

JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY (JKUAT)

DEPARTMENT OF COMPUTING

ICS2406: COMPUTER SYSTEMS PROJECT

PROJECT PROPOSAL REPORT

REF: JKU/2/83/022

**YOUR TITLE: RESEARCH ON INTERNET FRAUD PROTECTION FOR ONLINE SHOPPERS.**

***Author***

Name: **STANLEY NGUGI CHEGE**

Reg. No: **SCT212-0065/2017**

Sign:

Submission Date:

Course: **BSc. COMPUTER TECHNOLOGY**

***Supervisor 1***

Name:

Sign:

Date:

***Supervisor 2***

Name:

Sign:

Date:

***Supervisor 3***

Name:

Sign:

Date:

**Period: 2021 – 2022**

# Abstract

With the success of online businesses such as E-commerce platforms, cybercrimes have been on the rise. Often a fake website is publicly deployed to trick users into believing that the website is legitimate and safe to give away sensitive information such as passwords and credit card details. The perpetrators then use phishing techniques to attract vulnerable internet users. Users tend to overlook the URL of a website as the attacker may intelligently disguise themselves. This research will present a fraudulent URL detection mechanism to help internet users to stay protected from cyber criminals. This will be achieved by training a machine learning model to characterize the behavior of phishing attacks and therefore formulate a basis to predict the legitimacy of a URL. This will also provide suggest a response mechanism to alert an internet user in case of a fraudulent URL visit. This will enable online merchants and consumers to verify the authenticity of a website so that they can perform any business or data transactions with them without any hesitation.

Contents

[Abstract 2](#_Toc80518472)

[Contents 3](#_Toc80518473)

[Introduction 4](#_Toc80518474)

[1.1 Background 4](#_Toc80518475)

[1.2 Problem Statement 4](#_Toc80518476)

[1.3 Justification 5](#_Toc80518477)

[1.4 Objectives 5](#_Toc80518478)

[1.5 Research Questions 5](#_Toc80518479)

[1.6 Literature Review 5](#_Toc80518480)

[1.7 Research Methods and Design 7](#_Toc80518481)

[1.7.1 Data collection 7](#_Toc80518482)

[1.7.2 Data Analysis 7](#_Toc80518483)

[1.7.3 System implementation 7](#_Toc80518484)

[1.7.4 System Testing and Evaluation 9](#_Toc80518485)

[1.8 Schedule 9](#_Toc80518486)

[1.9 Budget 10](#_Toc80518487)

[2.0 Introduction 11](#_Toc80518488)

[2.1 Related Works 11](#_Toc80518489)

[2.2. Automated phishing detection 11](#_Toc80518490)

[2.2.1 Blacklist and whitelists Approach 11](#_Toc80518491)

[2.2.2 Heuristic Approach 12](#_Toc80518492)

[2.2.3 Machine Learning Approach 12](#_Toc80518493)

[2.3. Security indicators 12](#_Toc80518494)

[2.4 Machine Learning Algorithms 13](#_Toc80518495)

[2.5 Features Extraction 14](#_Toc80518496)

[2.6. Why Phishing Still works 16](#_Toc80518497)

[References 17](#_Toc80518498)

# Introduction

## 1.1 Background

Online businesses such as E-commerce platforms, auctioning websites and drop-shipping services are becoming the go-to model for most business today in order to keep their businesses afloat. Cyber Security threats have also been on the rise as we become more and more reliant on technology in our everyday lives. According to Sarno et al. (2019), often times such threats are a result of phishing scams in which individuals are tricked into clicking on malicious links attached to emails that are spoofed to look legitimate.

The number of phishing attacks has been growing considerably in recent years and is considered as one of the most dangerous modern internet crimes, which may lead individuals to lose confidence in e-commerce. Consequently, it has a tremendous negative effect on online commerce, marketing efforts, organizations’ incomes, relationships, customers, and overall business operations. (Ali, W. et.al., 2017). In a study conducted by Retruster in 2019, phishing is responsible for 90% of data breaches; Around 1.5M phishing sites are created every month; 30% of targets fall for phishing traps. Phishing attacks are not only increasing with time, but also evolving.

