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

****

test

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

test 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 test 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 test to access websites or run computer commands to simulate compromise of the network. testt at test, provided the TraceSecurity analyst a list of employees for testing. The analyst attempted to contact the employees, performing a total of 40 phone calls. 9 employees followed company security policies and did not cooperate with the analyst. 1 employees cooperated with the analyst and followed instructions that could have led to the compromise of confidential information. 30 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 test. The analyst created a phishing campaign and sent it to 20 employee email addresses. 19 employees followed company security policies and did not click on the malicious link or attachment included in the phishing email. 1 employees clicked on the malicious link or attachment included in the phishing email. This is considered a successful phishing attack for the analyst. Additionally, 2 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 test's employees and systems on 1/2/2019. 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 test'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

testt provided the TraceSecurity analyst with a list of employee emails. The TraceSecurity analyst then used the email address dataset to target the selected test'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 test by phone. The phone extensions were provided by testt and the analyst selected employees of test 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 testt. The TraceSecurity analyst then used these phone numbers to target the staff of test. In total, 40 calls were placed. All these calls were intended to have employees follow the analyst's instructions to run commands on their computers.

9employees were suspicious of the vishing attacks and did not comply with the analyst's requests.

1 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.

30 phone calls were not answered.

The breakdown of all calls is as follows:

Vishing Campaign Results

# Email Engagement Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Email | Clicked at | Opened at | First Name | Last Name | Email Template |
| ccobos@pnb.com |  |  | Cesar | Cobos | E-Card |
| jmartin@pnb.com |  | 8/3/2018 16:18 | Jose | Martin | New LinkedIn Message |
| yvilleda@pnb.com |  |  | Yvette | Villeda | Shared Google Drive File |
| gcastro@pnb.com |  |  | Gabriel | Castro | E-Card |
| ogonzalez@pnb.com |  |  | Orestes | Gonzalez | Shared Google Drive File |
| cfranzitta@pnb.com |  |  | Cristin | Franzitta | E-Card |
| wbermudez@pnb.com |  |  | Wilmer | Bermudez | E-Card |
| jinfante@pnb.com |  |  | Jose Miguel | Infante | E-Card |
| avelez@pnb.com |  |  | Alex | Velez | E-Card |
| ralbuja@pnb.com |  |  | Fausto | Albuja | E-Card |
| jrivera@pnb.com |  |  | Jesslin | Rivera | Shared Google Drive File |
| mwax@pnb.com |  |  | Moshe | Wax | Shared Google Drive File |
| kalvear@pnb.com |  |  | Ketty | Alvear | New LinkedIn Message |
| matesiano@pnb.com | 8/3/2018 10:36 | 8/3/2018 10:35 | Millie | Atesiano | E-Card |
| yalvarez@pnb.com |  |  | Yaima | Alvarez | E-Card |
| abrito@pnb.com |  |  | Ada | Brito | New LinkedIn Message |
| ocambrelen@pnb.com |  |  | Otoniel | Cambrelen | Shared Google Drive File |
| vcardenas@pnb.com |  |  | Viviana | Cardenas | New LinkedIn Message |
| tplaza@pnb.com |  |  | Tere | Plaza | E-Card |
| isolveyra@pnb.com |  |  | Ignacio | Solveyra | New LinkedIn Message |

