Social Engineering Assessment Report

Virginia Bankers Association
Glen Allen, Virginia

Performed:
February - March 2025

Prepared by:
SBS CyberSecurity's
Network Security Team

The information contained in this report was derived from proprietary data provided by:
Virginia Bankers Association - Glen Allen, Virginia

Table of Contents

Executive Summary **3**
Purpose **3**
Assessment Scope **3**
About This Assessment **3**
Methodology **4**
Results Analysis **5**
Previous Social Engineering Assessment (March 2024) **6**
Peer Comparison Results **7**
Findings and Recommendations **8**
Phishing Email Assessment 8
Pretext Phone Call Assessment 9
Appendix **10**

Executive Summary

A review of Virginia Bankers Association's security controls resulted in no major findings or recommendations, because no sensitive or confidential information was exposed. This indicates Virginia Bankers Association understands the importance of protecting the confidentiality of sensitive information. SBS CyberSecurity suggests that additional employee training should be offered to improve awareness of social engineering techniques and appropriate responses. The assessments performed are useful examples to include in Security Awareness training. Employees should be reminded that people will prey on their eagerness to provide excellent service to obtain sensitive information. The implementation of these recommendations is solely at the discretion of the Virginia Bankers Association's management department.

Please contact SBS CyberSecurity with any questions concerning this assessment.

Purpose

Social engineering is a non-technical method of intrusion used by hackers and attackers that relies heavily on human interaction. Social engineering often involves enticing employees into breaking normal security procedures. As such, it is one of the greatest threats that Clients today encounter. Social Engineering preys on qualities of human nature, such as the willingness to be helpful, the tendency to trust people, and the desire to perform job tasks successfully. The purpose of the Social Engineering Assessment is to protect Virginia Bankers Association's information by testing employees and business processes against common social engineering attacks.

Assessment Scope

The following assessments were conducted to identify weaknesses in the organization's security and employee awareness: Phishing Emails, Pretext Vendor Calls. The results of these assessments, including scope, findings, and recommendations of each test, are detailed below.

About This Assessment

This Social Engineering Assessment was performed at the request of Virginia Bankers Association in Glen Allen, Virginia on February 2025, by the Network Security Team for SBS CyberSecurity, LLC of Madison, SD. The Network Security Team consists of individuals who hold the following industry recognized certifications: Certified Penetration Tester (CPT), Certified Ethical Hacker (CEH) and Security+. This assessment was overseen by Justin Curtner, Information Technology Auditor for SBS CyberSecurity, LLC of Madison, SD. Justin has 8 years of experience in business operations and security. Justin has received his Bachelor of Science in Business Administration from Arkansas State University and is a Certified Community Banking Security Professional (CCBSP).

This Social Engineering Assessment was developed and performed to assist Virginia Bankers Association in improving and maturing the institute's security posture. It is at the discretion of Virginia Bankers Association to determine the relevance and order of importance of these findings herein. The findings are not requirements, and the implementation of recommendation(s) is solely at Virginia Bankers Association's discretion. SBS CyberSecurity assures the accuracy of this documentation to the best of its ability.

Methodology

SBS CyberSecurity has adopted the following methodology for conducting Social Engineering Assessments to ensure thorough and consistent results. Applicable documentation is included to support the findings of this report.

Pre-Engagement Interaction

The aim of this phase of the social engineering test is to define overall scope of the assessment. During this phase, the client will need to answer several questions in order to properly estimate the engagement scope. These may include (for example): amount and which email addresses will be tested, which type of calls will be performed, which employees are to be targeted, which branches will be tested. These details will be verified with the client during this initial phase of the social engineering test.

Information Gathering

In the information gathering (reconnaissance) phase of the Social Engineering Test, publicly available databases and sources are searched for information about the target. This information includes items such as address, email addresses, employee names, phone numbers, internal technologies, and contracted vendors. This information is used throughout the social engineering assessment.

Develop Attack Vectors

At the conclusion of the information gathering phase, the social engineers will then develop a method of attack that has the highest chance of success. This may include results from previous assessments, information gathering, or known possible weaknesses at the Client.

