[CLIENT]

Social Engineering Penetration Test Report

[DATE]

Table of Contents

Contents

Confidentiality Statement

All information in this document is provided in confidence. It may not be modified by or disclosed to a third party (either in whole or in part) without the prior written approval of White Knight Labs (WKL). WKL will not disclose to any third-party information contained in this document without the prior written approval of [CLIENT].

Document Control

Date	Change	Change by	Issue
[DATE]	Document Created	[WKL ENGINEER]	V0.1
[DATE]	Document Updated	[WKL ENGINEER]	V1.0
[DATE]	Document Edited	[WKL ENGINEER]	V1.1
[DATE]	Document Published	[WKL ENGINEER]	V1.2

Document Distribution

Name	Company	Format	Date
[CLIENT CONTACT]	[CLIENT]	PDF	[DATE]

White Knight Labs Contact Details

Address	**White Knight Labs** 10703 State Highway 198 Guys Mills PA 16327
Contact	**Tel:** +1 (877) 864-4204 **Mob:** +1 (814) 795-3110 **Email:** info@whiteknightlabs.com

Executive Summary

Security is a journey, not a destination. One must remain vigilant and continue invest in and strive towards a robust security posture. The threat landscape is ever-changing and malicious actors are always innovating. As the internet becomes more hostile, defenders must enhance their capabilities as well.

On [DATE], [CLIENT] engaged White Knight Labs to conduct a phishing assessment of the information technology (IT) environment used by [CLIENT]. This assessment was performed to test the susceptibility of [CLIENT]'s users to social engineering attacks and provide security assistance through identifying areas of weakness, validating the effectiveness of security awareness training, and proposing targeted measures to improve resilience to social engineering threats.

The phishing assessment was conducted from [DATE] to [DATE], providing a snapshot of the security posture of the users within the scope at that specific point in time.

Scoping and Rules of Engagement

While malicious actors have no limits on their actions, WKL understands the need to scope assessments to complete the assessment in a timely manner and protect third parties not participating in the engagement. The following limitations were placed upon this engagement:

- **Phishing/Vishing Assessment** – The goal of a phishing/vishing assessment is to test an organization's susceptibility to phishing/vishing attacks by simulating a real-world phishing scenario. The assessment is designed to evaluate the effectiveness of an organization's existing security controls and to identify areas where improvements are needed to reduce the risk of successful phishing attacks.

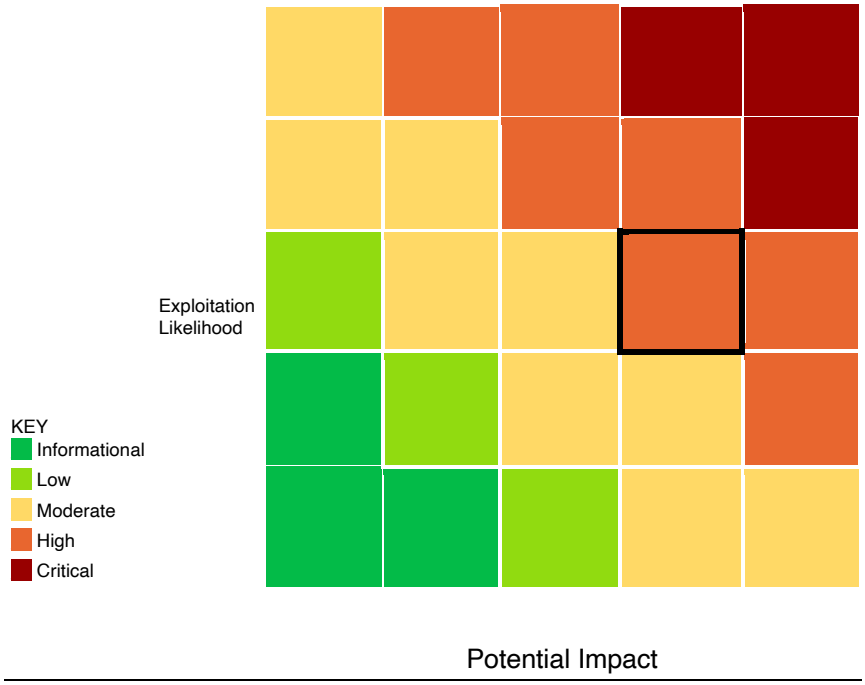
The following timeline details the entire engagement of the [CLIENT] network:

- **Kickoff Call** – [DATE]
- **Engagement Testing** – [DATE] – [DATE]
- **Debrief Call** – TBD

[CLIENT] Risk Rating

WKL calculated the risk to [CLIENT] based on exploitation likelihood (ease of exploitation) and potential impact (potential business impact to the environment).

Overall Risk Rating: High



Summary of Findings

[CLIENT] Email Phishing Campaign

From [DATE] to [DATE], the phishing campaign was active and allowed user interaction from the [CLIENT] employees. WKL received the following stats from the [CLIENT] – New Domain Phishing Campaign:

Figure 1 - Phishing Statistics

WKL received the following data from the [CLIENT] employees during the [CLIENT] – New Domain Phishing Campaign:

- Emails Sent: 168
- Emails Opened: 25
- Email Links Clicked: 25
- User Accounts Compromised: 12

Phishing Assessment Methodology

Our phishing assessment methodology is based on industry best practices and years of experience in conducting successful phishing assessments for organizations of all sizes. Our methodology follows a comprehensive approach to testing the susceptibility of an organization's IT users to phishing attacks. By simulating real-world phishing scenarios, our assessments are designed to evaluate the effectiveness of an organization's security awareness training and identify areas where improvements are needed to reduce the risk of successful phishing attacks.

Reconnaissance:

In this phase, we conduct open source intelligence gathering (OSINT) to gain an understanding of the target's users and digital footprint. This may involve generating user lists, searching historical records, scraping data from the web, and accessing relevant breach data. We will review the target organization's website and social media platforms to identify any relevant details. We will also search online for any employee email addresses, job titles, and other details. Our goal is to obtain as much information as possible about the target organization and its IT users.

Attack Planning and Pretexting:

In this phase, we combine the information gathered in the reconnaissance phase into a plan of attack. The plan includes creating a pretext (the story being used and who will be shown as the sender of the phishing email), the email content, the email addresses and names of targets, the goals of the engagement (e.g., gathering credentials, testing the email infrastructure for the ability to detect malicious files), timing, etc. We develop a set of phishing templates that we will use in the campaign. We also work with the client to ensure that the phishing templates are tailored to their organization's culture and tone.

Execution:

In this phase, we launch the email phishing campaign and monitor the results. Phishing emails are sent out in a phased manner, over a period of hours or days depending on the number of IT users in scope. The phishing campaign remains active for a week or two, allowing recipients enough time to act upon the phishing email received. We use Excel files to track the campaign's progress, including which users received the email, how many users clicked on the email, and how many users provided their credentials. We also monitor activity on the client's email infrastructure to ensure that the phishing emails do not cause any disruptions.

Analysis and Reporting:

In this phase, we provide a report that includes the pretext/content included in the email, a summary of the results (e.g., who read the email, who took an action), and the results for each IT user. We analyze the results to identify any trends or patterns in user behavior. We also provide recommendations on how the client can improve their security posture to reduce the risk of successful phishing attacks. Our report includes a detailed description of the campaign and all the communication we had with the client during the assessment.

During the engagement, we document all relevant network or system configurations used in the phishing campaign. We also document all communication with the client, including progress reports and recommendations, for future reference. Our goal is to provide the client with a comprehensive assessment of their security posture and actionable recommendations to improve their resilience to phishing attacks.

