**Phishing Attack Report**

**CECS 378**



**Members:** 015843540 Jalon Flores

011667576 Andre Barajas

014058185 Anthony Diaz

**Date:**

Table of Contents

[**1. Overview**](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_mi224s12o9ru) **3**

[1.1 Purpose](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_yvnht7vm568j) 3

[**2. What is a Phishing Attack?**](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_yd3bigoq9gtk) **3**

[2.1 Definition](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_oc9vq6rg4vqd) 3

[2.2 How does it work?](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_snhgxenju1mz) 3

[2.2 Types of Phishing Attack](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_cjt9i96036fx) 3

[2.3 How to identify Phishing Attacks](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_f5m45a7ob851) 3

[**3. Implementation**](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_93znmq5ylzpf) **3**

[**4. Results**](file:///C:\Users\baraj\Desktop\csulb.fall19\cs378\CECS%20378%20Phishing%20Attack%20Report%20.docx#_fhzdmwduzet7) **3**

# **1. Overview**

## **1.1 Purpose**

# **2. What is a Phishing Attack?**

## **2.1 Definition**

Phishing - fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

## **2.2 How does it work?**

An individual is sent an email that looks like it’s coming from a reputable company. This email can say a number of topics including:

1. Fill out a survey and be entered in a raffle to win a new Playstation 4.
2. Your account may be in danger. Please click the link to change your password.

After the individual clicks the link, they are taken to a website that looks like a reputable company. The user will fill out any information that they are prompted to fill such as name, password, address, etc. After they submit this information, the data is now in the hands of the phishers.

## **2.2 Types of Phishing Attack**

1. **Clone Phishing**

This type of phishing attack requires hacking a previously sent email. The email is “resent” to the recipients with a new and updated link that allows the data to be sent to the phishers. This usually requires that the sender or recipient was previously attacked in order to obtain the email information.

1. **Search Engine Phishing**

This type of phishing attack involves the usage of a fake website. The website waits for a user to click on the link to the website, which is usually found through a search engine. Once the individual is taken to the website, their data is sent to the phishers.

1. **Smishing**

This type of phishing attack is sent through text. The message contains details about canceling an order while being provided a link. The individual is sent to a fake page where they fill out their information.

1. **Spear Phishing**

This type of phishing attack is directed towards specific individuals or companies. The phishers gather and use other’s personal information to make their emails look more credible.

1. **Vishing**

This type of phishing attack is done through a phone call. The phisher disguises themself as a trusted person such as a family member, friend, etc. They get the individual to give them personal data.

1. **Whaling**

This type of attack is similar to a phishing attack, except it is specifically targeted to higher profiled individuals. An email can potentially be disguised as a customer complaint to get the individual to follow the link.

## **2.3 How to identify Phishing Attacks**

There are a number of ways to identify a phishing attack.

1. **Reputable companies don’t ask for sensitive information through email.**

If an individual is receiving an email from someone who is asking them to visit a link or download a file to fill out personal information, it’s most likely a scam. Trusted companies won’t ask you to provide such information through an email.

1. **Reputable companies will provide the individual’s name in the email.**

If an individual is being referred nouns such as customer or member, then it's probably a scam. A trusted company will address someone by their name. The phisher could also avoid putting a salutation in the email, making it look like an email from a reliable source. The domain of the email can give away the phisher.

1. **Reputable companies contain emails with domains.**

It’s best to check the name of the email of the sender. The domain should be unique and usually shouldn’t contain any numbers. A trusted company wouldn’t use a domain that the individual would question.

1. **Reputable companies won’t make punctuation/grammatical errors.**

An email written from a trusted company should be well written with no errors. Phishers, sometimes, write the email poorly to attract more uneducated individuals.

1. **Reputable companies won’t try to force an individual to visit their website.**

There is a chance that an individual can accidently click on an email which would take them to a fake website, or to download an infected file. An individual should be careful when scrolling through an email to avoid accidently clicking anywhere on the email.

1. **Reputable companies won’t provide attachments in the email.**

An email containing attachments was probably sent by a phisher. A trusted company will direct an individual to their website to download any files. This one can be a little harder to verify. If in doubt, it is best to contact the company regarding the email.

1. **Reputable companies will provide a link with a trusted URL.**

An individual should check any links by hovering over it first. If both links don’t match, then it is going to take them to a fake website. If the link doesn’t match the description of the email, then the user will more than likely be taken to a fake website too. The link should begin with https://. If it doesn’t, then it’s best not to trust it.

# **3. Implementation**

# **4. Results**