Launch Attack

The attack process attempts to take advantage of employees' trusting nature using methods identified during the previous phases. Successful attacks may result in unauthorized system access, internal network information, customer account information, access to employee credentials, and possibly other forms of information.

Reporting

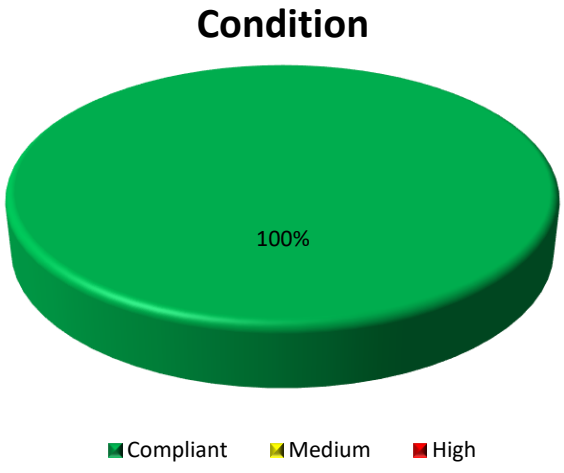
The final phase of the social engineering test will provide the client with details and analysis regarding the test results. The report will contain all of the key components, including: executive summary, purpose of the test, scope of the test, test history result comparison, peer comparison, identified finding and their impact, and remediation suggestions.

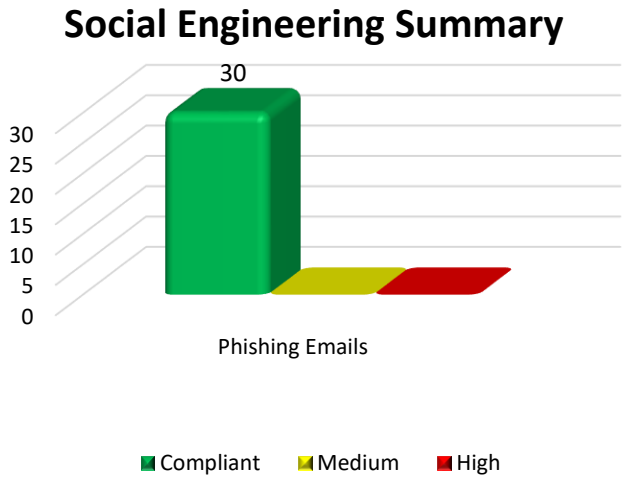
Results Analysis

February 2025 Social Engineering Assessment

The SBS Network Security Team assessed both the internal and external security controls at Virginia Bankers Association.

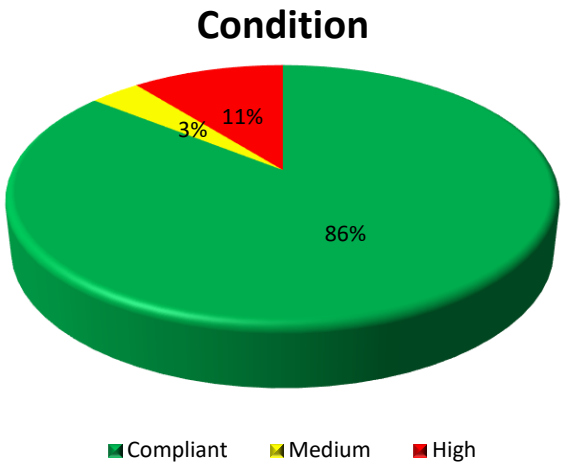
- Phishing Emails: Out of the thirty (30) email addresses that received the phishing email, no employees visited the website, therefore no sensitive information was submitted.
- Pretext Vendor Calls: Out of three (3) attempts made by a social engineer to retrieve internal network information, all employees denied releasing internal network information to the social engineer due to proper verification methods and employee training.