Phishing Attack Path

WKL recently performed a comprehensive phishing assessment of the information technology (IT) environment used by [CLIENT]. The main objective of this assessment was to identify any areas of vulnerability in [CLIENT]'s IT environment, validate the effectiveness of security awareness training, and propose targeted measures to improve resilience to social engineering threats. Our assessment involved several targeted phishing campaigns that simulated real-world social engineering attacks.

The phishing campaign was designed to be as convincing as possible, using a variety of techniques such as email spoofing, domain name spoofing, and clone phishing to create convincing phishing emails and webpages.

Our aim is to help [CLIENT] better understand the threat posed by social engineering attacks and provide them with the tools and knowledge needed to reduce the risk of successful attacks. By simulating real-world attacks, we can help [CLIENT] improve their security posture and better protect their organization from the growing threat of social engineering attacks. Please see the detailed write-up of the phishing campaign that was executed against [CLIENT] below, which includes a comprehensive breakdown of each campaign and our analysis of the results.

Phishing Email Scenarios

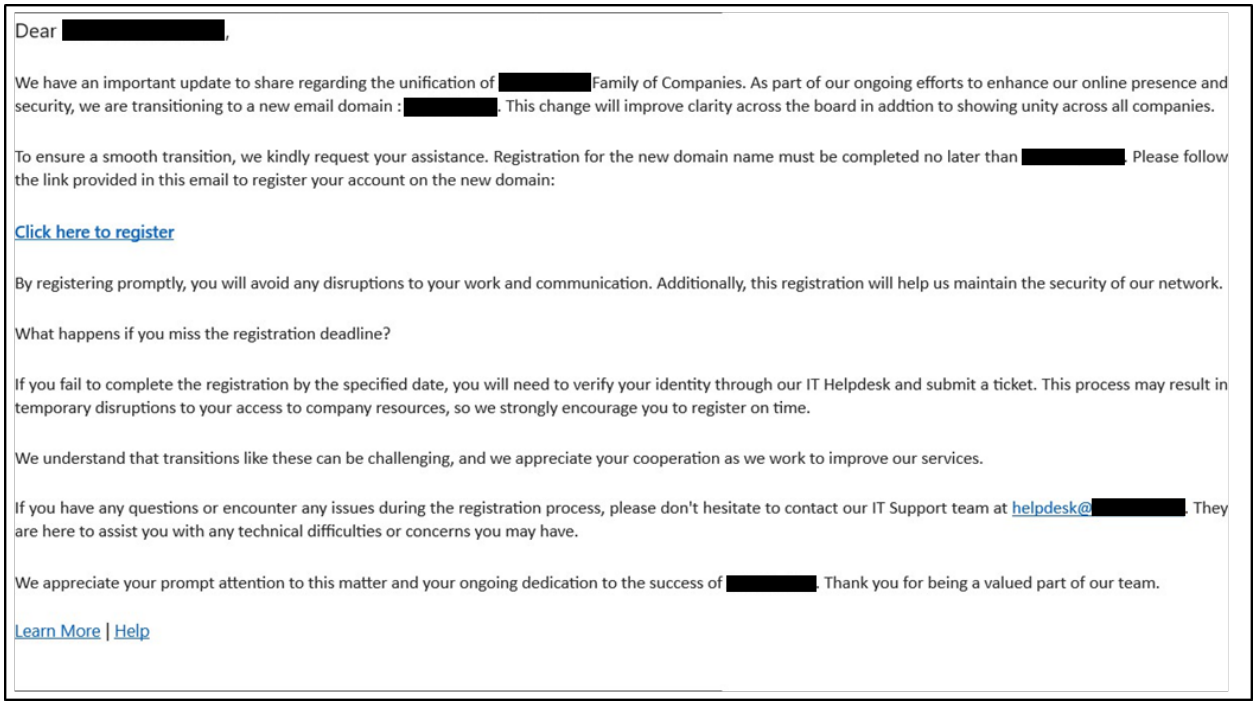
The following scenario was executed against the [CLIENT] users:

- **[CLIENT] – New Domain Phishing Campaign** – Using the domain "[DOMAIN NAME]", an email was sent to 168 users informing them that [CLIENT] would be unifying the different companies under a single email domain, [DOMAIN NAME]. Employees were told that they would need to register their email addresses on the new site by [DATE] to prevent any disruption to work.