The Anti-Phishing Working Group (APWG) is an international consortium that brings together enterprises affected by phishing attacks. With support from 2300+ members and 1700 companies and agencies, The APWG tracks the number of unique phishing sites reported across the globe by the community. The following statistics were reported by APWG in the first quarter of 2021:

|  |  |  |  |
| --- | --- | --- | --- |
|  | January | February | March |
| Number of unique phishing Web sites detected | 245,771 | 158,898 | 207,208 |
| Number of brands targeted by phishing campaigns | 430 | 407 | 465 |

Phishing cases reported in January 2021 were the most reported cases ever reported to APWG. This is only a primary measure of reported phishing cases across the globe. There are clearly not enough prevention mechanisms in place to protect online consumers from attackers.

## 1.2 Problem Statement

Internet fraudsters, an elite team of cyber-criminals, are individuals who make use of technology to commit malicious activities on the internet with the intention of personal gain such as making profits. The absence of laws that restrict the acquisition of domains for online businesses and the ease of acquiring them paves way for internet fraudsters who acquire domains with malicious intentions. They are able to disguise their identities and IP addresses through the use of Virtual Private Networks and proxies which makes it difficult to track them once their deception comes to light.

Most internet users are not computer security specialists and are therefore vulnerable to an attack. A phishing email would easily capture their attention and they will fall under the control of the phisher. The problem can be minimized by addressing it in two folds; developing more targeted anti-phishing detection and interventions techniques; implementing a round-the clock protection mechanism to notify internet users in case they come across fraudulent URLs.

## 1.3 Justification

As phishers evolve and sharpen their skills, it becomes more difficult for novice users to detect or distinguish phishing websites from legitimate ones. Therefore, there is need to provide anti-phishing solutions that adopt Machine Learning which tends to be more practical and effective in combating phishing. Machine Learning anti-phishing techniques rely on website features to derive knowledge that can assist in identifying phishing websites. Phishing campaigns usually take significantly lower times in their attack (a few hours) such that relying on blacklists and whitelists does not guarantee their detection. Therefore, a binary classification of websites as either legitimate or fraudulent in real time will help internet users stay ahead of the game as they protect themselves from cyber attacks

## 1.4 Objectives

The main objective of the study is to make use and evaluate the efficiency of Supervised Machine Learning in the detection and classification of websites as fraudulent or legitimate. To achieve this, the following objectives will be met:

1. To train a machine learning model using a dataset to classify websites as legitimate or fraudulent.
2. To collect, analyze and organize training and testing dataset.
3. To identify common distinguishing features between fraudulent and legitimate websites
4. To develop an application that uses the trained machine learning model to provide a round-the clock protection mechanism to keep the user aware of suspicious websites

## 1.5 Research Questions

1. How will the machine learning model be trained using a dataset to classify websites as legitimate or fraudulent?
2. How will the dataset be collected, analyzed and organized?
3. What properties of a website will be used to distinguish legitimate and fraudulent websites?
4. How will an application that uses the trained machine learning model be implemented to provide a round-the-clock protection mechanism to keep users aware of suspicious websites?

## 1.6 Literature Review

Phishing is a type of social engineering attack often used to trick users into revealing private or sensitive information by masquerading as a trusted entity. These attacks occur in large numbers and have caused billions of dollars in losses (R. Verma et al., 2018).

**How Phishing is conducted**

An attacker conducts a successful phishing in 5 stages (Anjum & Shabut et al., 2016):

Stage 1: **Planning and Setup**: the attackers identify the target, digs out the essential details regarding their target, then set up the attacks to redirect the victim to the fraudulent URL.

Stage 2: **Phishing**: The attackers disguise themselves as some reputable organization, attract victim(s) and request confidential information from them.

