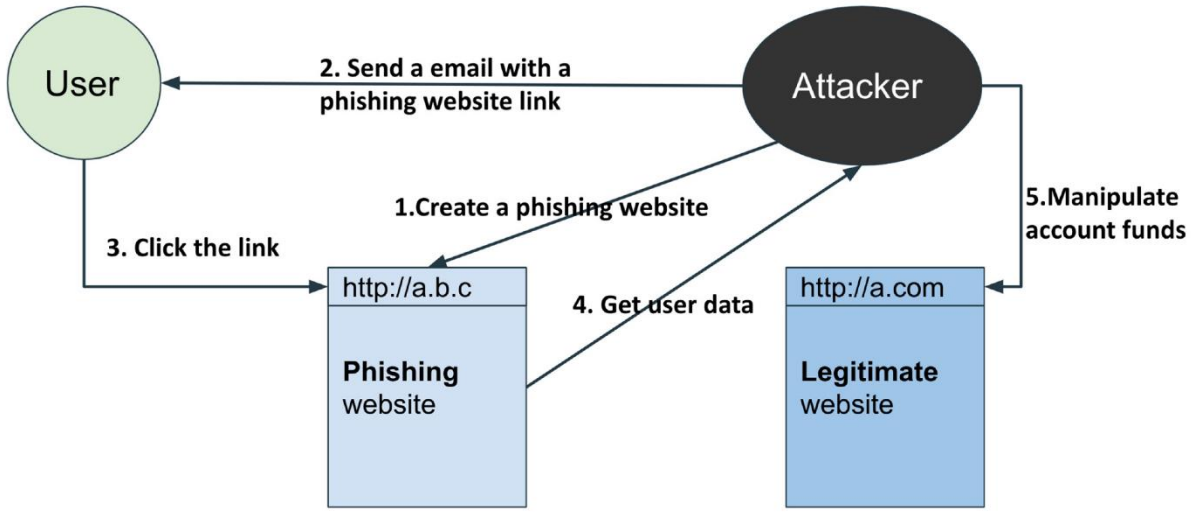
IDEATION PHASE

Varshini P	721719104089
SubaVarshini S	721719104081
Mythili R	721719104053
Navaneetha Krishnaveni	721719104056

Phishing URL may be a widely used and customary technique for cybersecurity attacks. Phishing is a cybercrime that tries to trick the targeted users to expose their private and sensitive information to the attacker. The motive of the attacker is to gain access to personal information like usernames, login credentials, passwords, financial account details, social networking data, and personal addresses. These private credentials are then often used for malicious activities like fraud, notoriety, gain, reputation damage, and lots of more illegal activities. This paper presents a comprehensive study of various existing systems used for phishing website detection. The system presented here uses advanced machine learning and to realize better precision and better accuracy while categorizing websites as phishing or benign.

Phishing is that the fraudulent plan to obtain sensitive information or data, such as usernames, passwords, and MasterCard details, or other sensitive details, by impersonating oneself as a trustworthy entity in digital communication. Typically administered by email spoofing instant messaging and text messaging, phishing often directs users to enter personal information at a fake website that matches the design and feel of the legitimate site. Phishing is an example of social engineering techniques wont to deceive users. Users are lured by communications purporting to be

from trusted parties such as social networking websites, auction sites, banks, emails/messages from friends or colleagues/executives, online



1.CREATE A PHISHING WEBSITE.

Step 1

In this article, I will show to create a facebook phishing page. To create phishing page, go to the Facebook.com and then right-click on the blank area, you will see the option **view source page.** Click on that.

Step 2

Now a tab will open which will contain the source code of Facebook login page. Select all code and copy all code and paste it into notepad.

Step 3

Now open notepad in which you have pasted this code and press CTRL+F and type ACTION.

Step 4

You will have to search again and again till you have found the text which looks like

action=”https://www.facebook.com/login.php?login_attempt=1&lwv=110“

Step 5

When you find something similar to this code (which is written above). Delete all the text code which is similar to the above code (written in grey colour box) and replace it with **Post.php**. Then it will look like action=”post.php.

Step 6

Now save it to your desktop with the name index.htm and yes remember not to save it as index.html. As many individuals do this mistakes. Now you have completely made your phishing page.

Step 7

Now you need to create a PHP file for this. Open a new notepad and copy the code given below and save it with the name **post.php.**

Step 8

Now you need to upload these two files in a free web hosting site.
Some best Web hosting site which is useful for you. you need to make an account on any of one below web hosting site.

1. www.my3gb.com
2. Bluehost
3. www.000webhost.com
4. Freehosting

Step 9

Now, you have to sign up for an account. Click on free sign up and fill all required information in the registration form. When your account completely set up simply log in with your username and password.

Step 10

Now open Cpanel (control panel) then click on file manager. After that, a new window will pop up. now go to public_html.

Step 11

Delete the file named default.php after that you need to upload index.htm and post.php file. Click on upload files button and upload both files one by one. Now click on index.htm which will look like same as that of the original Facebook page. This is your phishing page of Facebook.

2.SENDING A EMAIL WITH A PHISHING WEBSITE LINK

- The Fake Invoice Scam. Let's start with arguably the most popular phishing template out there - the fake invoice technique. ...
- Email Account Upgrade Scam. ...
- Advance-fee Scam. ...
- Google Docs Scam. ...
- PayPal Scam. ...

- Message From HR Scam. ...
- Dropbox Scam.

3.GET USER DATA

Some methods include **direct messages sent over social networks and SMS text messages**. Phishers can use public sources of information to gather background information about the victim's personal and work history, interests and activities. Typically through social networks like LinkedIn, Facebook and Twitter.

4.MANIPULATE ACCOUNT FUNDS

Understanding phishing techniques. 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.