# Phone Engagement Details

|  |  |  |  |
| --- | --- | --- | --- |
| Final Result | Name | Phone | Extension |
| PASSED | Alex Velez | 305-539- 7533 |  |
| Dates: 8/17/2018 | | | |
| Description: Analyst called in as Paul with Jack Henry & Associates. Analyst told the user that he was working with Richard Laguardi on some Jack Henry update issues. Analyst asked the user if he had a moment, and user confirmed he did. Analyst asked the user if he had experienced any issues with his Jack Henry software. User told the analyst that his software was working fine. User then asked the analyst to hold on, so he could talk to Richard. Analyst terminated the call while on hold. | | | |
| Final Result | Name | Phone | Extension |
| PASSED | Alexandra Silva | 305-539-7679 |  |
| Dates: 8/22/2018, 8/17/2018 | | | |
| Description: The analyst called in as Jack Henry & Associates who had a support ticket from Richard Laguardi. The analyst told the user that some of the Jack Henry software was having issues reaching the Pacific National Bank network. Therefore, the analyst was trying to identify where the issue was. The analyst asked the user to open a web browser and go to speedtest.net. The user asked the analyst for the name and phone number of the analyst, because they needed to call the IT department and verify this information. The analyst provided their contact information, and terminated the call. | | | |
| Final Result | Name | Phone | Extension |
| PASSED | Carmen Marchan | 305-539-7572 |  |
| Dates: 8/17/2018 | | | |
| Description: Analyst called in as Paul with Jack Henry & Associates. Analyst told the user that he was working with Richard Laguardi on some network issues, and asked the user to good to speedtest.net. User was confused what the analyst was asking him to do. Analyst told the user that some of the Jack Henry updates were having issues reaching the network, so the analyst was trying to identify where the problems were. The user told the analyst that he couldn't help him, and the analyst would have to talk to IT to do any network testing. User took down the analyst name and number to give to IT regarding the Jack Henry update issue. | | | |
| Final Result | Name | Phone | Extension |
| PASSED | Daniel Cassis | 305-539-7503 |  |
| Dates: 8/17/2018 | | | |
| Description: Analyst called in as Paul with Jack Henry & Associates. Analyst told the user that he was working with Richard Laguardi, and they were doing some network testing due to some Jack Henry software update issues. User told the analyst that Richard was already out of the office for the day, so he could see if there was anyone else in IT that could help the analyst. The analyst told the user that he had already spoken to Richard earlier that week, and Richard gave the analsyt a list of employees to call. The analyst was to use this list to find out where the exact problem is in the network since it wasn't just an IT issue. User asked the analyst to hold on so he could atleast verify this info with someone in IT. Analyst terminated the call while on hold. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Final Result | Name | Phone | Extension |
| PASSED | Gina Zenck | 305-539-7588 |  |
| Dates: 8/24/2018 | | | |
| Description: The analyst called in as Paul with Jack Henry & Associates. The analyst told the user that they had a support ticket from Richard Laguardi regarding Jack Henry software updates that were not reaching the Pacific National Bank network. Therefore, the analyst was trying to identify were the issue was. The user told the analyst to hold on while they transfer the analyst to Richard. While being transferred, the analyst terminated the call. | | | |
| Final Result | Name | Phone | Extension |
| PASSED | Gloria Alvarado | 305 539-7514 |  |
| Dates: 8/24/2018 | | | |
| Description: The analyst called in as Paul with Jack Henry & Associates. The analyst told the user that they had a support ticket from Richard Laguardi regarding some Jack Henry software that was having issues reaching the Pacific National Bank network. The user asked the analyst if they wanted to talk to Richard. The analyst stated that Richard gave the analyst some employees to call to see who recieved the update and who did not. The analyst asked the user if they have had any issues with their Jack Henry software. The user stated that their Jack Henry had been working fine. The analyst asked if the user had a quick moment to help the analyst even though they hadn't experienced any issues. The user said they were willing to help, so the analyst asked the user to go to speedtest.net. The user then asked the analyst to hold on. While on hold, the analyst terminated the call. | | | |
| Final Result | Name | Phone | Extension |
| PASSED | Julio Soto | 305-539-7593 |  |
| Dates: 8/24/2018 | | | |
| Description: The analyst called in as Paul with Jack Henry & Associates. The analyst told the user that he had a support ticket from a Richrad Laguardi regarding Jack Henry software that was having issues reaching the Pacific National Bank network. The analyst asked the user if he had experienced any issues with his Jack Henry software. The user stated that their software was working fine. The analyst asked the if the user still had a moment to help the analyst out. The user stated that the analyst should call Richard about software issues. The analyst told the user that they had spoken to Richard earlier that week, and Richard gave the analyst a couple employees to call to find where the problem is since some employees would reach the update and other would not. The user understood and asked the analyst to hold on while they call Richard and verify this info. While on hold, the analyst terminated the call. | | | |