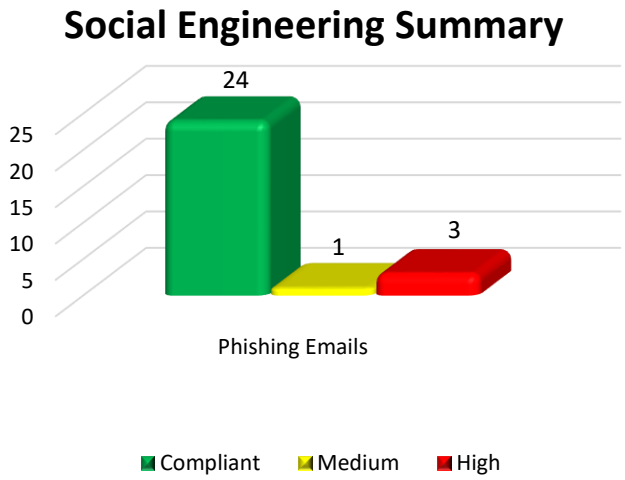




Previous Social Engineering Assessment (March 2024)

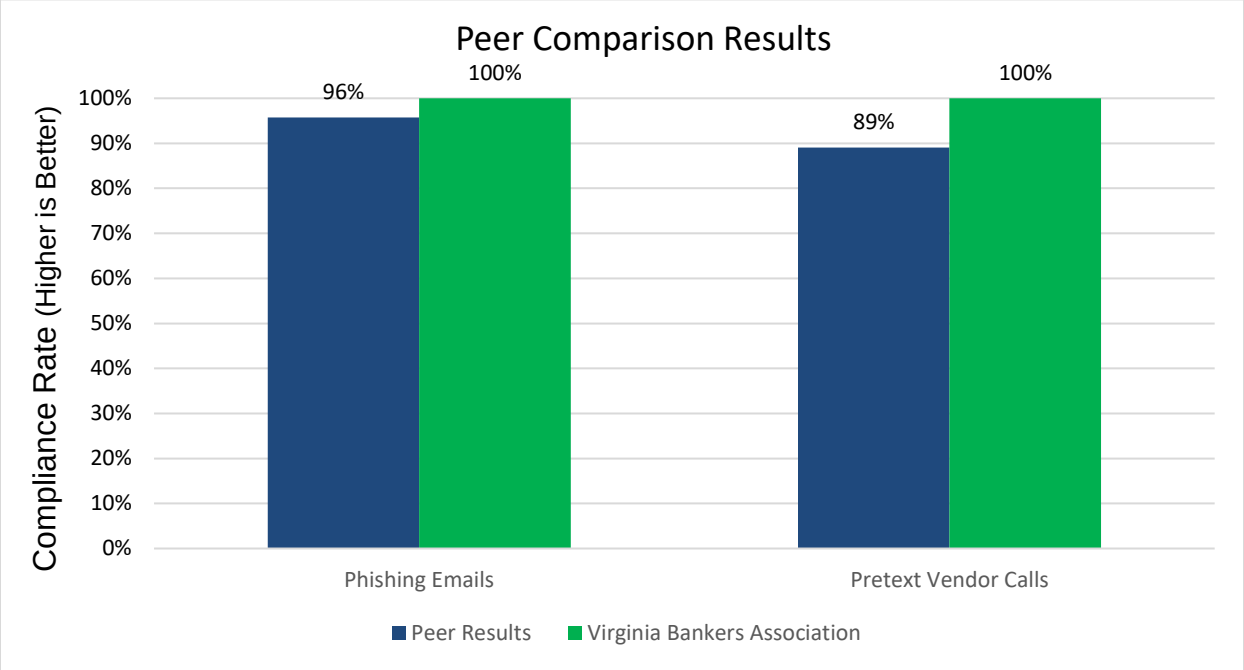
Although the two reports are not directly comparable, we can conclude that it is very important for the Client to continue Security Awareness Training and stress the importance of the protecting sensitive and confidential information and the threat of social engineering.





Peer Comparison Results

The following chart compares Virginia Bankers Association's assessment results with results from other Clients within the same peer group. Peer groups are defined by Client's asset size.