Phishing Campaign Execution

[CLIENT] – New Domain Phishing Campaign

This phishing assessment aimed to capture user credentials as they attempt to register for an email address on the new [DOMAIN NAME] domain. For this phishing assessment, WKL began with the domain "[DOMAIN NAME]". The email was created to appear as an email from [CLIENT]. The premise of the campaign was that there is a new domain that would unify the different parts of the company and all employees needed to register to get their email address.



Dear [redacted],

We have an important update to share regarding the unification of [redacted] Family of Companies. As part of our ongoing efforts to enhance our online presence and security, we are transitioning to a new email domain : [redacted]. This change will improve clarity across the board in addtion to showing unity across all companies.

To ensure a smooth transition, we kindly request your assistance. Registration for the new domain name must be completed no later than [redacted]. Please follow the link provided in this email to register your account on the new domain:

Click here to register

By registering promptly, you will avoid any disruptions to your work and communication. Additionally, this registration will help us maintain the security of our network.

What happens if you miss the registration deadline?

If you fail to complete the registration by the specified date, you will need to verify your identity through our IT Helpdesk and submit a ticket. This process may result in temporary disruptions to your access to company resources, so we strongly encourage you to register on time.

We understand that transitions like these can be challenging, and we appreciate your cooperation as we work to improve our services.

If you have any questions or encounter any issues during the registration process, please don't hesitate to contact our IT Support team at helpdesk@[redacted]. They are here to assist you with any technical difficulties or concerns you may have.

We appreciate your prompt attention to this matter and your ongoing dedication to the success of [redacted]. Thank you for being a valued part of our team.

Learn More | Help

Figure 2 - Phishing Email

Once the user clicked the link in the email, they were brought to a login page with [CLIENT] branding along with a picture taken from the [CLIENT] website. Users were instructed to enter their current and requested email address along with their password. After users clicked 'Sign In', they were redirected to [DOMAIN NAME].

