WEB PHISHING DETECTION

INTRODUCTION

1.1 Project Overview

Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced. Besides, the most common technique used, blacklist-based method, is inefficient in responding to emanating phishing attacks since registering a new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database. Furthermore, page content inspection has been used by some strategies to overcome the false negative problems and complement the vulnerabilities of the stale lists. Moreover, page content inspection algorithms each have different approach to phishing website detection with varying degrees of accuracy. Therefore, ensemble can be seen to be a better solution as it can combine the similarity in accuracy and different error-detection rate properties in selected algorithms.

1.2 Purpose

- The purpose of Phishing Domain Detection is detecting phishing domain names. Therefore, passive queries related to the domain name, which we want to classify as phishing or not, provide useful information to us.
- URL is the first thing to analyze a website to decide whether it is a phishing or not. As we mentioned before, URLs of phishing domains have some distinctive points. Features which are related to these points are obtained when the URL is processed.
- Page-Based Features are using information about pages which are calculated reputation ranking services. Some of these features give information about how reliable a website is.
- Obtaining these types of features requires active scanning to the target domain. Page contents are processed for us to detect whether the target domain is used for phishing or not.

All of the features explained above are useful for phishing domain detection.

2.LITERATURE SURVEY

2.1 Existing Problem

In previous years, researchers have developed phishing detection systems using different techniques and data sources. Next, we review these approaches together with the datasets presented.

In phishing detection, an incoming URL is identified as phishing or not by analyzing the different features of the URL and is classified accordingly. Different machine learning algorithms are trained on various datasets of URL features to classify a given URL as phishing or legitimate.

2.2. References

Detecting Phishing Websites Using Machine Learning by Sagar Patil, Yogesh Shetye, Nilesh Shendage published in the year 2020.

Machine Learning-Based Phishing Attack Detection by Sohrab Hossain, Dhiman Sarma, Rana Joythi Chakma published in the year 2020.

Phishing website detection based on an effective machine learning approach by Gururaj Harinahalli Lokesh published in the year 2020.

2.3. Problem Statement Definition

Phishing is a major problem, which uses both social engineering and technical deception to get users' important information such as financial data, emails, and other private information. Phishing exploits human vulnerabilities; therefore, most protection protocols cannot prevent the whole phishing attacks.

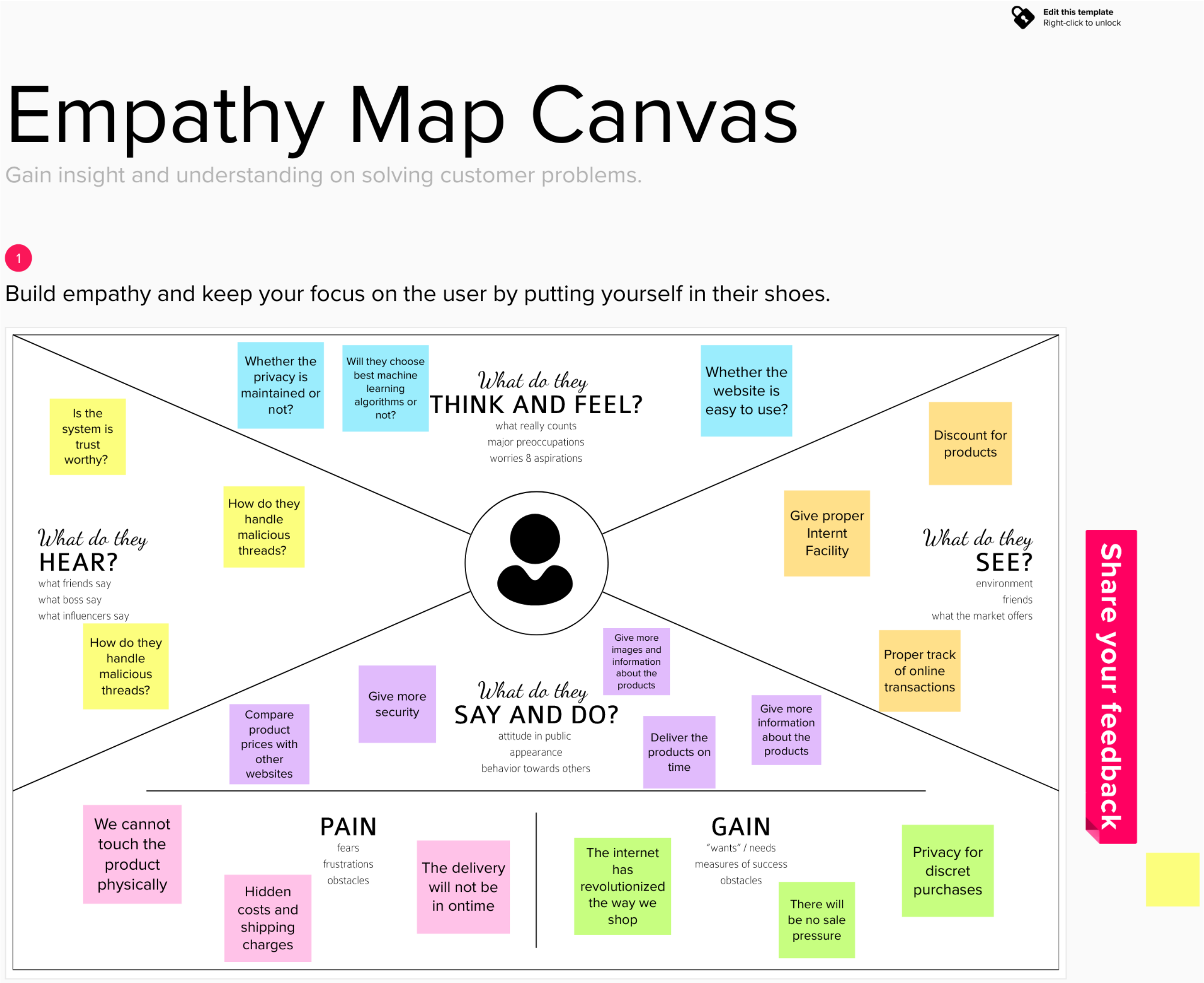
Many of them use the blacklist/whitelist approach, however, this cannot detect zero-hour phishing attacks, and they are not able to detect new types of phishing attacks.

'Phishing sites' are some type of internet security issues that mainly targets the human vulnerabilities compared to software vulnerabilities.

3. IDEATION AND PROPOSED SOLUTION

3.1 Empathy Map Canvas

Visualizing user attitudes and behaviors in an empathy map helps UX teams align on a deep understanding of end users. The mapping process also reveals any holes in existing user data.



Empathy Map Canvas

Gain insight and understanding on solving customer problems.

1

Build empathy and keep your focus on the user by putting yourself in their shoes.

What do they THINK AND FEEL?
what really counts
major preoccupations
worries & aspirations

- Is the system is trust worthy?
- Whether the privacy is maintained or not?
- Will they choose best machine learning algorithms or not?
- Whether the website is easy to use?

What do they HEAR?
what friends say
what boss say
what influencers say

- How do they handle malicious threads?
- How do they handle malicious threads?

