**FAST- National university of Computer and Emerging Sciences**

**INFORMATION SECURITY**

**PHISHING ATTACK**

**Project Report**

**Supervisor**:

Ms. Nausheen Shoaib

**Group Members:**

[Ishaq Ahmed18k-0295]

[Burhanuddin, 18k-0213]

[Umer Alam, 18k-0164]

* **Objective:**
  + This initiatives pursuits to observe about unique kinds of phishing assaults which might additionally display approximately the numerous defenses that may be implemented to save you from such assaults.
  + Determining different types of phishing attack along with their solutions
  + Conclude reports and finding from attacking various machines, stealing data if possible
* **Introduction:**

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or gather recon, install malicious scripts/files, or to extract data such as user information, financial info, and more.

* **Methodology and Applications:**

As phishing messages and techniques become increasingly sophisticated, despite growing awareness and safety measures taken, many organizations and individuals alike are still falling prey to this pervasive scam. We will delve into the five key phishing techniques that are commonly employed:

1) Link manipulation

2) Smishing

3) Vishing

4) Website forgery

5) Pop-ups

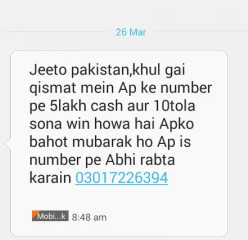
1. **LINK MANIPULATION**

Link manipulation is done by directing a user fraudulently to click a link to a fake website. This can be done through many different channels, including emails, text messages and social media. There are 4 common methods used for this.

* + Misspelled URL’s (This is when a phisher hides the actual URL of a phishing website under plain text, such as “Click Here” or “Subscribe”.)
  + Use of subdomains (A phisher may try to trick you with the fraudulent link yahoo.mail.com which will lead you to a page with a main domain of Mail and a subdomain of Yahoo)
  + Hidden URL’s (When a hacker buys domains with a variation in spellings of a popular domain, such as Facebook.com, googlle.com, yahooo.com. This technique is also known as URL hijacking or typo squatting.)
  + IDN Homographic Attack (In this technique, a malicious individual misguides a user towards a link by taking advantage of similar looking characters.)

1. **SMISHING**

Smishing is a form of phishing where someone tries to trick a victim into giving their private information via a text message. The most common form of smishing is a text with a link that automatically downloads malware. An installed piece of malware can steal personal data such as banking credentials, tracking locations, or phone numbers from contact lists to spread the virus in hopes to exponentially multiply.

1. **VISHING**

Vishing is the telephone version of phishing, or a voice scam. Similar to email phishing and smishing, vishing is designed to trick victims into sharing personal information, such as PIN numbers, social security numbers, credit card security codes, passwords and other personal data.

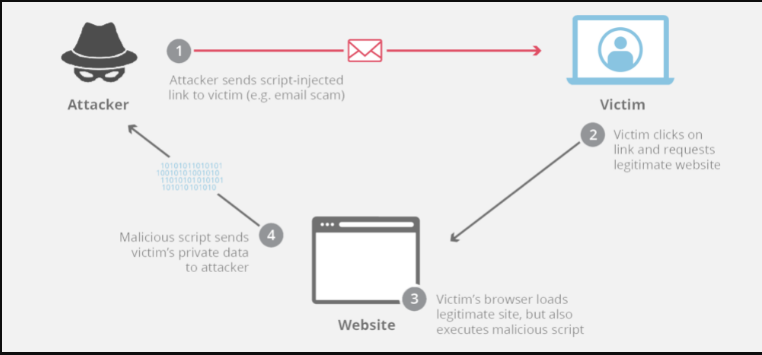


1. **WEBSITE FORGERY**

Website forgery works by making a malicious website impersonate an authentic one, so as to make the visitors give up their sensitive information such as account details, passwords, credit card numbers. Web forgery is mainly carried out in two ways:

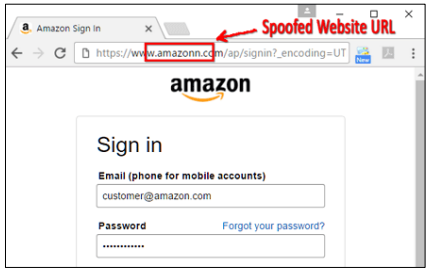
* + **Cross-Site Scripting**

Cross-Site Scripting This is when a hacker executes malicious script or payload into a legitimate web application or website through exploiting a vulnerability.