Stage 3: **Break-in/Infiltration**: The victim clicks on the malicious link and either a malware that allows the attacker to access the device automatically installs on his device or the victim is redirected to a URL.

Stage 4: **Data Collection**: As soon as the attackers gain access to the victim’s system, they extract the required data.

Stage 5: **Break-out/Ex-filtration**: Once the attacker has access and gained the required information, they remove all the evidence then track the degree of success of their attack to refine their future attacks

**How Phishing is detected**

Two popular approaches are used to detect the phishing websites (Ali, Waleed, et al., 2017):

1. **Blacklist and whitelist-based approach**: Blacklists are essentially a database of URLs that have been confirmed to be malicious in the past. This database is compiled over time (often through crowd-sourcing solutions, e.g., PhishTank (LLC OpenDNS. et al., 2016). The main drawback of the blacklist and whitelist-based approach is that it cannot distinguish the newly created phishing websites from legitimate websites
2. **Intelligent heuristics-based approach**: In this approach, some features of websites are collected and evaluated to select the most influential website features, which play an important role in detecting the phishing websites. The selected significant features of many websites can be utilized as training dataset. Then, the machine learning techniques are trained based on the prepared training dataset in order to effectively classify the websites as either phishing or legitimate.

**SUPERVISED MACHINE LEARNING**

Machine learning concentrates on developing the computational algorithms that reason and induce patterns and rules from externally supplied instances and prior data in order to produce general models, which are able to make predictions about future instances. The machine learning is called supervised if known labels are given with instances in the training phase, whereas instances are unlabeled in unsupervised machine learning. (D. Sahoo et. al 2019.)

The phishing website can be detected based on some important characteristics like URL and Domain identity, and security and encryption criteria in the final phishing detection rate. According to APWG (et al. 2021), Phishers continue to use certain domain name registrars to obtain domains for their schemes. In a URL, lexical features can be extracted such as the URL string, information about the host, and sometimes even HTML and JavaScript content. Host-based features obtained from the hostname properties of the URL allow us to know the location, identity, and the management style and properties of malicious hosts. An underlying assumption is that there is an array of features to differentiate malicious and benign URLs. Based on this information, a prediction model can be built, which can make predictions on new URLs. This can be formalized as a binary classification task of a machine learning algorithm. (D. Sahoo et. al 2019.)

## 1.7 Research Methods and Design

Various data collection and analysis methods will be used to gather data for this research.

### 1.7.1 Data collection

The primary requirement for training a machine learning model is the presence of training data. In the context of malicious URL detection, this would correspond to a set of large number of URLs. This will use a set of URLs as training data, and based on the statistical properties, learn a prediction function to classify a URL as malicious or benign. Data required for this will be acquired through the following methods:

1. **Web scrapping** – This will involve collecting dataset containing phishing and legitimate websites from open-source platform. An example of such an open-source project is PhishTank (LLC OpenDNS. et al., 2016).
2. **Published Documents and journals**- Written journals, books, reports and material gathered from previous research will be assessed to gather as much data as possible. Data drawn from published documents will provide supplementary research data.

### 1.7.2 Data Analysis

Once all the required data has been gathered, cleaning, transforming, and modeling operations will be conducted on the data to discover useful information. The following activities will be undertaken in order to draw out computable characteristics on the acquired dataset.

1. Write a program to extract various distinguishing features of a URL such as the domain name (or IP address), protocol and the suffix.
2. Analyze the dataset using Exploratory Data Analysis tools
3. Divide the data into training and testing sets

### 1.7.3 System implementation

The proposed system will be Web-based system which will make use of the following technologies during development:

**Front-End Language(s)**

|  |  |
| --- | --- |
| **Language** | **Justification** |
| **HTML** | Necessary in order to create pages to are displayed on the world wide web |
| **CSS** | Necessary for defining the style properties of Web page elements, including colors, layout, and fonts |
| **JavaScript** | Necessary for dynamic and interactive user-experience |