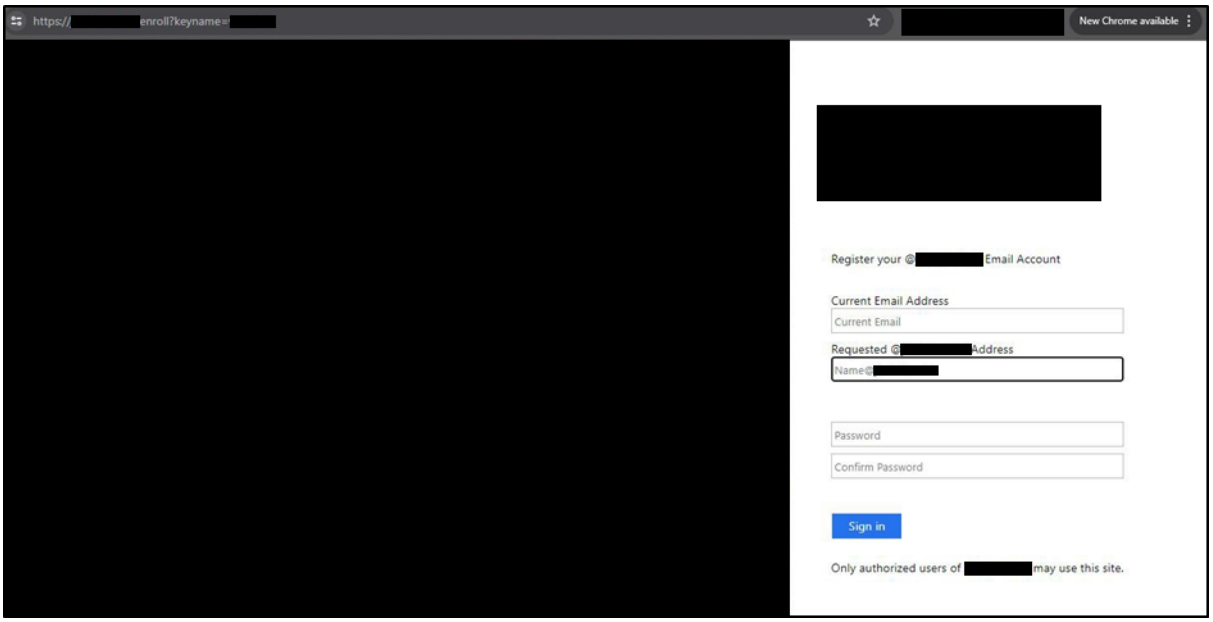


Figure 3 - Phishing Login Page

Phishing Campaign Results

WKL started the phishing campaign on [DATE]. WKL measured four different actions taken by [CLIENT] employees after the phishing emails were received:

- Email Sent
- Email Opened
- Email Link Clicked
- Submitted Data

[CLIENT] – New Domain Phishing Campaign

From [DATE] to [DATE], the phishing campaign was active and allowed user interaction from the [CLIENT] employees. WKL received the following stats from the [CLIENT] – New Domain Phishing Campaign:

Figure 4 - Phishing Statistics

WKL received the following data from the [CLIENT] employees during the [CLIENT] – New Domain Phishing Campaign:

- Emails Sent: 168
- Emails Opened: 25
- Email Links Clicked: 25
- User Accounts Compromised: 12

Vishing

Summary of Findings

[CLIENT] provided a list of 20 users/departments to attempt vishing. Of the 20 targets:

- Calls Made: 20
- Calls Answered: 11
- User Accounts Compromised: 5

Overall, the [CLIENT] targets were found to be vulnerable. WKL felt it was important to note that of the five targets that failed, at least three were not direct [CLIENT] employees and mentioned being employed by [THIRD-PARTY COMPANY].

Vishing Attack Path

On [DATE], WKL launched a vishing campaign against a provided list of targets. WKL utilized a service called Bluff My Call to make the calls for the vishing engagement. With Bluff My Call, WKL was able to spoof the Caller ID to display any number.