What do they SEE?
environment
friends
what the market offers

- Discount for products
- Give proper Internt Facility
- Proper track of online transactions

What do they SAY AND DO?
attitude in public
appearance
behavior towards others

- Compare product prices with other websites
- Give more security
- Give more images and information about the products
- Deliver the products on time
- Give more information about the products

PAIN
fears
frustrations
obstacles

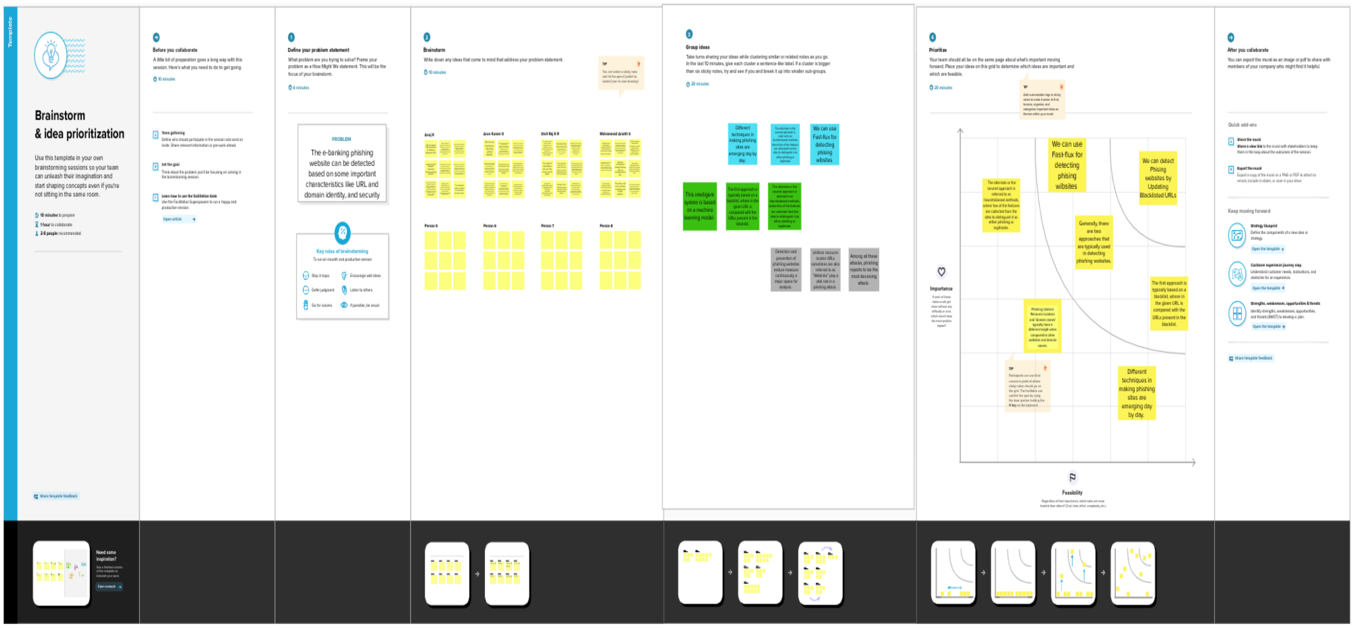
- We cannot touch the product physically
- Hidden costs and shipping charges
- The delivery will not be in ontime

GAIN
"wants" / needs
measures of success
obstacles

- The internet has revolutionized the way we shop
- There will be no sale pressure
- Privacy for discret purchases

3.2 Ideation And Brainstorming

Ideation is often closely related to the practice of brainstorming, a specific technique that is utilized to generate new ideas. A principal difference between ideation and brainstorming is that ideation is commonly more thought of as being an individual pursuit, while brainstorming is almost always a group activity.



Template

Brainstorm & idea prioritization

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

10 minutes to prepare
1 hour to collaborate
2-8 people recommended

Before you collaborate
A little bit of preparation goes a long way with this session. Here's what you need to do to get going.
10 minutes

A Team gathering
Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.

B Set the goal
Think about the problem you'll be focusing on solving in the brainstorming session.

C Learn how to use the facilitation tools
Use the Facilitation Superpowers to run a happy and productive session.

Open article

1 Define your problem statement
What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.
5 minutes

PROBLEM
The e-banking phishing website can be detected based on some important characteristics like URL and domain identity, and security

Key rules of brainstorming
To run an smooth and productive session
Stay in topic.
Encourage wild ideas.
Defer judgment.
Listen to others.
Go for volume.
If possible, be visual.

2 Brainstorm
Write down any ideas that come to mind that address your problem statement.
10 minutes

3 Group ideas
Take turns sharing your ideas while clustering similar or related notes as you go. In the last 10 minutes, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you and break it up into smaller sub-groups.
20 minutes

Different techniques in making phishing sites are emerging day by day.

We can use Fast-flux for detecting phising wibsites

This intelligent system is based on a machine learning model.

The first approach is typically based on a blacklist, where in the given URL is compared with the URLs present in the blacklist.

The alternate or the second approach is referred to as heuristic-based methods, where few of the features are collected from the sites to distinguish it as either phishing or legitimate.

Detection and prevention of phishing websites endure measure continuously a major space for analysis.

Uniform resource locator URLs sometimes are also referred to as "Weblinks" play a vital role in a phishing attack.

Among all these attacks, phishing reports to be the most deceiving attack.

4 Prioritize
Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.
20 minutes

We can detect Phising websites by Updating Blacklisted URLs

Generally, there are two approaches that are typically used in detecting phishing websites.

Different techniques in making phishing sites are emerging day by day.

After you collaborate
You can export the mural as an image or pdf to share with members of your company who might find it helpful.

3.3 Proposed Solution

Problem Statement

- Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced.
- Besides, the most common technique used, blacklist-based method, is inefficient in responding to emanating phishing attacks since registering a new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database.

Idea/Solution Description

- Identify the criteria that can recognize fake URLs
- Build a decision tree that can iterate through the criteria
- Train our model to recognize fake vs real URLs
- Evaluate our model to see how it performs
- Check for false positives/negatives

Novelty Uniqueness

- There are three phases in the proposed approach.
- The first stage is the pre-processing stage.
- Through this stage, characteristics and sub-functions are derived from phishing and related websites.

Social Impact / Customer Satisfaction

- Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities.
- These effects work together to cause loss of company value, sometimes with irreparable repercussions.
- Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities.