**Back-End Language(s)**

|  |  |
| --- | --- |
| Language | Justification |
| PHP | PHP codes runs much faster than other server scripting languages such as ASP which makes it ideal for this system |
| SQL | Used to perform tasks on a database |
| Python | Optimum for machine learning modeling |

**Database Management System**

|  |  |
| --- | --- |
| Software | Justification |
| LAMP (Linux, Apache, MySQL, PHP/Perl/Python) software bundle | This will be used to simulate a hosting environment on a local workstation therefore facilitating database hosting and software testing |

**Integrated Development Environment**

|  |  |
| --- | --- |
| Software | Justification |
| Visual Studio Code | Fast source code editor with multi-language support and offers syntax highlighting, bracket-matching, auto-indentation features and the ability to install plugins on the IDE making it flexible to use |
| Sublime Text | An easy-to-use source code editor, a less sophisticated alternative to visual studio code |

**Prototyping tools**

|  |  |
| --- | --- |
| Language | Justification |
| Figma | A cloud-based tool used to design wireframes and prototypes |

### 1.7.4 System Testing and Evaluation

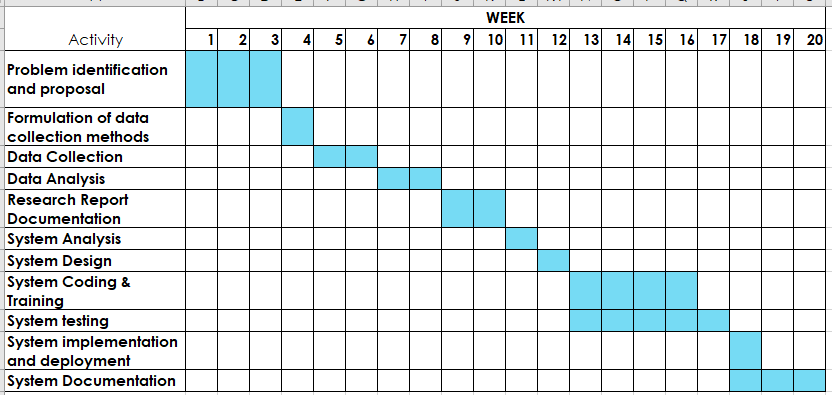
Testing is required to check for software failures so that defects may be discovered and corrected. The following tests will be used to check for errors

|  |  |
| --- | --- |
| Test | Description |
| Functional Testing | To check if the output is as per the requirement or not (ignores the internal system parts and focuses only on the output) |
| Dry Running | To Test sections of a program that are suspected of having an error |
| Syntax checking | To uncover syntax errors by a compiler |
| Unit/module testing | To discover any error that may exist in a module's code |
| Integration testing | To discover any error that may exist by combining modules |
| Desk checking | Manually work through the code, executing each instruction using test cases |

## 1.8 Schedule

The aforementioned research with be carried out in phases during the following estimated timelines

|  |  |
| --- | --- |
| Task | Timeline |
| Problem identification and proposal | 3 Weeks |
| Formulation of data collection methods | 1 Week |
| Data Collection | 2 Weeks |
| Data Analysis | 2 Weeks |
| Research Report Documentation | 2 Weeks |
| System Analysis | 1 Week |
| System Design | 1 Week |
| System Coding | 5 Weeks |
| System testing | 1 Week |
| System implementation and deployment | 1 Week |
| System Documentation | 2 Weeks |



**Fig 1: *Gantt Chart – Project Schedule***

## 1.9 Budget

Below is an estimation of the expected expenses that will be incurred

|  |  |  |
| --- | --- | --- |
| ***Service*** | **Cost** | **Justification** |
| ***Hosting Space and Domain Name Registration*** | 5,000/- | The system will require a hosting space on the World Wide Web for testing and deployment |
| ***Stationery and Printing of material*** | 2,000/- | Printing documentation, binding reports, cost of notebooks and pens |
| *Total* | **7,000/-** | **-** |

Literature Review

## 2.0 Introduction

This chapter consists of related literature on phishing detection and prevention mechanisms acquired from books, journals, academic papers and articles. This includes research on related approaches to phishing detection, machine learning algorithms that have been used to detect phishing, browser security indicators and features that can be used to flag websites as legitimate or fraudulent.