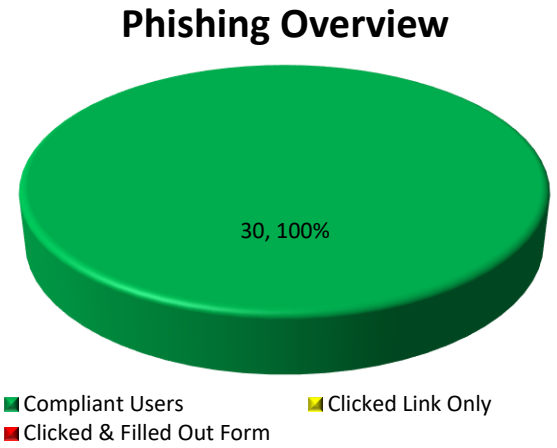


Findings and Recommendations

Phishing Email Assessment

Scope:
On February 28th, 2025, a phishing email was sent to thirty (30) email accounts belonging to Virginia Bankers Association. Phishing is the criminally fraudulent process of acquiring sensitive information such as usernames, passwords, and credit card details by posing as a trustworthy website whose URL and appearance are often nearly identical to a legitimate site. Phishing is typically carried out by email or instant message and often directs users to enter confidential information. Additionally, clicking on email links may direct a user to a website with embedded malicious software that could compromise a workstation, or provide additional information about the workstation, operating system, and potential vulnerabilities.

The phishing email was designed to entice employees to visit a malicious website (*see Appendix A and Appendix B*). The website had an option to enter account information to log into the website. SBS CyberSecurity recorded visits and attempts to log into the website.

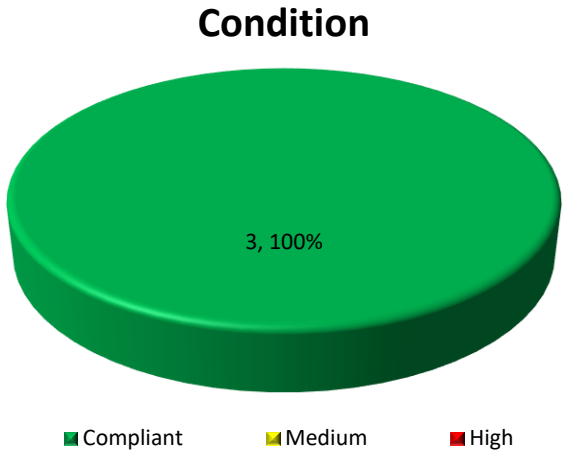


Finding:
Out of the thirty (30) email addresses that received the phishing email, no employees visited the website, therefore no sensitive information was submitted.

Recommendation - Low:
Current employee training and detection procedures are compliant; however, Virginia Bankers Association should continue to education and test employee's aptitude for dealing with social engineering attacks.

Pretext Phone Call Assessment

Scope:
During the Pretexting Assessment, Virginia Bankers Association employees were contacted by a social engineer via telephone. During the telephone call, an invented scenario (known as the pretext) was used to convince an employee of the Client to release confidential information or perform a series of tasks. On March 12th, 2025, a social engineer made a series of calls to the Client impersonating a Virginia Bankers Association third party employee (*see Appendix C and Appendix D*).