Business Model

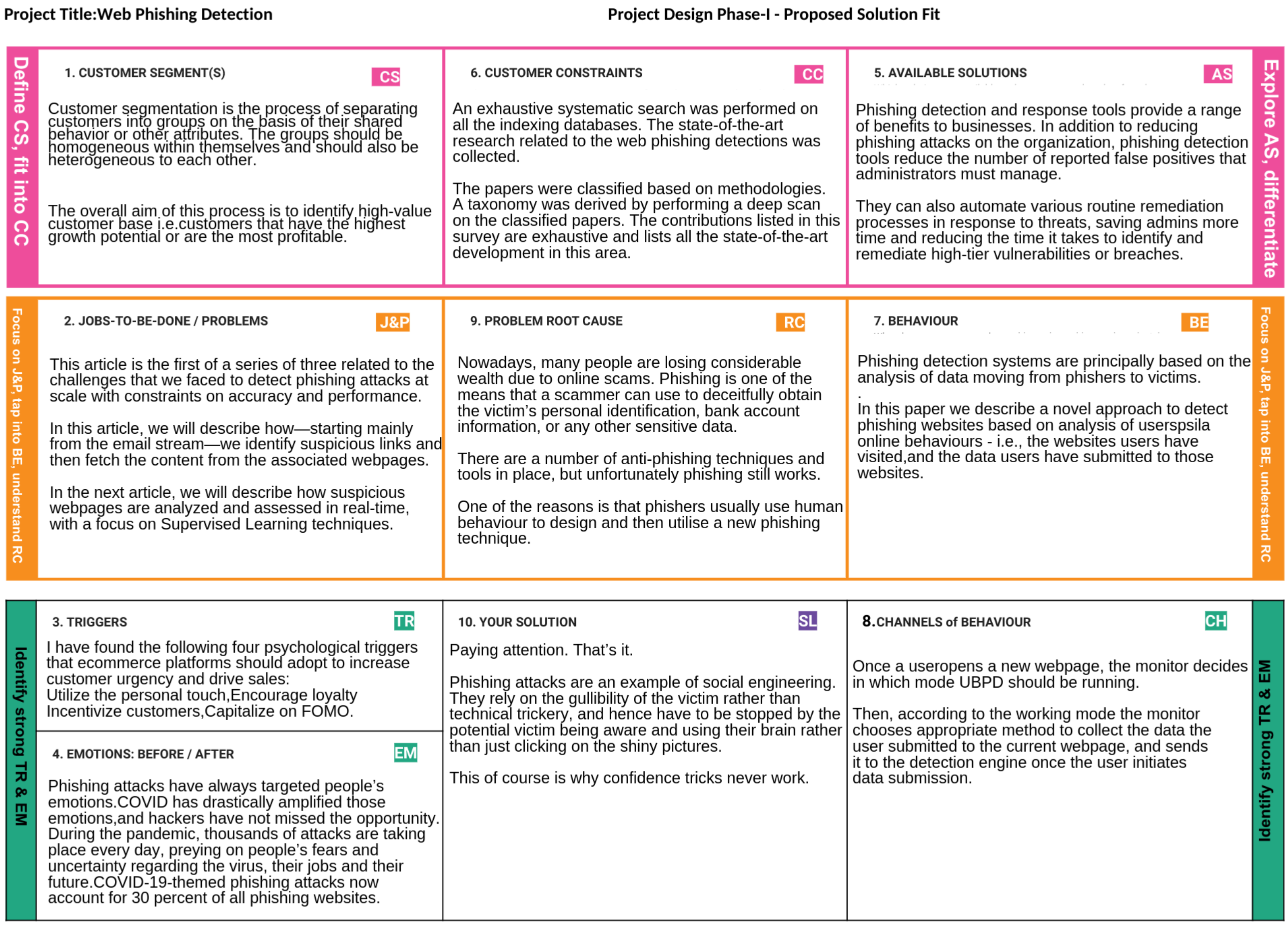
- Most people completely overestimate their ability to identify a phishing attack.
- As users, we’ve been bombarded for years with “phishing” training that has largely been in the form of the “don’t click” ideology.
- Phishing is generally defined as a social engineering attack against the enduser and is the primary attack vector for almost every single cyber-attack.

Scalability Of The Solution

- The tremendous and jaw-dropping growth in the deployment of web applications comes hand-in-hand with apprehensions over security.
- Undeniably, the security of web applications has to be addressed at every step of the software development life cycle (SDLC), and even after the deployment of the application is complete.

3.4 Problem Solution Fit

The Problem-Solution Fit simply means that you have found a problem with your customer and that the solution you have realized for it actually solves the customer's problem.



Project Title:Web Phishing Detection

Project Design Phase-I - Proposed Solution Fit

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

Customer segmentation is the process of separating customers into groups on the basis of their shared behavior or other attributes. The groups should be homogeneous within themselves and should also be heterogeneous to each other.

The overall aim of this process is to identify high-value customer base i.e.customers that have the highest growth potential or are the most profitable.

6. CUSTOMER CONSTRAINTS CC

An exhaustive systematic search was performed on all the indexing databases. The state-of-the-art research related to the web phishing detections was collected.

The papers were classified based on methodologies. A taxonomy was derived by performing a deep scan on the classified papers. The contributions listed in this survey are exhaustive and lists all the state-of-the-art development in this area.

5. AVAILABLE SOLUTIONS AS

Phishing detection and response tools provide a range of benefits to businesses. In addition to reducing phishing attacks on the organization, phishing detection tools reduce the number of reported false positives that administrators must manage.

They can also automate various routine remediation processes in response to threats, saving admins more time and reducing the time it takes to identify and remediate high-tier vulnerabilities or breaches.

Explore AS, differentiate

Focus on J&P, tap into BE, understand RC

2. JOBS-TO-BE-DONE / PROBLEMS J&P

This article is the first of a series of three related to the challenges that we faced to detect phishing attacks at scale with constraints on accuracy and performance.

In this article, we will describe how—starting mainly from the email stream—we identify suspicious links and then fetch the content from the associated webpages.

In the next article, we will describe how suspicious webpages are analyzed and assessed in real-time, with a focus on Supervised Learning techniques.

9. PROBLEM ROOT CAUSE RC

Nowadays, many people are losing considerable wealth due to online scams. Phishing is one of the means that a scammer can use to deceitfully obtain the victim's personal identification, bank account information, or any other sensitive data.

There are a number of anti-phishing techniques and tools in place, but unfortunately phishing still works.

One of the reasons is that phishers usually use human behaviour to design and then utilise a new phishing technique.

7. BEHAVIOUR BE

Phishing detection systems are principally based on the analysis of data moving from phishers to victims.
.
In this paper we describe a novel approach to detect phishing websites based on analysis of userspsila online behaviours - i.e., the websites users have visited,and the data users have submitted to those websites.

Focus on J&P, tap into BE, understand RC

Identify strong TR & EM

3. TRIGGERS TR

I have found the following four psychological triggers that ecommerce platforms should adopt to increase customer urgency and drive sales:
Utilize the personal touch,Encourage loyalty
Incentivize customers,Capitalize on FOMO.

4. EMOTIONS: BEFORE / AFTER EM

Phishing attacks have always targeted people's emotions.COVID has drastically amplified those emotions,and hackers have not missed the opportunity. During the pandemic, thousands of attacks are taking place every day, preying on people's fears and uncertainty regarding the virus, their jobs and their future.COVID-19-themed phishing attacks now account for 30 percent of all phishing websites.

10. YOUR SOLUTION SL

Paying attention. That's it.

Phishing attacks are an example of social engineering. They rely on the gullibility of the victim rather than technical trickery, and hence have to be stopped by the potential victim being aware and using their brain rather than just clicking on the shiny pictures.

This of course is why confidence tricks never work.