## 2.1 Related Works

Research on phishing detection and prevention mainly explores four areas; automating phishing detection, providing user interface cues to help users detect phishing, educating users about protecting themselves and understanding user's vulnerability (Alsharnouby, Mohamed & Alaca, Furkan & Chiasson, Sonia. 2015). This research mainly explores automating phishing detection and providing user interface cues to help users to detect phishing.

## 2.2. Automated phishing detection

Automatic phishing detectors exist at various levels such as web browser tools, internet service providers and mail servers and clients (Alsharnouby et. al. 2015). These tools restrict access to detected websites or request the website's internet service provider to take it down. Automatic email classification tools make use of machine learning algorithms, spam filter techniques and statistical classifiers to identify potential phishing messages. They have a varying degree of effectiveness and misclassifications are a common occurrence which affects the reliability of the service as users are likely to be intolerant to loosing legitimate messages.

Automated phishing detection techniques to detect phishing websites include the use of blacklists and whitelists, the use of heuristic methods, and use of machine learning principles. (Anjum & Shabut et al., 2016)

### 2.2.1 Blacklist and whitelists Approach

This method often maintains a list of URLs that are labelled as malicious or benign. Whenever a new URL is visited, a database lookup is performed. The URL is checked whether it exists on the list and if it is found the label allocated to it is returned as output. A major problem with this method is the inability to maintain a list of all possible malicious URLs as new URLs can be easily generated daily, thus making it impossible for them to detect new threats. This is a critical concern when the attackers generate new URLs using algorithms, and can therefore bypass all blacklists as the URLs are dynamic (Doyen, Chenghao & Steven, 2019)

PhishTank is a popular blacklist launched in 2006 and has been in service ever since (LLC OpenDNS. 2016). The blacklist is populated through crowdsourcing volunteers who submit potential phishing websites and vote on the legitimacy of websites. PhishTank is not protection. "PhishTank is an information clearinghouse, which helps to pour sunshine on some of the dark alleys of the Internet. PhishTank provides accurate, actionable information to anyone trying to identify bad actors, whether for themselves or for others" (LLC OpenDNS, 2016). PhishTank offers a blacklist for use by other tools through an API. Popular organizations such as Kaspersky, MacAfee, APWG and Avira make use of Phishtank's dataset.

### 2.2.2 Heuristic Approach

Heuristic approaches are similar to blacklist methods since their basic idea is to create a blacklist of signatures. When common attacks are detected, a signature is assigned to the type of attack. The idea is to look out for a signature of malicious activity such as unusual process creation, repeated redirection etc. Intrusion detection systems are able to detect these behaviors and respond to them appropriately. These approaches are able to detect new threats but to a limited extent since new threats may be completely unrelated. Modern heuristic methods analyze the execution dynamics of webpages. They require visiting the actual URL which may initiate the attack. The techniques are resource intensive and require complete execution of the code (including the server-side scripts). The techniques may go undetected since the malware in place may not launch the attack immediately (Sahoo, Liu & Hoi, 2019).

### 2.2.3 Machine Learning Approach

These are intelligent heuristic-based methods which try to analyze the information of a URL and its corresponding webpages by extracting the features of URLs and training a prediction model using training data. In static analysis, the website is analyzed based on the features extracted from the URL string such as lexical features, information about the host, and sometimes the HTML and JavaScript content. The underlying assumption is that the distribution of these features is different for malicious and benign URLs. Using this distribution information, a prediction model can be built, which can make predictions on new URLs. Since no execution is required, they are safer than dynamic approaches which require complete execution of the URL. Dynamic methods monitor the behavior of the websites looking for anomalies. (Sahoo et. al., 2019)