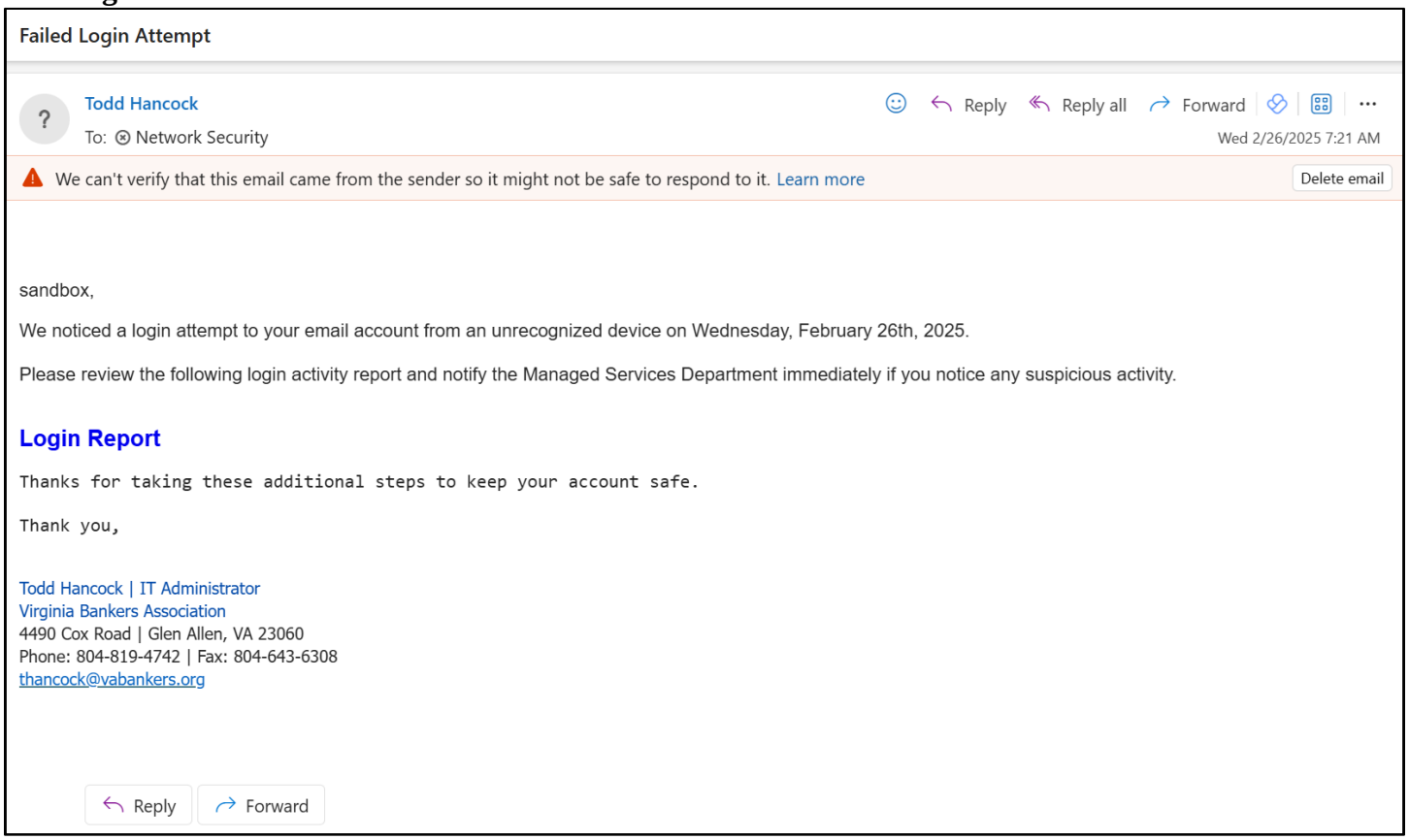
Pretext Vendor Calls:
Out of three (3) attempts made by a social engineer to retrieve internal network information, all employees denied releasing internal network information to the social engineer due to proper verification methods and employee training.

Recommendation - Low:
Virginia Bankers Association should continue to train employees on the proper procedures when verifying a vendor over the phone. Also, Virginia Bankers Association should continue to educate employees on current social engineering attacks that impersonate vendors over the phone.