8.CHANNELS of BEHAVIOUR CH

Once a useropens a new webpage, the monitor decides in which mode UBPD should be running.

Then, according to the working mode the monitor chooses appropriate method to collect the data the user submitted to the current webpage, and sends it to the detection engine once the user initiates data submission.

Identify strong TR & EM

4. REQUIREMENT ANALYSIS

4.1 Functional Requirement

A function of software system is defined in functional requirement and the behavior of the system is evaluated when presented with specific inputs or conditions which may include calculations, data manipulation and processing and other specific functionality.

- Our system should be able to load air quality data and preprocess data.
- It should be able to analyze the air quality data.
- It should be able to group data based on hidden patterns.
- It should be able to assign a label based on its data groups.
- It should be able to split data into train set and testset.
- It should be able to train model using train set.
- It must validate a trained model using testset.
- It should be able to display the trained model accuracy.
- It should be able to accurately predict the air quality on unseen data.

4.2 Nonfunctional requirement

Nonfunctional requirements describe how a system must behave and establish constraints of its functionality. Some Non-Functional Requirements are as follows:

- Reliability
- Maintainability
- Performance
- Portability
- Scalability
- Flexibility

Resource Requirement

Anaconda 3-5.0.3: Anaconda is a free and open source distribution of the Python and R programming languages for data science, machine learning and other applications.

Jupyter Notebook

The code is fully written in Python language using Jupyter notebook. It is the spin-off projects from the IPython project, which used to have an IPython Notebook project itself.

Hardware Requirements

The following is the hardware requirements of the system for the proposed system:

- Processor : Any Processor above 500 MHz
- RAM : 8 GB
- Hard Disk : 1 TB
- Input device : Standard keyboard and mouse

Software Requirements

The following is the software requirements of the system for the proposed system:

- OS : Windows 10
- Platform : Jupyter Notebook
- Language : Python
- IDE/tool : Anaconda 3-5.0.3

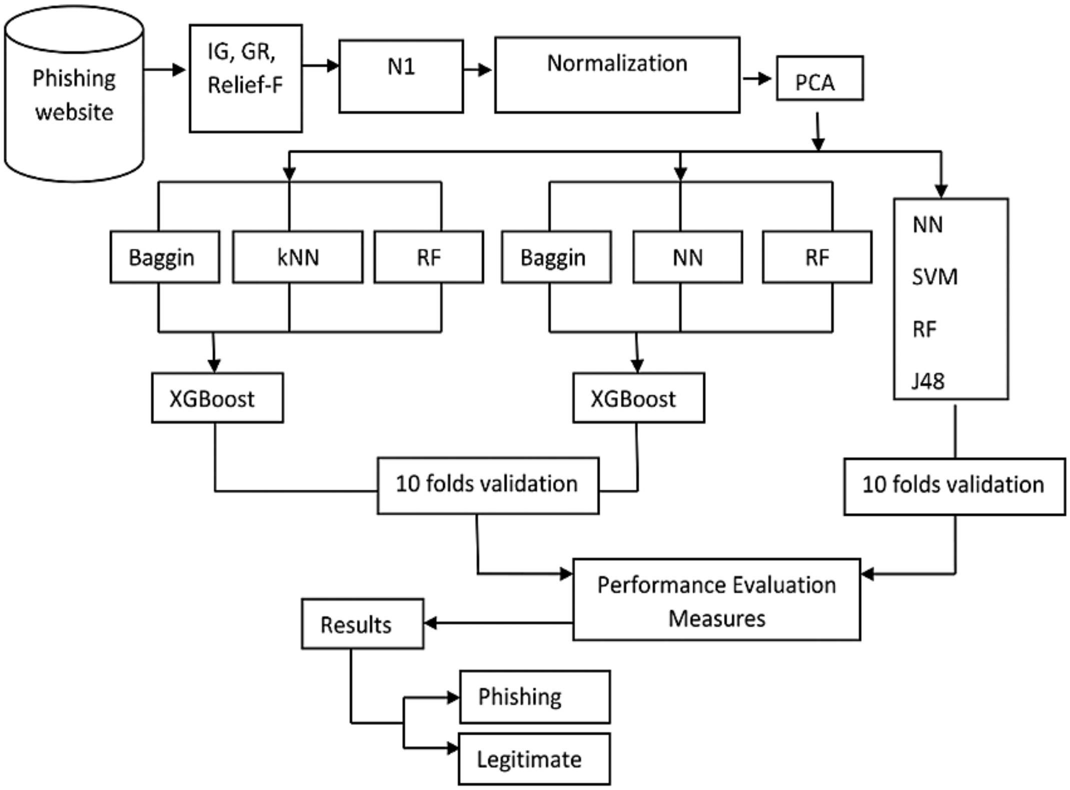
Detection Process. Detecting Phishing Domains is a classification problem, so it means we need labeled data which has samples as phish domains and legitimate domains in the training phase. The dataset which will be used in the training phase is a very important point to build successful detection mechanism.

urlscan.io is a service that allows you to scan and analyze URLs. URLScan records this activity by analyzing the URL it receives from users. As a result, URLScan has many suspicious domains in its pool, among which we can detect phishing domains using some dorks.

5. PROJECT DESIGN

5.1 Data Flow Diagrams

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.



5.2 Solution And Technical Architectiure

Solution architecture is a practice to provide ground for software development projects by tailoring IT solutions to specific business needs and defining their functional requirements and stages of implementation.

A user story is an informal, general explanation of a software feature written from the perspective of the end user or customer. The purpose of a user story is to articulate how a piece of work will deliver a particular value back to the customer.

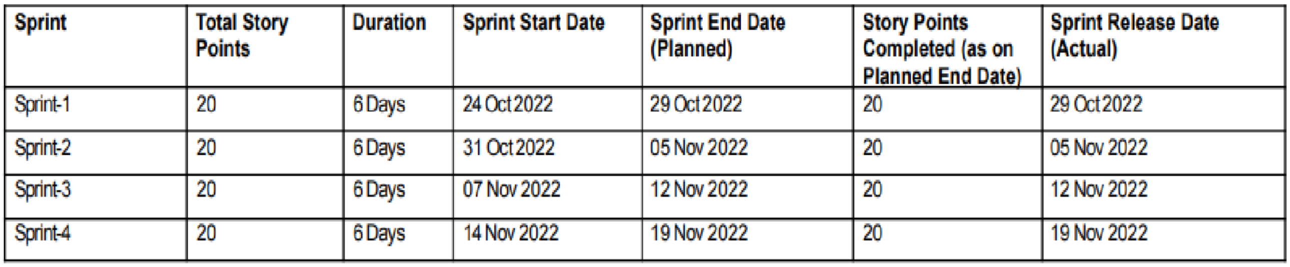
User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (web user)	Registration	USN-1	As a user,I can register my personal details only in official websites.	I can access my account dashboard.	Medium	Sprint-1
		USN-2	As a user,I should create strong passwords.	I can access my account more safely.	High	Sprint-1
		USN-3	As a user,I can register in websites which does not navigate me to any other websites.	I can store my details in correct websites.	Low	Sprint-2
	Login	USN-4	As a user,I can login into required websites.	I can accss my account.	Low	Sprint-1
Customer (Mobile user)	Registration	USN-5	As a user, I can register with verification code.	This protects from strangers.	High	Sprint-1
		USN-6	As a user,I should not register at any calls.	I can be saft with attacts.	Medium	Sprint-1
		USN-7	As a user, I should not register in other devices.	I can access in my device.	:Low	Sprint-2
Adminstrator		USN-8	Admin should maintain his/her database safly.	This reduse form phishing.	High	Sprint-2
Customer care		USN-9	As a user, If my account is phished.	I can complain.	High	Sprint-1
		USN-10	As a user,I should not take others information.	I can be punished for it.	Medium	Sprint-1