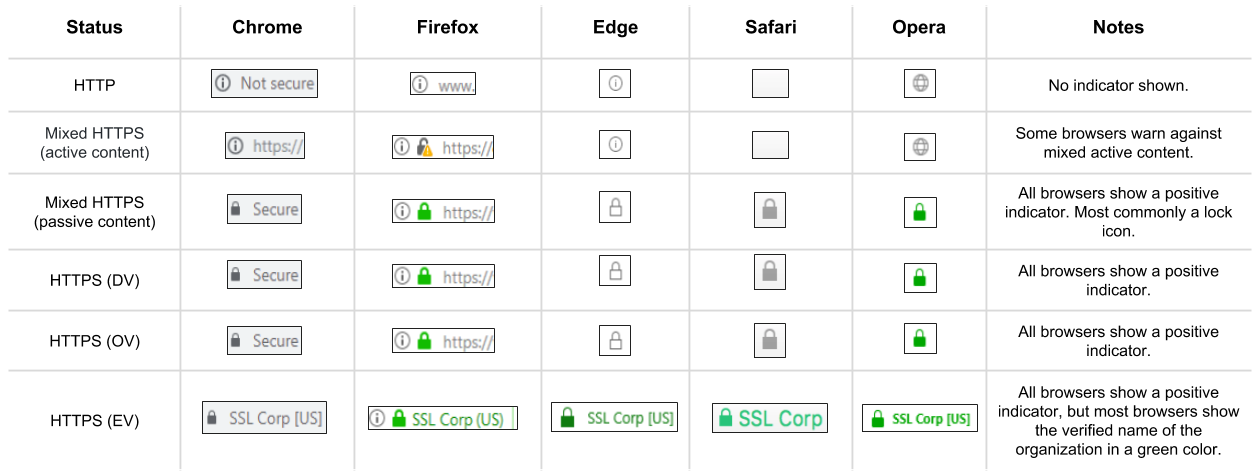
## 2.3. Security indicators

Phishing is primarily a problem because users are unable to verify the authenticity of a website. Security indicators are readily available every time a user launches the web browser. However, an average internet user rarely pays attention to them or may not understand their meaning. In general, most authors consider URL bar HTTPS indicators (SSL/TLS) and digital certiﬁcate indicators as the main cues (Jelovčan, Luka, Vrhovec, Simon, Mihelič, Anže. 2020)

Hypertext Transmission Protocol (HTTP), the most widely used protocol in the world, is the protocol that is used to view web pages. When you type an address, say www.example.com, HTTP is added automatically at the beginning of the address, ie http://www.example.com. HTTP sends and retrieves all data in clear text making it vulnerable to anyone who wants it, eg hackers. Secure Hypertext Transmission Protocol (HTTPS) is used to secure communications by encrypting the data exchanged between a person’s browser and the web site he or she is visiting. HTTPS is especially important on sites that offer online sales or password-protected accounts. Browsers indicate that a website uses HTTPS by use of a padlock (colored in some browsers). (Jelovčan et. al., 2020 & APWG 2021)

Secure Hypertext Transmission Protocol (HTTPS) uses Secure Sockets Layer (SSL), a protocol used to ensure security on the internet using public key encryption. When a computer connects to a website using SSL the computer's browser will ask the website to identify itself. The web server responds by sending the computer a copy of its SSL certificate, a small digital certificate used to authenticate the identity of a website. Once the browser establishes trust with the website, encrypted data can be transmitted to and from the website. (Jelovčan et. al., 2020)

The following table is a summary of the general state of security indicators in modern browsers. Starting with HTTP (which is not secure at all) each item further along the list is more secure than the previous ones. (Naziridis, 2018)



To help users stay safe on the internet, browsers require websites to use certificates from trusted organizations. This is because anyone can create a certificate (e.g., Using OpenSSL) claiming to be whatever website they claim to be. According to APWG (2021), PhishLabs, an active contributor to APWG, has been tracking the proportion of phishing sites that are protected by the HTTPS encryption protocol. Studying HTTP on phishing sites provides insight onto how phishers are fooling Internet users by turning an Internet security feature against them. 83% of the phishing attacks reported to APWG in the first quarter of 2019 used HTTPS protocol.

