

**PO Box 62, Brooklyn, PA 18813 | 800.956.6065 |** [**www.social-engineer.com**](http://www.social-engineer.com/)

LEONARDO MONTANO

XXXXXXXX

XXXXXXXXXXXX

Police Officer

[Xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Frank.Valdez@SIERRAVISTAAZ.GOV)

**Prepared by Social-Engineer, LLC**

LEONARDO MONTANO | lemontano@XXXXXXX.edu

**Table of Contents**

[Executive Summary 4](#_Toc152878237)

[OSINT (OPEN-SOURCE INTELLIGENCE) 5](#_Toc152878238)

[Phishing 7](#_Toc152878239)

[Level 1 Phishing Findings 7](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878240)

[Level 1 Operating Systems Detected 8](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878241)

[Level 2 Phishing Findings 9](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878242)

[Level 2 Operating Systems Detected 11](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878243)

[Phishing Recommendations 13](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878244)

[Vishing 14](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878245)

[Vishing Findings 14](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878246)

[Vishing Analysis 15](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878247)

[Vishing Recommendations 16](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878248)

[Conclusion 17](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878249)

[About Social-Engineer, LLC 18](file:///C:\Users\leomo\OneDrive\Documents\UofA%20Class\CYBV%20481\Finish%20Reports\MontanoL_Frank_Valdez_SE_Report.docx#_Toc152878250)

# Executive Summary

This report provides the results of the DECEMBER 2023 social engineering assessment conducted by Social- Engineer, LLC (SECOM) for XXXXXXXXXXXX CITY EMPLOYEES. The purpose of this ongoing assessment is to determine COMPANY’s vulnerabilities to human-based attacks using phishing, spear phishing, and vishing attack vectors.

Particularly on this target Xxxxxxxxxxxx is a police officer who works at a school. I was giving certain information about the target, which was the phone number and email address. I was able to find out during the open-source intelligence phase about what XXXXX does and where he works. There was little information on XXXXX, but I was able to get a PRETEXT to try and lure him in. I noticed that XXXXX likes to be a part of fundraisers. I called XXXXX twice but was sent to his voicemail and sent a total of three emails. Two of the emails were about a fundraiser and the third email was about a FedEx delivery. I decided to go with the delivery method since we are in the month of December and most people do online shopping.

According to Lucy, which is our phishing software XXXXX did not click on any of the fundraiser phishing emails. Unfortunately, XXXXX clicked on the FedEx email from various sources according to our software.

# OSINT (OPEN-SOURCE INTELLIGENCE)

**Executive Summary**

Google Search: "Xxxxxxxxxxxx" AND "Xxxxxxxxxxxx"

Results: [https://www.linkedin.com/in/XXXXX-valdez-69806a3a](https://www.linkedin.com/in/frank-valdez-69806a3a)

Information Found: LinkedIn Profile

POSSIBLE PRETEXT: Talk to him about volunteering at a youth sports complex in Xxxxxxxxxxxx to raise awareness in drugs.

Google Search: "Xxxxxxxxxxxx" AND "Xxxxxxxxxxxx"

Results: [https://www.google.com/search?sca\_esv=579478752&sxsrf=AM9HkKkkPFNBNiiPR1KRiSefDSF2dlLA7A:1699117170463&q=%22XXXXX+Valdez%22+AND+%22Sierra+Vista%22&tbm=isch&source=lnms&sa=X&ved=2ahUKEwiP-oHb6KqCAxVSnWoFHRv6BcUQ0pQJegQICRAB&biw=1278&bih=1277&dpr=1#imgrc=pKRhaqBUEIJ0GM](https://www.google.com/search?sca_esv=579478752&sxsrf=AM9HkKkkPFNBNiiPR1KRiSefDSF2dlLA7A:1699117170463&q=%22Frank+Valdez%22+AND+%22Sierra+Vista%22&tbm=isch&source=lnms&sa=X&ved=2ahUKEwiP-oHb6KqCAxVSnWoFHRv6BcUQ0pQJegQICRAB&biw=1278&bih=1277&dpr=1#imgrc=pKRhaqBUEIJ0GM)