6. PROJECT PLANNING & SCHEDULING

6.1 Sprint Planning And Estimation

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-1	User input	USN-1	User inputs an URL in the required field to check its validation.	1	Medium	Anuj k
Sprint-1	Website Comparison	USN-2	Model compares the websites using Blacklist and Whitelist approach.	1	High	Arunkumar D
Sprint-2	Feature Extraction	USN-3	After comparison, if none found on comparison then it extract feature using heuristic and visual similarity.	2	High	Divit raj K R
Sprint-2	Prediction	USN-4	Model predicts the URL using Machine learning algorithms such as logistic Regression, KNN.	1	Medium	Mohammad Arsath S
Sprint-3	Classifier	USN-5	Model sends all the output to the classifier and produces the final result.	1	Medium	Anuj k
Sprint-4	Announcement	USN-6	Model then displays whether the website is legal site or a phishing site.	1	High	Divit raj K R
Sprint-4	Events	USN-7	This model needs the capability of retrieving and displaying accurate result for a website.	1	High	Arunkumar D

6.2 Sprint Delivery Schedule



Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	20	6 Days	24 Oct 2022	29 Oct 2022	20	29 Oct 2022
Sprint-2	20	6 Days	31 Oct 2022	05 Nov 2022	20	05 Nov 2022
Sprint-3	20	6 Days	07 Nov 2022	12 Nov 2022	20	12 Nov 2022
Sprint-4	20	6 Days	14 Nov 2022	19 Nov 2022	20	19 Nov 2022

6.3 Reports from JIRA

7. CODING & SOLUTIONING

7.1 Feature 1

Mainly, the feature selection method aims at reducing the feature space dimensionality and enhancing the compactness of features by exploring the most contributing features in order to eliminate the less contributing ones.

In the hybrid phishing detection, feature selection has been an active field of research owing to the curse of high dimensional web data (emails or websites), the existence of many irrelevant features and redundant in the examined web data, and less comprehensive and less effective machine learning classifiers against phishing evolution

For such key challenges, different methods of feature selection have been employed in hybrid phishing detection approaches (Basnet and Sung, 2012; Basnet et al., 2012; Hamid and Abawajy, 2011; Olivo et al., 2013; Toolan and Carthy, 2010).

7.2 Feature 2

It is noteworthy to mention that feature selection methods currently in use have shared the same process of selection involving search procedure and evaluation criterion.

This means that the search procedure often discards or adds one feature against the evaluation criterion.Thus, feature selection methods in use broadly fall into two categories with respect to the search procedure: filter and embedded with classifiers.

Those of the former category, rely on evaluating the features of data without any learning classifier.

Whilst, methods of the latter category incorporate a predetermined learning classifier and use its performance for the purpose of features evaluation.

On the other hand, both categories of feature selection methods may result in either a selective subset of features or a subset of selective and weighted features owing to the concept of selection that they employ.

Accordingly, they fall into two kinds of methods, namely feature subset selection methods, and features weighting methods.

8. TESTING

8.1 Test Cases

For the URL verifier module in the ISOT phishing detection system, phishing detection is done using 16 different heuristic rules.

In the system, 11 main classes were defined, and 1 class was defined with 5 sub-classes. This covers all 16 heuristic rules.

To test the system, 15 test cases were designed using assertion methods.

Ten test cases were designed to test the 10 main classes and 5 test cases were designed to test the class with five sub-classes.

The getter-setter method was used to test the class with five sub-classes.

The getter method is used to obtain or retrieve a variable value from the class, and the setter method is used to store the variables.

The class with five subclasses checks the 5 different heuristic rules, length of the URL, number of dots and slashes in the URL, presence of @ symbols in the URL, IP address mentioned in the URL, and the presence of special character such as ',', '_', ';' in the URL.

Initially, only a single test case was created for the class with five sub-classes, but it was failing as this class has five methods. After applying the getter setter method, all the test cases passed without any issues.

8.2 UserAcceptance Testing

User Acceptance Testing (UAT) is a type of testing performed by the end user or the client to verify/accept the software system before moving the software application to the production environment. UAT is done in the final phase of testing after functional, integration and system testing is done.

8.2.1 Purpose of Document

The purpose of this document is to briefly explain the test coverage and open issues of [Web Phishing Detection] project at the time of the release to User Acceptance Testing (UAT).

8.2.2 Defect Analysis

Section	Total Cases	Not Tested	Fail	Pass
Print Engine	10	0	0	10
Client Application	50	0	0	50
Security	5	0	0	4
Outsource Shipping	3	0	0	3

This report shows the number of resolved or closed bugs at each severity level, and how they were resolved

Resolution	Severity 1	Severity 2	Severity 3	Severity 4	Subtotal
By Design	10	4	2	3	20
Duplicate	1	0	3	0	4
External	2	3	0	1	6
Fixed	10	2	4	20	36
Not Reproduced	0	0	1	0	1
Skipped	0	0	0	0	0
Won't Fix	0	0	2	1	3
Totals	23	9	12	25	60

8.2.3 Test Case Analysis

This report shows the number of test cases that have passed, failed, and untested

Exception Reporting	10	0	0	9
Final Report Output	10	0	0	10
Version Control	4	0	0	4

9. RESULTS

9.1 Performance Metrics

This paper presents the performance of machine learning classification model for phishing detection using a lightweight Google chrome extension. PhishNet was developed to detect phishing sites on the web. PhishNet provides a convenient solution to reduce the risk of phishing which in return would effectively alleviating the fear users feel when submitting sensitive information on the web.

The paper was able to evaluate the performance of three machine learning tools namely Random Forest, K-Nearest Neighbor and Support Vector Machine. The result given proved that Random Forest performed better than the other two machine learning tools. Consequently, our study has proffered a better solution to the issue of phishing attack on web pages.

The major shortcoming of this approach is its over-dependence on webpage content. Further work is hereby recommended in this area for future study.

Furthermore, the paper recommends more data to be gathered in the future to get more accurate results and the use of other machine learning tools could be tested.

10. ADVANTAGES AND DISADVANTAGES

Advantages

•This system can be used by many E-commerce or other websites in order to have good customer relationship.

•Users can make online payments securely.

•Data mining algorithm used in this system provides better performance as compared to other traditional classifications algorithms.

•With the help of this system user can also purchase products online without any hesitation.

Disadvantages

•If the Internet connection fails, this system won’t work.

