst selected employees of Client’s Name to call. During the calls, the analyst attempted to trick the employees into divulging information about the organization's network. This could include IP addresses, gateways, subnet mask, and user names, to name a few. A variety of vishing techniques could have been used for this engagement. If the employee complied with the analyst’s requests, the attempt was considered successful because a real-world attacker's instructions could have misled the employee into downloading malicious code or visiting a malicious website to compromise the employee’s system.

If an actual malicious social engineering attempt occurs, it is vital that employees know how to react to these types of phone calls. Employees should be trained to verify the identity of the person calling. When caller ID information is blocked, the employees have no way of determining the identity of the caller. If caller ID is blocked, the best course of action is to ask the caller for his or her first and last name and a callback number. Employees should then verify the identity of the caller before following caller instructions or disclosing any information.

# Statistical Details of Phone Engagement

All phone numbers and extensions were provided by Contact’s Name. The TraceSecurity analyst then used these phone numbers to target the staff of Client’s Name. In total, total calls calls were placed. All these calls were intended to have employees follow the analyst's instructions to run commands on their computers.

Uncompromisedemployees were suspicious of the vishing attacks and did not comply with the analyst's requests.

compromised employees were willing to run the requested commands and assist the analyst during the vishing attack. If compromised, the employee disclosed private information and showed poor awareness of security policies.

unanswered phone calls were not answered.

The breakdown of all calls is as follows:

Vishing Campaign Results

# Phone Engagement Details