* + **Website spoofing**

This is done by creating a fake website that looks similar to a legitimate website that the user intends to access.

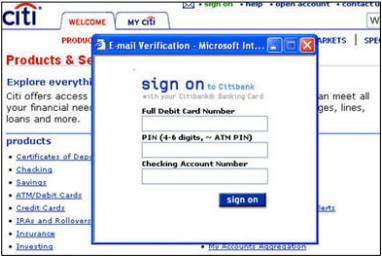


1. **POP-UPS**

Pop-up messages, other than being intrusive, are one of the easiest techniques to conduct phishing scams. They allow hackers to steal login details by sending users pop-up messages and eventually leading them to forged websites.

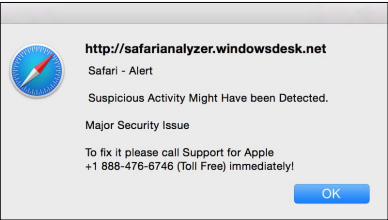
* + In-session phishing

This variant of phishing works by displaying a pop-up window during an online banking session, asking the user to retype his username and password as the session has expired. The user enters his details, not expecting the pop-up to be a fraud as they had already logged into the bank’s website.



* + Pop-up tech support

Another widespread pop-up phishing scam is the “popup tech support.” When browsing the Internet, you will suddenly receive a pop-up message that your system is infected and you need to contact your vendor for technical support.



**COUNTERMEASURES:**

In general, we can prevent ourselves from phishing by

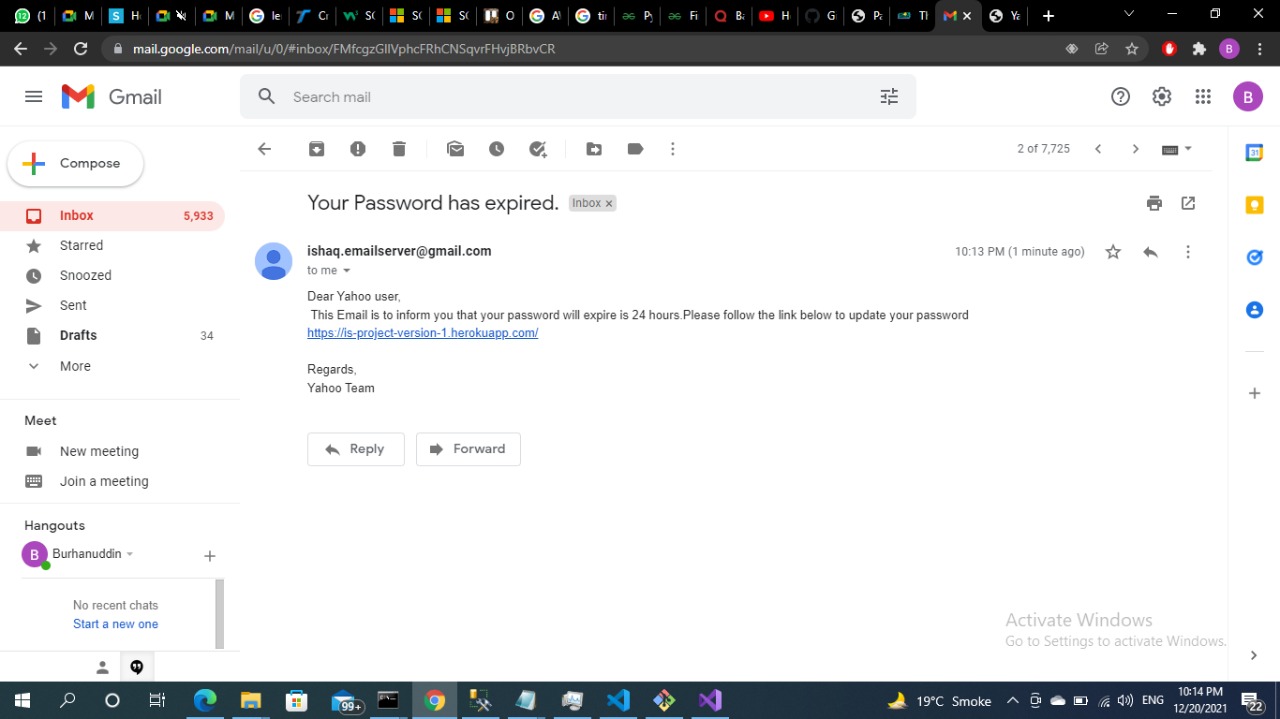


The most commonly used method for phishing is web. So, to avoid phishing we can keep in mind following information.