•All website related data will be stored in one place.

11. CONCLUSION

It is outstanding that a decent enemy of the phishing apparatus ought to anticipate the phishing assaults in a decent timescale. We accept that the accessibility of a decent enemy of phishing devices at a decent time scale is additionally imperative to build the extent of anticipating phishing sites. This apparatus ought to be improved continually through consistent retraining. As a matter of fact, the accessibility of crisp and cutting-edge preparing dataset which may be gained utilizing our very own device [30, 32] will help us to retrain our model consistently and handle any adjustments in the highlights, which are influential in deciding the site class. Albeit neural system demonstrates its capacity to tackle a wide assortment of classification issues, the procedure of finding the ideal structure is very difficult, and much of the time, this structure is controlled by experimentation.Our model takes care of this issue via computerizing the way toward organizing a neural system conspire; hence, on the off chance that we construct an enemy of phishing model and for any reasons we have to refresh it, at that point our model will encourage this procedure, that is, since our model will mechanize the organizing procedure and will request scarcely any client defined parameters.

12. FUTURE SCOPE

In the future if we get a structu red dataset of phishing we can perform phishing detection much faster than any other technique.In future we can use a combination of any other two or more classifiers to get maximum accuracy. We also plan to explore various phishing techniques that use Lexical features, Network based features,Content based features, Webpage based features and HTML and JavaScript features of web pages which can improve the performance of the system. In particular, we extract features from URLs and pass it through the various classifiers.

13. APPENDIX

Source Code

About.css

```
* {
   margin: 0;
   padding: 0;
   height: 100hv;
   box-sizing: border-box;
}

body{
   width: 100%;
   height: 100vh;
   background-repeat: no-repeat;
   background-size: cover;
   background-color: cadetblue;
}



.menu_bar {
   background-color:rgb(255, 255, 0);
   height:60px;
```

```
    width: 100%;
    display: flex;
    align-items: center;
    justify-content: space-between;
    padding: 0 5%;
    box-shadow:0px 0px 25px black;

}
h2{
box-shadow:0px 0px 25px black;
padding: 7px 20px;
margin-right: 15px;
box-shadow:0px 0px 25px black;
border-radius: 5px;
}

.menu_bar ul {
    list-style: none;
    display: flex;


}


.menu_bar  ul li {
    padding: 10px 20px;
    margin-right: 15px;
}
.menu_bar ul li a{
    color: var(--color-white);
    text-decoration: none;
    font-size: 20px;

}

button {
    padding: 9px 20px;
    border-radius: 45px;
    cursor: pointer;
    font-size: 15px;
    background-color: rgb(2, 255, 213);
    color: var(--color-white);
}

h1{
    position: absolute;
    top: 45%;
    left: 50%;
    bottom: 0.5px;
    color: rgb(255, 255, 255);
    text-shadow:0px 0px 25px black;
    transform: translate(-50%,-50%);
}

h1:after{
 content: "";
   height: 5px;
   width: 50px;
   background-color: rgb(255, 0, 111);
   display: block;
   margin: auto;

}

h4{
  text-align: left;
  position: absolute;
    top: 53%;
    left: 38%;
    bottom: 15px;
    transform: translate(-70%,-50%);
    color: rgb(255, 253, 255);
    text-shadow:0px 0px 25px black;

}

.content{
  position: absolute;
    top: 55%;
    left: 74%;
    bottom: 10px;
    transform: translate(-50%,-10%);
    padding: 1px;
    font-family: 'Times New Roman';
 text-justify: auto;
    color: rgb(255, 255, 255);
    text-shadow:0px 0px 25px black;
```

```
}
img{
    position: absolute;
    top: 105%;
    left: 12%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(1, 1, 1);
}
```

Content.css

```
* {
    margin: 0;
    padding: 0;
    height: 100hv;
    box-sizing: border-box;
}

body{
    background-color: rgb(132, 240, 247);
}

h1{
 position: absolute;
    top: 40%;
    left: 30%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(15, 15, 15);
}

.menu_bar {
    background-color:rgb(255, 255, 0);
    height:60px;
    width: 100%;
    display: flex;
    align-items: center;
    justify-content: space-between;
    padding: 0 5%;
    box-shadow:0px 0px 25px black;

}

h2{
    box-shadow:0px 0px 25px black;
    padding: 7px 30px;
    margin-right: 15px;
    box-shadow:0px 0px 25px black;
    border-radius: 5px;


    }
.menu_bar ul {
    list-style: none;
    display: flex;
}
```

```
.menu_bar  ul li {
    padding: 10px 30px;
}

.menu_bar ul li a{
    color: var(--color-white);
    text-decoration: none;
    font-size: 20px;
}

h3{
    position: absolute;
    top: 70%;
    left: 40%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(2, 2, 2);
}
```

Getstarted.css

```
* {
    margin: 0;
    padding: 0;
 height: 100hv;
    box-sizing: border-box;
}
body{
    width: 100%;
    height: 100vh;
    background-repeat: no-repeat;
    background-size: cover;
    background-color: rgb(0, 149, 255);
}

h1{
    position: absolute;
    top: 60%;
    left: 15%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(255, 255, 255);
}
h2{
    box-shadow:0px 0px 25px black;
    padding: 7px 20px;
    margin-right: 15px;
    box-shadow:0px 0px 25px black;
    border-radius: 5px;
    }
  h4{
        position: absolute;
        top: 75%;
        left: 15%;
        padding-bottom: 6%;
        transform: translate(-20%,-60%);
        color: rgb(1, 1, 1);
    }
    .btn{
        position: absolute;
        top: 90%;
        left: 15%;
        padding-bottom: 6%;
        transform: translate(-20%,-60%);
        color: rgb(248, 244, 244);
 }
.menu_bar {
    background-color:rgb(255, 255, 0);
    height:60px;
    width: 100%;
    display: flex;
    align-items: center;
    justify-content: space-between;
    padding: 0 5%;
    box-shadow:0px 0px 25px black;

}
.menu_bar ul {
    list-style: none;
    display: flex;

}
.menu_bar  ul li {
    padding: 10px 20px;
    margin-right: 15px;
}
```

```
.menu_bar ul li a{
    color: var(--color-white);
    text-decoration: none;
    font-size: 20px;

}
button {
    padding: 9px 20px;
    border-radius: 45px;
    cursor: pointer;
    font-size: 15px;



    background-color: rgb(7, 255, 251);
}



h3{
 position: absolute;
    top: 105%;
    left: 50%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(1, 1, 1);
}

img{
    position: absolute;
    padding: 9px 10px;
    border-radius: 25px;
    top: 70%;
    left: 50%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(1, 1, 1);
}
```