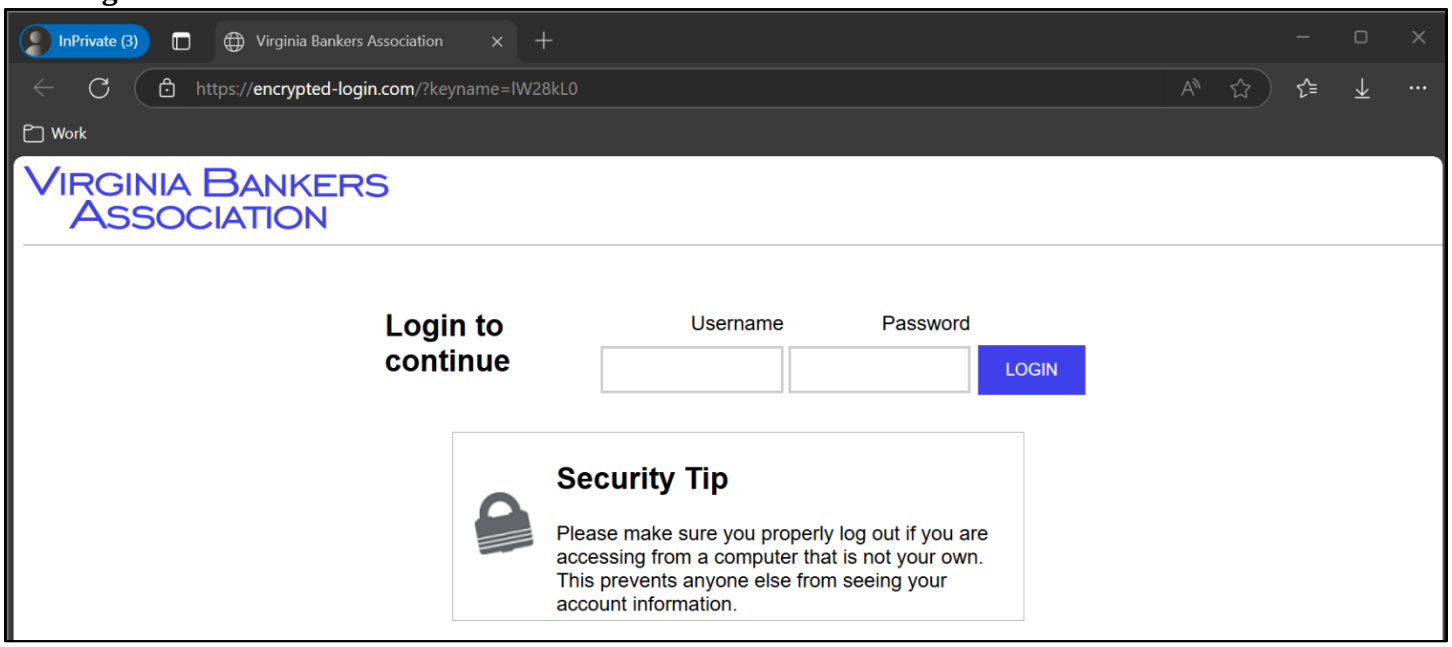
Appendix

Appendix A: Phishing Email & Website

Phishing Email



Landing Website



Appendix B: Phishing Results

Target Emails:

Amy	Binns	abinns@vabankers.org
Ann	Devilbiss	adevilbiss@mdbankers.com
Anne	Boerner	aboerner@vabankers.org
Bobbi	Weimer	bweimer@vabankers.org
Bruce	Whitehurst	bwhitehurst@vabankers.org
Carla	Moore	cmoore@vabankers.org
Chandler	Owdom	cowdom@vabankers.org
Cindy	Beazley	cbeazley@vabankers.org
Claire	Pollock	cpollock@vabankers.org
DeMarion	Johnston	djohnston@vabankers.org
Evan	Richards	erichards@mdbankers.com
Gabrialla	Bond	gbond@vabankers.org
Gail	Queen	gqueen@vabankers.org
John	Snead	jsnead@vabankers.org
Kellee	Edelin	kedelin@vabankers.org
Kristen	Reid	kreid@vabankers.org
Laurie	Milligan	lmilligan@vabankers.org
Liz	Frediani	lfrediani@mdbankers.com
Marie	Basil	mbasil@vabankers.org
Matthew	Bruning	mbruning@vabankers.org
Michele	Dunn	mdunn@vabankers.org
Monica	McDearmon	mmcdearmon@vabankers.org
Pamela	Connelly	pconnelly@vabankers.org
Rachel	Weatherby	rweatherby@vabankers.org
Stacy	Puckett	spuckett@vabankers.org
Suzanne	Jenkins	sjenkins@vabankers.org
Tammy	Clark	tclark@vabankers.org
Tracy	Ottinger	tottinger@vabankers.org
Vicky	Heller	vheller@vabankers.org
Walt	Lyons	wlyons@vabankers.org

Results:

All clicks proved to be false positives. No legitimate clicks were recorded.

Appendix C: Pretext Call Scripts

Vendor Script:

Bank: Good morning, **Bank Name**, this is _____.

SBS: Hi, how are you today?