Information Found: PIC

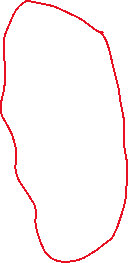


LinkedIn Search: Xxxxxxxxxxxx

Results:[https://www.linkedin.com/in/XXXXX-valdez-69806a3a/recent-activity/reactions/](https://www.linkedin.com/in/frank-valdez-69806a3a/recent-activity/reactions/)

Information Found: PIC





Google Search: “"Xxxxxxxxxxxx" AND "Xxxxxxxxxxxx"

Results:

Information Found: HQ Phone

xxxxxxxxxxxx

# Phishing

To simulate the actions of potential attackers, SECOM employs a social engineering technique called phishing, or sending unsolicited emails to recipients to influence them into clicking an attachment containing malware or a malicious link. Most commonly, the link will lead to a website that will collect network credentials or load malicious software.

The purpose of SECOM phishing emails is twofold. First, SECOM can record and analyze employees’ response to a potential attack by collecting statistics (including total emails sent, number of recipients who clicked a potentially malicious link, number of recipients who reported receiving the email, and other data of interest).

Second, if recipients click a link in one of the phishing emails, they are routed to an internal landing page. This landing page explains how they could have identified a specific phish and how their organization wishes for them to respond. By repeating this process with the population and analyzing the data collected, SECOM can determine the effectiveness of training over time.

## Level 1 Phishing Findings

The first phishing email that I sent out to Xxxxxxxxxxxx was about a Fundraiser. There was a total of two emails sent from [leo.d@sierravistaz.com](mailto:leo.d@sierravistaz.com). One email sent on 11/27/2023 to email address [Xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Frank.Valdez@SIERRAVISTAAZ.GOV). Below on Figure 1.1 is what the email looked like. XXXXXXXXXXXXXX

Figure 1.1

A close-up of a text

Description automatically generated

### Level 1 Operating Systems Detected

The email was opened via Windows operating system on Chrome 117 from IP address of XXXXXXXXXXXXXXminutes after sending. When investigating the IP address, I noticed that it had belonged to Cisco. That indicated that the email was opened from a security measure standpoint and not the user. I had to send another email. I sent another email from the same email and PRETEXT but there was no click not even from a CISCO server.

## Level 2 Phishing Findings

For the second Phishing Attempt I decided to go with a notification from FedEx. Since we are in the middle of the holiday season, I assumed that he could have ordered something online. According to Lucy the user clicked on the email eighteen separate times from different IP addresses. As shown below on Figure 2.1 you can notice the different web browsers and IP addresses. The campaign started on 12/05/2023 at 13:06 and the first click registered at 13:27 on 12/05/2023.

Figure 2.1

A screenshot of a computer

Description automatically generated

Below on Figure 2.2 is the email that was sent to XXXXX to email address [Xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Frank.Valdez@SIERRAVISTAAZ.GOV).

Figure 2.2

A screenshot of a mail

Description automatically generated

### Level 2 Operating Systems Detected

The following operating systems were used to click on the phishing email shown on figure 2.2. Windows, IOS, and LINUX. The browsers that were used to also click were Chrome, Edge, Firefox, Chrome Mobile IOS, and Internet Explorer 10. The figures below are going to show the clicks with the different operating systems as well as the number of clicks.

Figure 2.3

*A screenshot of a computer

Description automatically generated*

Figure 2.4

A screenshot of a computer

Description automatically generated

## Phishing Recommendations

Overall, 33.33% of emails that were sent were clicked. 1 of 3 emails succeeded. My recommendation for this user is to make sure to verify tracking information before clicking a link. Go to the website or email that was first originally sent to target when the order was placed. Make sure the user is attending or completing annual cyber awareness training and let the user know about the different phishing spams that are out there especially during the holiday season.