Predict.css

```
* {
    margin: 0;
    padding: 0;
    height: 100hv;
    box-sizing: border-box;
}

body{
background-color: rgb(0, 181, 90);
}

h1{
    position: absolute;
    top: 40%;
    left: 30%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(0, 0, 0);
}
```

```
.menu_bar {
    background-color:rgb(255, 255, 0);
    height:60px;
    width: 100%;
    display: flex;
    align-items: center;
    justify-content: space-between;
    padding: 0 5%;
    box-shadow:0px 0px 25px black;

}

h2{
    box-shadow:0px 0px 25px black;
    padding: 7px 30px;
    margin-right: 15px;
    box-shadow:0px 0px 25px black;
    border-radius: 5px;


    }

.menu_bar ul {
    list-style: none;
    display: flex;
}


.menu_bar  ul li {
    padding: 10px 30px;
}

.menu_bar ul li a{
    color: var(--color-white);
    text-decoration: none;
    font-size: 20px;
}
```

Style.css

```
* {
    margin: 0;
    padding: 0;
    height: 100hv;
    box-sizing: border-box;
}
body{
    background-color: rgb(0, 181, 90);
}

h1{
    position: absolute;
    top: 40%;
    left: 30%;
    padding-bottom: 6%;
    transform: translate(-20%,-60%);
    color: rgb(0, 0, 0);
}

.menu_bar {
    background-color:rgb(255, 255, 0);
    height:60px;
    width: 100%;
    display: flex;
    align-items: center;
    justify-content: space-between;
    padding: 0 5%;
    box-shadow:0px 0px 25px black;

}

h2{
    box-shadow:0px 0px 25px black;
    padding: 7px 30px;
 margin-right: 15px;
    box-shadow:0px 0px 25px black;
    border-radius: 5px;


    }

.menu_bar ul {
    list-style: none;
    display: flex;
}


.menu_bar  ul li {
    padding: 10px 30px;
}
```

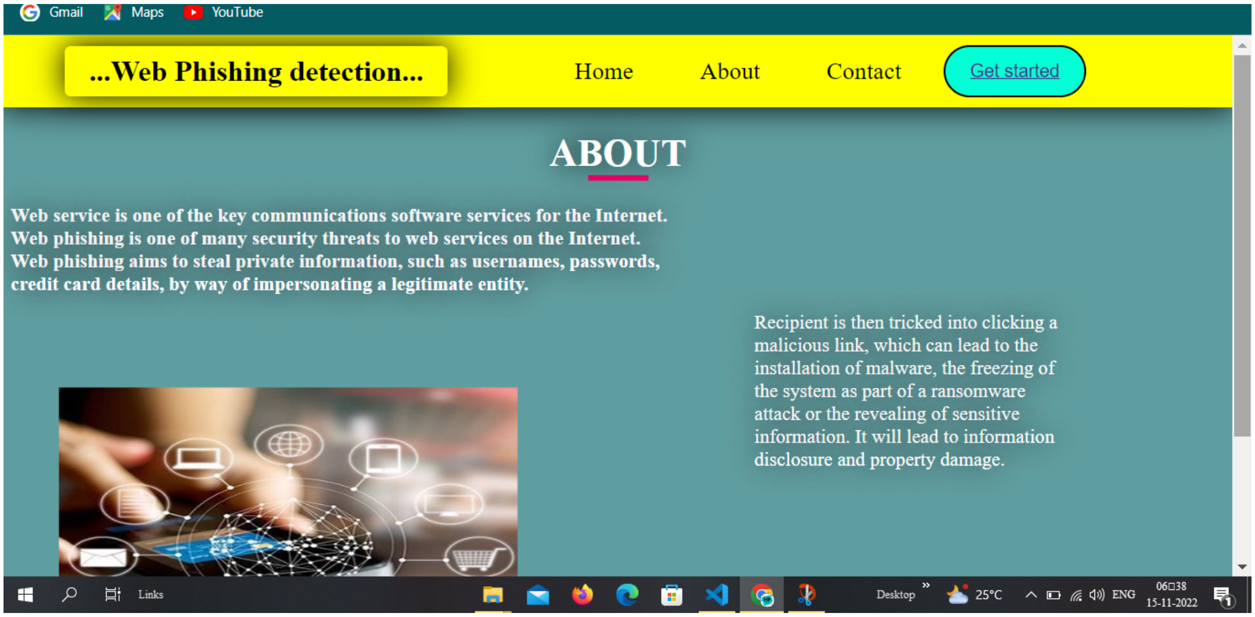
```
.menu_bar ul li a{
    color: var(--color-white);
    text-decoration: none;
    font-size: 20px;
}
.main{
    position: absolute;
    top: 50%;
    left: 50%;
    transform: translate(-50%,-50%);
}

input{
border: 3px solid rgb(255, 3, 192);
    height: 40px;
    width: 600px;
    /* padding-left: 20px; */
    box-shadow:0px 0px 25px black;
}

form{
    position: absolute;
    top: 50%;
    left: 50%;
    transform: translate(-50%,-50%);
}


#submit {
    position: absolute;
    top: 100px;
    left: 50%;
    transform: translate(-50%,-50%);
    font-size: larger;
    font-family:'Times New Roman';
    cursor: pointer;
    border-radius: 10px;
    height: 50px;
    width: 200px;
}
#sumbit:hover{
    background-color: rgb(2, 166, 255);
    border-radius: 10px;
    box-shadow:0px 0px 5px rgb(2, 166, 255),0px 0px 50px rgb(2, 166, 255),0px 0px 50px rgb(2, 166, 255);
}
```

