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 Email Engagement 4

Statistical Details of Email Engagement 4

Overview of Phone Engagement 5

Statistical Details of Phone Engagement 5

Email Engagement Details 6

Phone Engagement Details 7

# 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 2 exercises: phone calls placed to selected employees and the distribution of simulated malicious emails to 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.

The email exercise of the social engineering engagement is structured to entice the recipient to click on an embedded HTML link that leads to what appears to be a legitimate, secure website. Instead, the site has been specially crafted by TraceSecurity to simulate malicious third-party websites but without executing malicious code. Utilizing TraceSecurity's TracePhishing Simulator, the analyst sent a randomized assortment of previously agreed upon email templates that simulate “malicious" emails to personnel of Client’s name. The analyst created a phishing campaign and sent it to total emails employee email addresses. passed employees followed company security policies and did not click on the malicious link or attachment included in the phishing email. failed employees clicked on the malicious link or attachment included in the phishing email. This is considered a successful phishing attack for the analyst. Additionally, opened targeted email accounts downloaded images embedded in the phishing email. Downloading embedded images can indicate to an attacker that the email has been opened and can provide information to a remote attacker about valid or active email addresses.

To prevent successful phishing attacks, TraceSecurity recommends a combination of technical, administrative, and personnel controls to decrease the possibility of real-world phishing exploits. Security awareness training should be conducted on a regular basis and should address ever-evolving phishing techniques. There are also several technical features that may be used to thwart or limit an email social engineering attack. Restricting the use of HTML emails would prevent the inbound delivery of embedded images which could be used for malicious attacks. Configuring emails to open HTML links in Restricted Zones is a desktop or group policy feature, which may be used to help defend against some attacks by limiting the user-initiated connection features. Additionally, firewall egress filtering that validates the website address with the true DNS record may help to control the user-initiated connection.

# Overview of Email Engagement

The analyst began remote social testing of Client’s name's employees and systems on testing date. The TraceSecurity analyst utilized specially crafted emails that are similar to successful real-world phishing attacks. The embedded links direct users to websites that simulate the methods that malicious attackers utilize to compromise employee workstations. By having users click on the links within the emails, the users initialize connections to malicious entity and bypass firewall protections. The significance of establishing a connection is that it enables the attacker to inject code on the user’s workstation allowing it to be used as a remote attack platform. This connection would subvert the firewall to allow access into Client’s name's network.

The TracePhishing application records the user’s first name, last name, email address, whether the user viewed embedded images (i.e. “opened” the email), whether the user failed the test, and the failed date if applicable.

In addition, an embedded image was also included in the email. To view the image, the email client downloads it from an external website. Commonly-used email clients often disable this functionality and instead require the end user to choose to download the image. There are two primary risks associated with downloading these types of images. The first, more popular risk is information disclosure. When the image is viewed, the website that the image is received from tracks the email address that requested the download as well as the IP address and web browser information. This is often used by spammers to validate real email addresses and associate them to company names. The second risk is present within the email client itself if automatic image downloading is enabled. Email clients contain vulnerabilities that allow them to connect to a website and download an image automatically. This can lead to immediate compromise with malicious software. While patches are constantly being released for all known issues, a new vulnerability could be discovered and exploited at any time. Therefore, TraceSecurity recommends that images are never downloaded via email unless users can verify the identity of the sender, the content to be downloaded, and that the email was sent through a secure channel.

# Statistical Details of Email Engagement

Contact’s name provided the TraceSecurity analyst with a list of employee emails. The TraceSecurity analyst then used the email address dataset to target the selected Client’s name's email addresses.

The statistical breakdown is as follows:

Phishing Campaign Results

# 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

# Email Engagement Details

# Phone Engagement Details