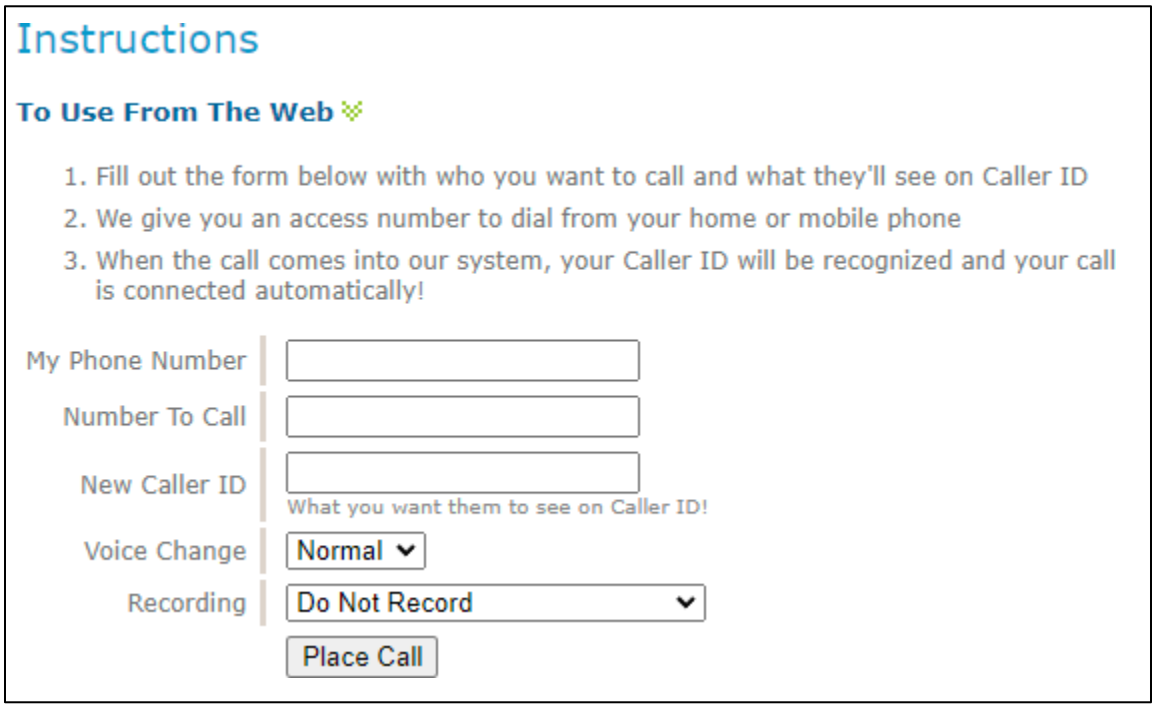


Figure 5 - Bluff My Call Spoofing Portal

WKL used the [CLIENT] headquarters' contact number found on their public website to make the vishing call appear to be from an internal source. WKL attempted to call each user twice during regular business hours.

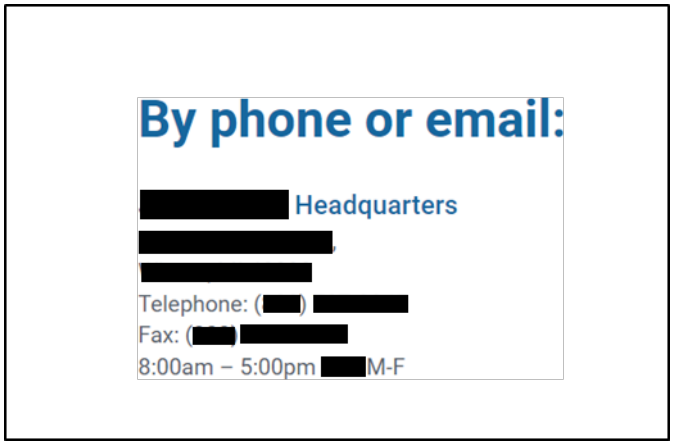


Figure 6 – [CLIENT] Headquarters phone number found on [WEBSITE]

WKL used the domain [DOMAIN NAME], which was created to appear as their internal portal login page to collect the target's username and password.