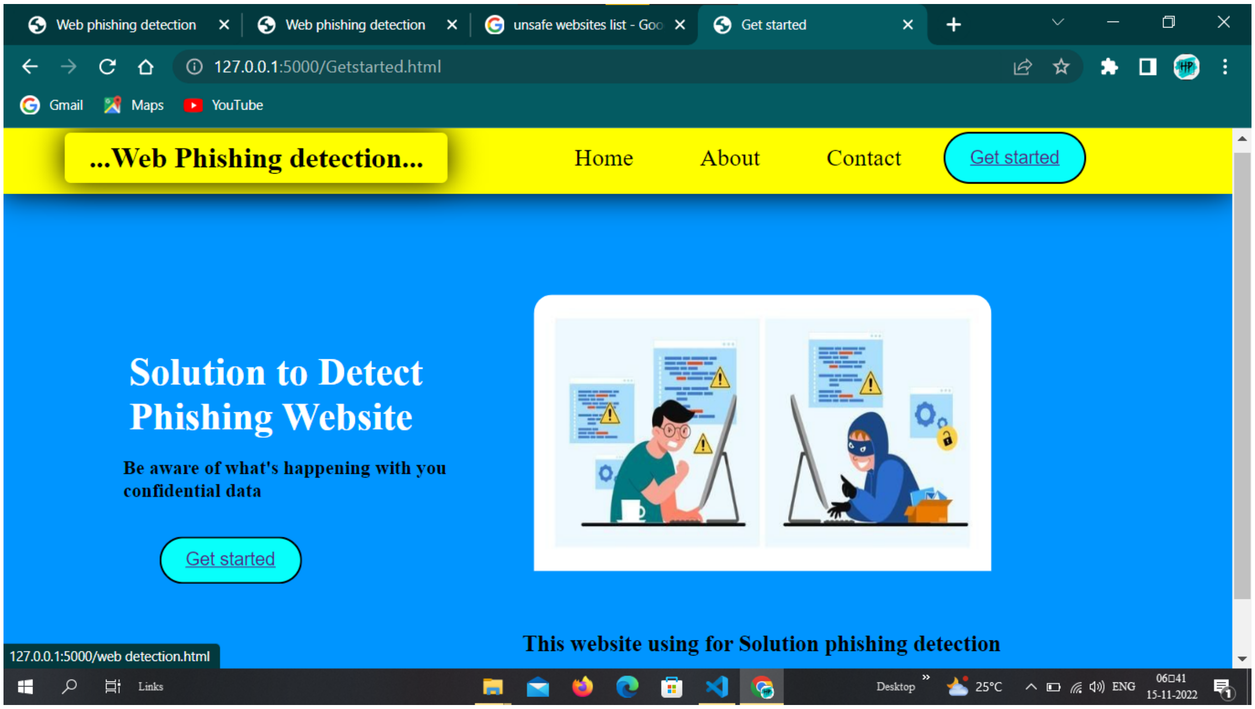
SCREEN SHOTS



ABOUT

Web service is one of the key communications software services for the Internet. Web phishing is one of many security threats to web services on the Internet. Web phishing aims to steal private information, such as usernames, passwords, credit card details, by way of impersonating a legitimate entity.

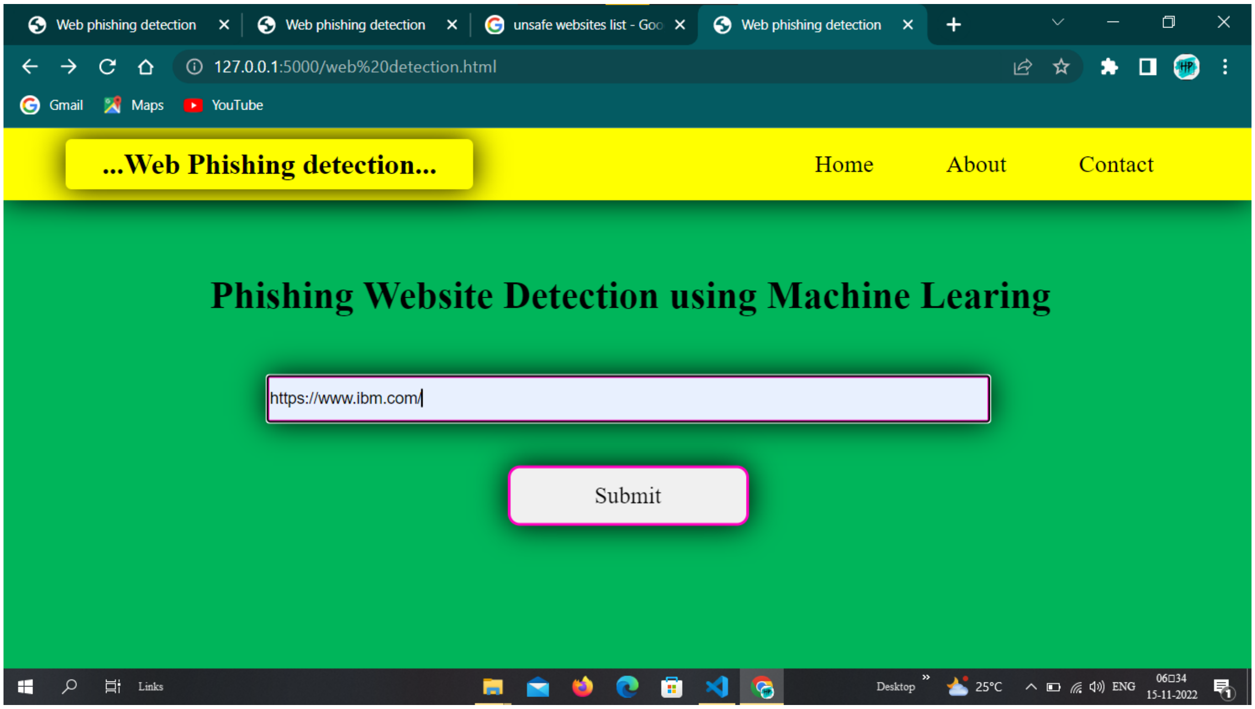
Recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. It will lead to information disclosure and property damage.



Solution to Detect Phishing Website

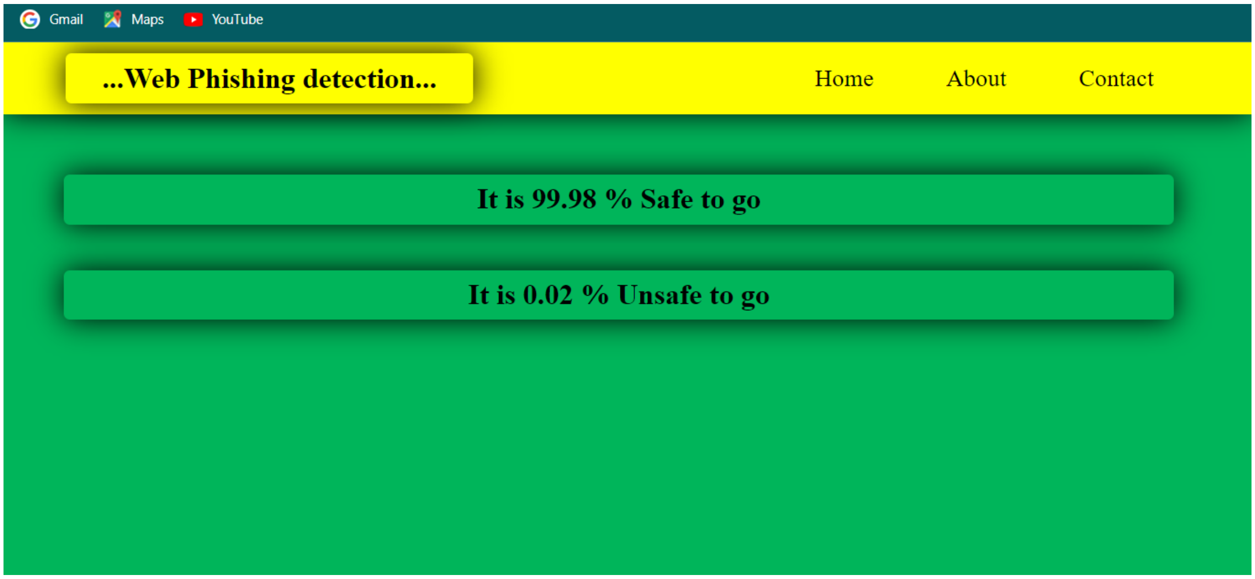
Be aware of what's happening with you confidential data

This website using for Solution phishing detection



Phishing Website Detection using Machine Learing

https://www.ibm.com/



It is 99.98 % Safe to go

It is 0.02 % Unsafe to go

GitHub & Project Demo Link

GitHub Link: https://github.com/IBM-EPBL/IBM-Project-31859-1660205675

Project Demo link:
https://drive.google.com/file/d/15c3lq_lFdkwhUFDWDCdRSiuDq0Y47vm/view?usp=share_link