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

Email 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 the distribution of simulated malicious emails to employees.

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 Choose an item 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

# Email Engagement Details