# Vishing

Attackers often elicit information via the telephone, called “vishing,” to further develop their attacks. It is important for a company to be aware of the amount of information employees provide to unconfirmed callers, whether intentionally or not.

## Vishing Findings

Attempted to contact Target using different phone numbers. One of the phone numbers that was used was XXXXXXXXXXXXfor Leonardo Dominguez. Target did not answer the phone and was sent to voicemail. That attempt was for fundraiser PRETEXT of the Phishing email. The second PRETEXT was for the delivery from FedEx. The phone number that was used for this was XXXXXXXXXXXX. I also got a voicemail but this time I left a message stating who I was and that a package was being held at our location in Xxxxxxxxxxxx. I also mentioned that I sent an email and to look for an email from Jake Flanagan. The number that was called was XXXXXXXXXXXXX. The UID to the different calls are d10c23d3-ae17-4fb7-b745-dc2d9ec1965d and ce338cf1-d7c6-49bd-9952-aeaf7c947d23.

**SEVERITY**: **LOW**

The following pretext(s) were used during the vishing campaign:

* Call from Leonardo Domiguez to discuss a fundraiser for Children who do not have gifts this season.
* Call from Jake Flanagan to let user know that a FedEx package was being held at our Location in Xxxxxxxxxxxx.

The following tables are summaries of employee performance.

|  |  |
| --- | --- |
| **SUMMARY** | |
| Number of calls attempted | **2** |
| Number of individuals contacted | **1** |
| Number of compromises | **0** |
| Number of Employee IDs elicited | **0** |
| Number of last 4 of SSN elicited | **0** |
| Number of Emails elicited | **0** |

*Table 1: vishing summary*

## Vishing Analysis

The overall result was that the user did not answer a phone call from an unrecognized number. I am not sure if the Targets job is to answer phone calls since he does work at a school and as a Police officer. Could have not answered since we are in the holiday season and could be on vacation.

## Vishing Recommendations

Although the user did not answer the phone and I was sent to voicemail. A recommendation I can make is to always verify who is calling and make sure to not give out too much information when talking over the phone. Always make sure to report the call to the CISO if it seems strange or feels strange.

# Conclusion

These tests are meant to catch the vulnerabilities of humans. The phishing and vishing attacks that were performed on the target were meant to raise awareness especially during the holiday season. There were multiple emails sent out to the target and the one that succeeded was the delivery email from FedEx. Target did not answer any calls, so I was not able to try and obtain information about other employees or the resources within the company. Unfortunately, all you need is just one click and by the looks of the third email it was clicked eighteen times from multiple operating devices, browsers, including a mobile device.

Ensuring the employee is exposed to cyber security awareness is crucial to maintain a good healthy environment according to this report. The goal of these tests is to make sure that the company raises awareness, saves embarrassment, and prevents financial ruin. Should you have any questions, require additional reporting data, or wish to discuss further, please do not hesitate to contact us directly. XXXXXXXXXXXXXXXXXXXXXXXXX looks forward to a continuing partnership with the city of Xxxxxxxxxxxx.

# About Social-Engineer, LLC

Social-Engineer, LLC is the premier consulting and training company specializing in the art and science of social engineering (SE). Social tactics are an established and quickly growing trend in information security in the forms of phishing, phone elicitation (vishing), and impersonation.

With more than three decades of combined experience, Social-Engineer, LLC assists organizations in government, law enforcement, and the private sector in detection and mitigation of the devastating effects of both physical and information breaches. Social-Engineer, LLC focuses on the abilities of a hostile attacker to exploit the human element of businesses to gain access to corporate assets. Through assessment, education, and training, Social-Engineer, LLC helps organizations protect themselves and their trade secrets. To learn more about professional social engineering, services please visit: <http://www.social-engineer.com/social-engineering-services/>