## 2.4 Machine Learning Algorithms

Several machine learning algorithms have been implemented in real life applications. (Ali, Waleed, 2017). The identification of malicious and legitimate URLs can be regarded as a classification task and some of the popular machine learning algorithms applicable include the following:

1. **Back-Propagation Neural Network (BPNN)**

BPNN are popular algorithms in network models. They are particularly used in prediction and classification problems. They learn in two phases: the forward pass and the backward pass. In the forward pass, the input layer is presented with a training input pattern which is propagated from layer to layer until the desired output is produced. In the backward phase, the output is compared with the anticipated output in order to compute the error. The error is then propagated backward through the network from output to input layers and the weights are adjusted accordingly to minimize the error (Ali et. al., 2017).

1. **Radial Basis Function Network (RBFN)**

RBFN is a type of neural network that uses radial basis functions as activation functions. In the architecture of RBFN, there are three feedback networks: the input layer, the hidden layer and the output layer. In each hidden unit, a radial activation function is implemented while a weighted sum of outputs of hidden units is implemented for each output unit. Learning is conducted in two phases. The first stage involves clustering in order to determine the centers and widths of the hidden layer. In the next phase, the weights connecting the hidden layer with the output layer are optimized through the use of Least Mean Squared (LMS) or Singular Value Decomposition (SVD) algorithms. (Ali et. al., 2017).

1. **Support Vector Machine (SVM)**

SVM, very popular and robust machine earning techniques have been utilized effectively in many applications. They are based on maximizing the margin and thereby creating the largest possible distance between the hyperplane and the instances in order to reduce an upper bound on the anticipated generalization error. Support vectors close to the hyperplane provide the most useful information for classification. An appropriate kernel function is used to transform the data into a high-dimension to use linear discriminate functions (Ali et. al., 2017).

1. **Decision Tree and Random Forest (RF)\* RF ONLY**

In decision trees, a node corresponds to a feature of an instance being classified. The instances are classified through sorting based on feature values. Each branch represents a value that the node can predict. Random Forest is a popular decision tree that can be used for classification and regression. RF is a group of decision trees trained independently on selected training datasets. The classification is then determined by voting among all the trained decision trees. (Ali et. al., 2017).

The performances in terms of correct classification rate (CCR) of the above algorithms were compared together in a study (Ali et. al., 2017). The following table summarizes the results.

|  |  |
| --- | --- |
| **Classifier** | **Correct Classification Rate** |
| Back-Propagation Neural Network (BPNN) | 0.970 |
| Radial Basis Function Network (RBFN) | 0.928 |
| Support Vector Machine (SVM) | 0.963 |
| Random Forest (RF) | 0.971 |

*Fig: Performance measures of the machine learning classifiers*

The Random Forest and Back-Propagation Neural Network classifiers achieved the best correct classification rate while the Radial Basis Function Network attained the lowest.

## 2.5 Features Extraction

Several features can be extracted from a website to distinguish phishing websites from legitimate ones. Feature selection is necessary in order to decrease computation time and to reduce noise and irrelevant features. The choice of extracted features is critical for the success of the detection mechanism in place. Once the selected features are selected, the machine learning model can be trained. (Ali et. al., 2017)

The following features can contribute to the effective prediction of the phishing websites: (Ali et. al., 2017).

|  |  |
| --- | --- |
| Feature Category | Feature Name |
| Address bar-based features | Using the IP Address  Long URL to Hide the Suspicious Part  Using URL Shortening Services “TinyURL”  URL’s having “@” Symbol  Redirecting using “//”  Adding Prefix or Suffix Separated by (-) to the Domain  Sub Domain and Multi Sub Domains  HTTPS (Hyper Text Transfer Protocol with Secure Sockets Layer)  Domain Registration Length  Favicon  Using Non-Standard Ports  The Existence of “HTTPS” Token in the Domain Part of the URL |
| Abnormal-based features | URL of Anchor  Links in <Meta>, <Script> and <Link> tags  Server Form Handler (SFH)  Submitting Information to Email  Abnormal URL |
| HTML and JavaScript-based features | Website Forwarding  Status Bar Customization  Disabling Right Click  Using Pop-up Window  IFrame Redirection |
| Domain-based features | Age of Domain  DNS Record  Website Traffic  Page Rank  Google Index Number of Links  Pointing to Page  Statistical-Reports Based Feature |