| Final Result | Name | Phone | Extension |
| PASSED | Maria Lopez | 305-539-7658 |  |
| Dates: 8/24/2018 | | | |
| Description: The analyst called in as Paul with Jack Henry & Associates. The analyst told the user that he had a support ticket from Richard Laguardi regarding Jack Henry software having issues reaching the Pacific National Bank network. Therefore, the analyst was trying to identify where the problem was. The analyst asked the user if they had any issue with their Jack Henry software. The user stated that everything was working fine. The analyst asked the user if they would go to speedtest.net. The user asked if that was on the web. The analyst confirmed that it was. The user started typing and then asked the analyst to hold on. While on hold, the analyst terminated the call. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Final Result | Name | Phone | Extension |
| PASSED | Martha E. Calderon | 305 539-7620 |  |
| Dates: 8/24/2018 | | | |
| Description: The analyst called in as Paul with Jack Henry & Associates. The analyst told the user that they had a support ticket from Richard Laguardi regarding Jack Henry software that was having issues reaching the Pacific National Bank network. Therefore, the analyst was trying to identify where the issue was. The user told the analyst that they should talk to Richard about this since he is in IT. The analyst stated that they had spoken to Richard who gave them the user name, because she didn't have the recent update. Therefore, the analyst was trying to figure out why. The user asked the analyst to hold on while she called Richard to verify this information, because she doesn't get these kinds of calls. While on hold, the analyst terminated the call. | | | |
| Final Result | Name | Phone | Extension |
| FAILED | Freddy Zeron | 305-539-7622 |  |
| Dates: 8/24/2018 | | | |
| Description: The analyst called in as Paul with Jack Henry & Associates. The analyst told the user that he had a support ticket from Richard Lagaurdi regarding Jack Henry software updates that couldn't reach the Pacific National Bank network. The analyst asked the user if he had any issues with his Jack Henry software this week. The user stated that his software was working fine. The analyst asked the user if they could help by going to speedtest.net. The user asked the analyst if he had spoken to Richard today. The analyst stated that they had spoken to Richard earlier in the week, and he was trying to identify where the exact problem is beacuse some employees recieved the update but others were not. The user complied and ran a speed test. The analyst then asked the user for the download speed: 89.62 Mbps, the upload speed: 13.55 Mbsp, the ISP: FiberNet Direct, and the IP Address: 74.120.43.132. The analyst thanked the user for their time and terminated the call. | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Alex Roca | 305-539-7512 |  |
| Dates: 8/24/2018, 8/22/2018, 8/17/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Andres Restrepo | 305-539-7676 |  |
| Dates: 8/24/2018, 8/17/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Carolina Reyes | 305-539-7511 |  |
| Dates: 8/24/2018, 8/17/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Danny Martin | 305 539-7564 |  |
| Dates: 8/24/2018, 8/17/2018 | | | |
| Description: | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Derek Yanez | 305-539-7612 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Felix Garcia | 305-539-7668 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Francia Morales | 305-539-7555 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Francis Gallegos | 305-539-7577 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Gerry Zambrana | 305-539-7671 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Gustavo Melendez | 305 539 7571 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | James Partridge | 305-539-7520 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Jenny Villamar | 305-539-7595 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Josefina Garcia | 305-539-7599 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Josephine Colon | 305 539-7603 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Kyle Sexton | 305-539-7557 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Lucy Nuñez | 305-539-7684 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Marcela Viales | 305-539-7618 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Marcella DeJesus | 305-539-7608 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Marta Perez-Pendas | 305-539-7589 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Mercedes Santiesteban | 305-539-7522 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Patricia Gilbert | 305-539-7540 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Polo Gross | 305-539-7552 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Ricardo Gonzalez | 305-539-7518 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |
| Final Result | Name | Phone | Extension |
| NO ANSWER | Ricardo Morales | 305-539-7675 |  |
| Dates: 8/24/2018 | | | |
| Description: | | | |