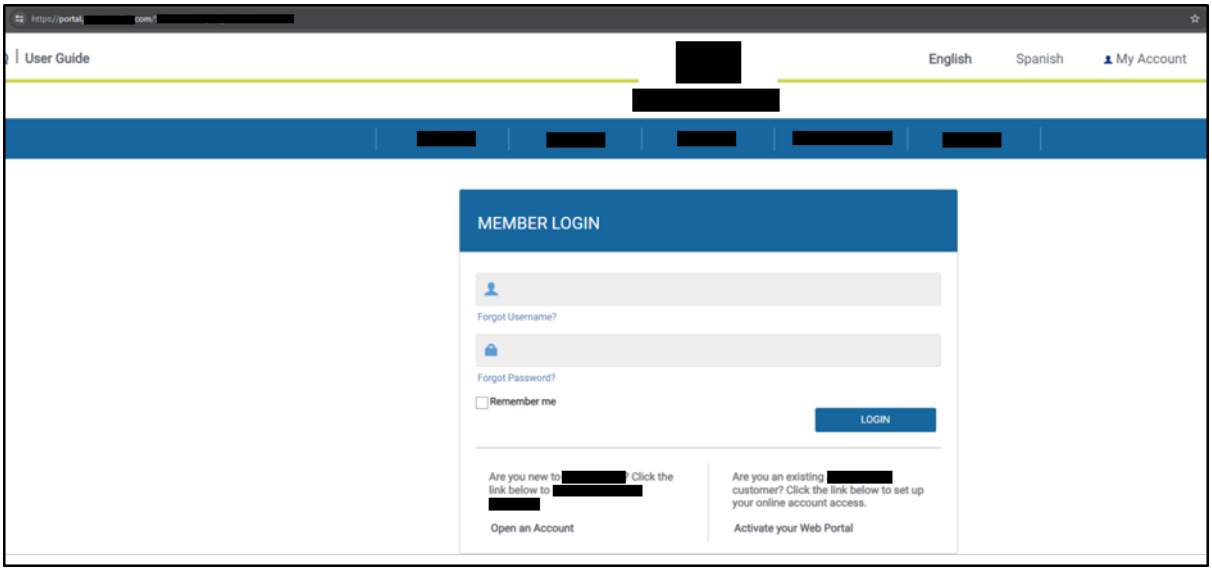


Figure 7 - Legitimate [WEBSITE] Login Site

The pretext WKL used was that the engineer calling was a [CLIENT] employee supporting the IT department to stand up a new domain that would unify [CLIENT] brands on one internal site.

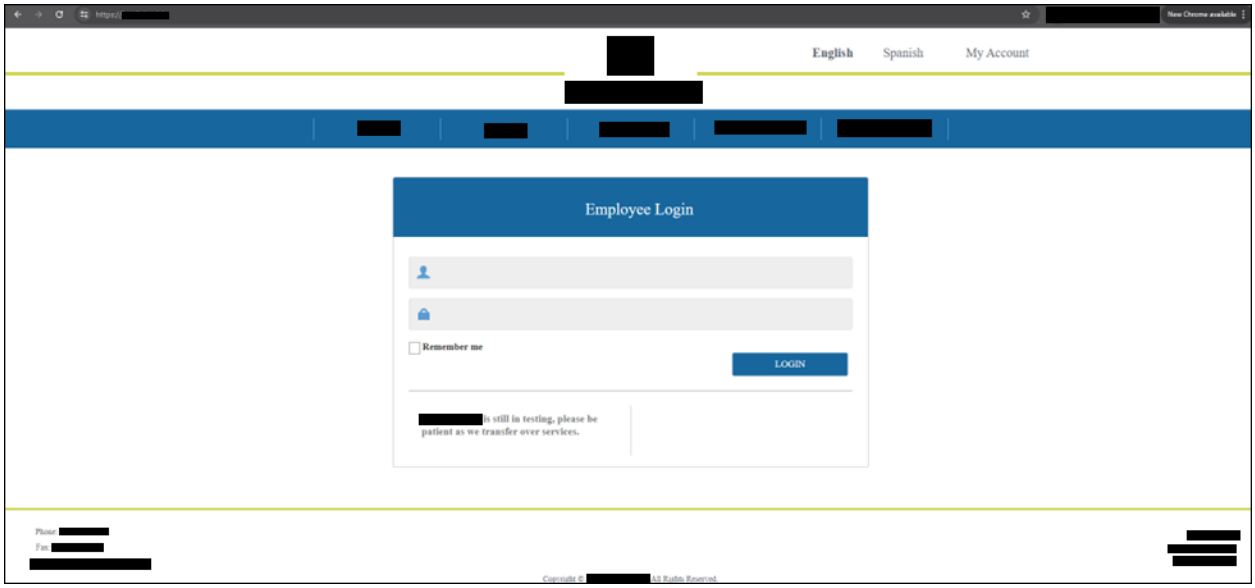


Figure 8 - WKL Vishing Login Page

Vishing Campaign Results

WKL targeted 20 users with the vishing campaign. WKL received the following data from the [CLIENT] employees:

- Calls Made: 20
- Calls Answered: 11
- User Accounts Compromised: 5