Bank: Just fine, how may I help you? <Or other response>

SBS: This is _____ from **Vendor Name**. I'm working with **Contact Name.** I'm so sorry to bother you but I need just a moment of your time. Would you be willing to help us for just one moment?

Bank: Sure. **<If they resist, tell them it will only take a few seconds & it will greatly help you out>**

SBS: We pushed out an update to your workstations this morning and it's been causing problems all day. **Contact Name** and I have been working to get it solved. I think we have it taken care of but he/she has asked that I call around and make sure everyone's workstations are functioning properly. How has yours been?

Bank: Yes it's been giving me lots of trouble! **<or>** It seems to be working just fine.

SBS: Hmmm alright, well could you verify some numbers for me? Go to Start Then Run*. Type CMD and hit Enter. Type **IPCONFIG** and please read off the numbers you get after the text:

IP Address: _____
Subnet Mask: _____
Default Gateway: _____

If that doesn't work, have her hold the **START key and then press the **R key***

SBS: Thank you. I have to check a couple things on my end now. **<Keyboard typing noise>**

**If the call is going well, try to ask them for their username (or even password?)*

Appendix D: Pretext Call Results

Results:

Group	Phone Number	Date/Time	Posed As	Employee	Pass/Fail
Group 1	443-926-3486	3/12/2025 12:35 pm PDT	Verizon	Liz Frediani	Pass
Group 2	804-819-4705	3/12/2025 12:25 pm PDT	Verizon	Cindy Beazley	Pass
Group 3	804-819-4718	3/12/2025 12:30 pm PDT	Verizon	Carla Moore	Pass

Group 1

The auditor called Liz posing as a Verizon representative. The auditor stated that they were working with Todd Hancock to push out some security updates to the networking equipment but were running into issues. The auditor explained that issues pushing out the security updates are related to the speed of the internet and asked Liz if they could assist with running a quick speed test to ensure the internet speeds are fast enough to handle the updates. Liz asked if the auditor was looking to update the equipment at the office. The auditor confirmed that it would be the networking equipment at the office. Liz stated that they are not currently at the office but would be there tomorrow if the auditor wanted to call back. The auditor stated that they would speak with Todd to see how they would like to move forward. The auditor thanked Liz for their time and disconnected the call.

Group 2

The auditor called Cindy posing as a Verizon representative. The auditor stated that they were working with Todd Hancock to push out some software updates to the networking equipment but were running into issues. The auditor explained that issues pushing out the security updates are related to the speed of the internet and asked if Cindy noticed any issues with the internet. Cindy advised having the auditor speak with Todd about the issue and stated that Todd usually lets them know if there is anything he would need for them to do. The auditor stated that they would speak with Todd and move forward from there. The auditor thanked Cindy for their time and disconnected the call.

Group 3

The auditor called Carla posing as a Verizon representative. The auditor stated that they were working with Todd Hancock to push out some security updates to the networking equipment but were running into issues. The auditor explained that issues pushing out the security updates are related to the speed of the internet and asked if Carla if they could assist with running a quick speed test to ensure the internet speeds are fast enough to handle the updates. Carla stated that they would not feel comfortable assisting with the updates as they did not receive a heads-up from Todd and had not received a call like this before. Carla stated that if the auditor could speak with Todd and have them give Carla a heads up, they would be able to assist. The auditor stated that they would speak with Todd and see how to proceed from there. The auditor thanked Carla for their time and disconnected the call.

Appendix E: Recommendation Definitions

Phishing Recommendation:

- **High** – Multiple clicks and/or a submission of sensitive information, such as username, password, or Client details, will result in a high recommendation.
- **Medium** – At least one user clicking the link in the assessment will result in a medium recommendation.
- **Low** – No users clicking the link in the assessment will result in a low recommendation.

Pretext Phone Call Recommendation: Vendor

- **High** – One or more test employees gave network information, such as IP address.
- **Medium** – One or more test employees followed the directions the social engineer gave them (i.e. during vendor calls, the employee opens the command line and runs a command, but realizes he/she is not allowed to give out any network information).
- **Low** – No test employees followed instructions or gave any information to the social engineer.