## 2.6. Why Phishing Still works

According to Retruster 2019, the problem lies in the detection and reporting of cybercrimes. It can take as long as 50 days from when a breach is discovered until the time when it is reported, a very huge risk for potential victims.

Users consider security as a secondary task. They are prone to concentrating on the real purpose of their interaction with their website making it unlikely for them to notice the security indicators displayed. Some security indicators are also only visible when visiting safe and secure websites (Alsharnouby, et. al., 2015). In a study conducted to assess whether browser security indicators and increased user awareness on phishing have led to users’ improved ability to protect themselves from phishing, a series of websites was presented to participants and they were asked to identify phishing websites. Participants were successfully able to detect only 53% of phishing websites even when forewarned to identify them. Using eye tracking, they found that two thirds of users looked at the SSL lock icon when prompted to be security-conscious but rarely used other cues on the browser-chrome (Alsharnouby, et. al., 2015). Users spend 85% of their time looking at the website content during a web interaction and only 6% of their time looking at security indicators. Even if users doubt the authenticity of the websites, they will still access it, primarily because they want the beneﬁts from it (Jelovčan et. al., 2020).

One major problem with cybercrime is establishing jurisdiction. Physical crimes are bound to a physical location. The crime is therefore considered territorial and its location determines the jurisdiction. Cybercrime activities are not bound to a physical location as the victim and the perpetrator can even be physically at different countries. To worsen the situation, some countries may not have extradition treaties and the law may therefore not be able to prosecute the perpetrators. Legislation of laws on cybercrime is still developing, and it may be challenging to bring justice to those who commit cybercrimes (Plachkinova, 2021).

For these reasons, developing a usable browser security to alert users when they are in danger remains a crucial and unsolved problem in security.

# References

**Rakesh Verma, Devin Crane, and Omprakash Gnawali, (2018). Phishing During and After Disaster: Hurricane Harvey. In 2018 Resilience Week (RWS). IEEE, 88–94**

**Shaikh, Anjum & Shabut, Antesar & Hossain, Alamgir. (2016). A literature review on phishing crime, prevention review and investigation of gaps. 9-15. 10.1109/SKIMA.2016.7916190.**

**LLC OpenDNS. 2016. PhishTank: An anti-phishing site. Online: https://www. phishtank. com (2016).**

**Retruster 2019, Phishing Statistics and Email Fraud Statistics for 2019, Accessed 6 August 2020, <https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html>**

**Ali, Waleed. (2017). Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection. International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080910.**

**Shaikh, Anjum & Shabut, Antesar & Hossain, Alamgir. (2016). A literature review on phishing crime, prevention review and investigation of gaps. 9-15. 10.1109/SKIMA.2016.7916190.**

**Phishing Activity Trends Report, 2021. 1st Quarter 2021 Report, APWG. Activity January-March 2021**

**Ali, W. (2017). Phishing website detection based on supervised machine learning with wrapper features selection. International Journal of Advanced Computer Science and Applications, 8(9), 72-78.**

**Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2019). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. Human factors. doi: 10.1177/0018720819855570**

**Mohammad R., Thabtah F., McCluskey L. Tutorial and critical analysis of phishing websites methods. Computer Science Review Journal. Volume 17, August 2015, Pages 1–24 Elsevier. 2015**

**Doyen Sahoo and Chenghao Liu and Steven C. H. Hoi, 2019. “Malicious URL Detection using Machine Learning: A Survey”. Eprint 1701.07179, arXiv, cs.LG**