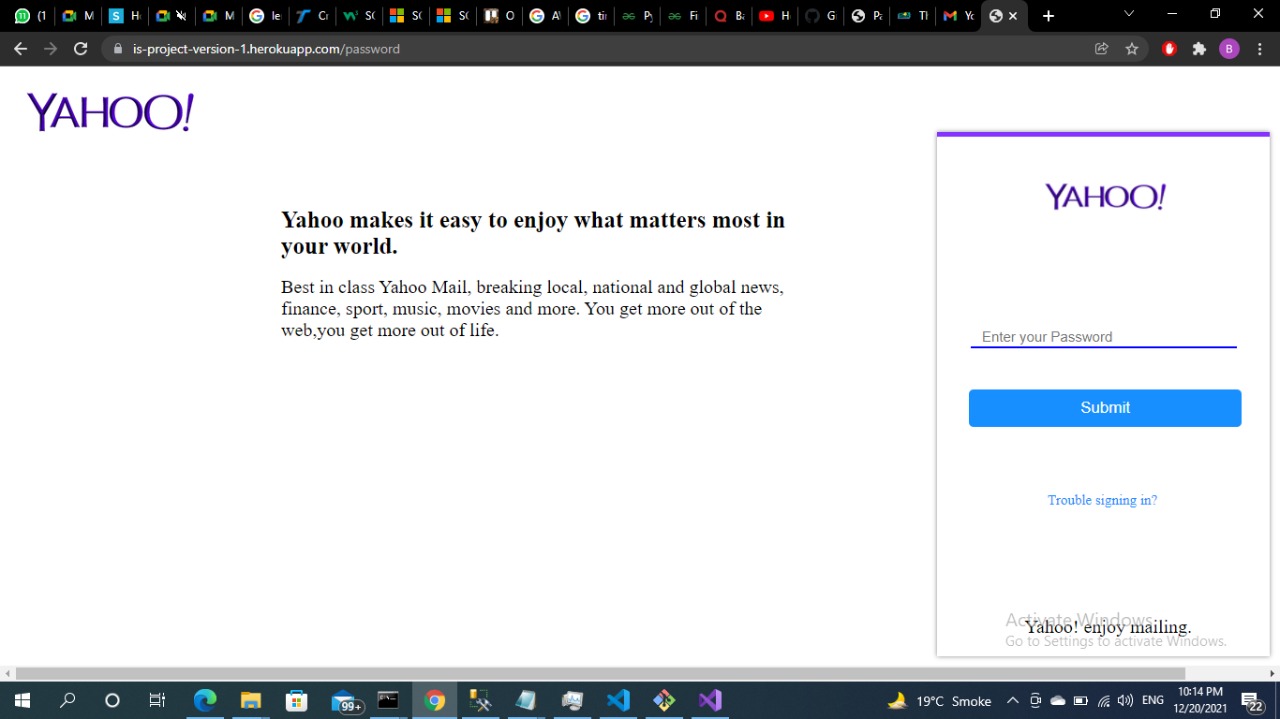


**METHODOLOGY WE USE:**

We have used Link Manipulation for our phishing attack on user. The email will be send to mass which will not be targeted to any particular person giving alert that their Yahoo account has been blocked. The email will include a link to restore the account.



The user will click on the given link and then he will be redirected to our fake website which resembles the login page of Yahoo



When he/she enters credentials to login in yahoo account, his email address and real password would be sent to our server, while a server down message would be shown on the fake login page, mistaken by the user that server is not working correctly. So that’s how hacker(we) has succeeded in stealing a valid user credential

