

Study of Phishing Attacks and Detection of Spoofing Websites using Machine Learning

Bhavik Shah

17BCN7006

ABSTRACT

Phishing is a type of cyber-crime where spammed messages and fake websites con people to enter their delicate credentials and data which in turn is stolen by the attackers. The goal of this paper is to research how modern-day phishing attacks occur, then to analyze the URLs and the fake websites to search for clues and patterns which can indicate whether they are safe or not, and finally to develop an algorithm so that our computer can classify the same on its own. Classification is a machine learning strategy that can be used to recognize spam, builds and tests models, utilizing diverse blends of settings, and compares various machine learning techniques, and measures the exactness of a prepared model and figures a lot of assessment measurements. During the present study, I was able to find 26 patterns or odd indicators to show a web application is a phishing website and used Neural Network with Adam, SGD, and RMSProp optimizers. The research ends with a final look at the change in the results brought in by Swarm Intelligence Technique with the TDLHBA parameter.

INTRODUCTION

As technology advances, the Internet along with email has become an integral part of one's life. Unfortunately, the flexibility provided by the advancement of technology has at the same time resulted in criminals following the trend. Many problems thus arise, and one of such is identity theft. Recently, one form of identity theft crime that has become a lethal security threat is phishing, targeted primarily at casual email users. Phishing is an illicit endeavor that adventures both social building and specialized misdirection to obtain touchy secret information (e.g. government managed savings number, email address, passwords, and so on.) and money related record certifications. Phishing includes spam messages camouflaged as authentic with a subject or message intended to trap the casualties into uncovering classified data.

Phishing is the most unsafe criminal exercise in cyberspace. Since most of the users go online to access the services provided by the government and financial institutions, there has been a significant increase in phishing attacks for the past few years. Phishers started to earn money and they are doing this as a successful business. Various methods are used by phishers to attack vulnerable users such as messaging, VOIP, spoofed links, and counterfeit websites. It is very easy to create counterfeit websites, which looks like a

genuine website in terms of layout and content. Even, the content of these websites would be identical to their legitimate websites. The reason for creating these websites is to get private data from users like account numbers, login IDs, passwords of debit and credit card, etc. Moreover, attackers ask security questions to answer posing as a high-level security measure providing to users. When users respond to those questions, they get easily trapped in phishing attacks.

The rest of this paper is organized as follows. Section 2 deals with exploring the social engineering framework as humans are the weakest link in the cybersecurity chain. Section 3 explains the different types of phishing attacks in theory. Following which section 4 discusses some examples of phishing attacks and a demo of a small-scale phishing attack. Section 5 explores identifying the URLs if they are safe or malicious. Section 6 deals with the existing detection techniques and section 7 with the algorithms I have used to detect phishing. Finally, section 8 concludes the paper with a summary and remarks.

LITERARY REVIEW

AP Kumar[1] gives us a very overall view of the world of phishing, concerning the challenges which phishing presents to the users and some general ideas of the possible solutions, out of one is being researched in this paper.

Salahdine[10] proposes and studies the social engineering framework which the attackers use, explains the existing counters, and encourages new countermeasures to defend against the same. Chauhan[13], Akamai[10], Shankar[19], and Dr. Damodaram[15] majorly helped in formulating the idea and developing the study on the types of phishing attacks and the examples of phishing attacks occurring in the world.

Authors in this paper[3] have researched the accuracy of different machine learning techniques and have presented the results in a very simple yet elegant table. This formed the basis of this research, encouraging the fact to develop further upon neural network as it showed promising results. Before selecting convolutional neural network as the final algorithm, random forest[4], support vector machine[7], and recurrent neural network[6],[8] were taken into consideration but all of them were crutched on the machine to identify a general pattern which might result in many false positives and false negatives.

The swarm intelligence approach was inspired by the research paper by Fisher[5], where the author has proposed the idea of how swarms generally perform better in nature, and

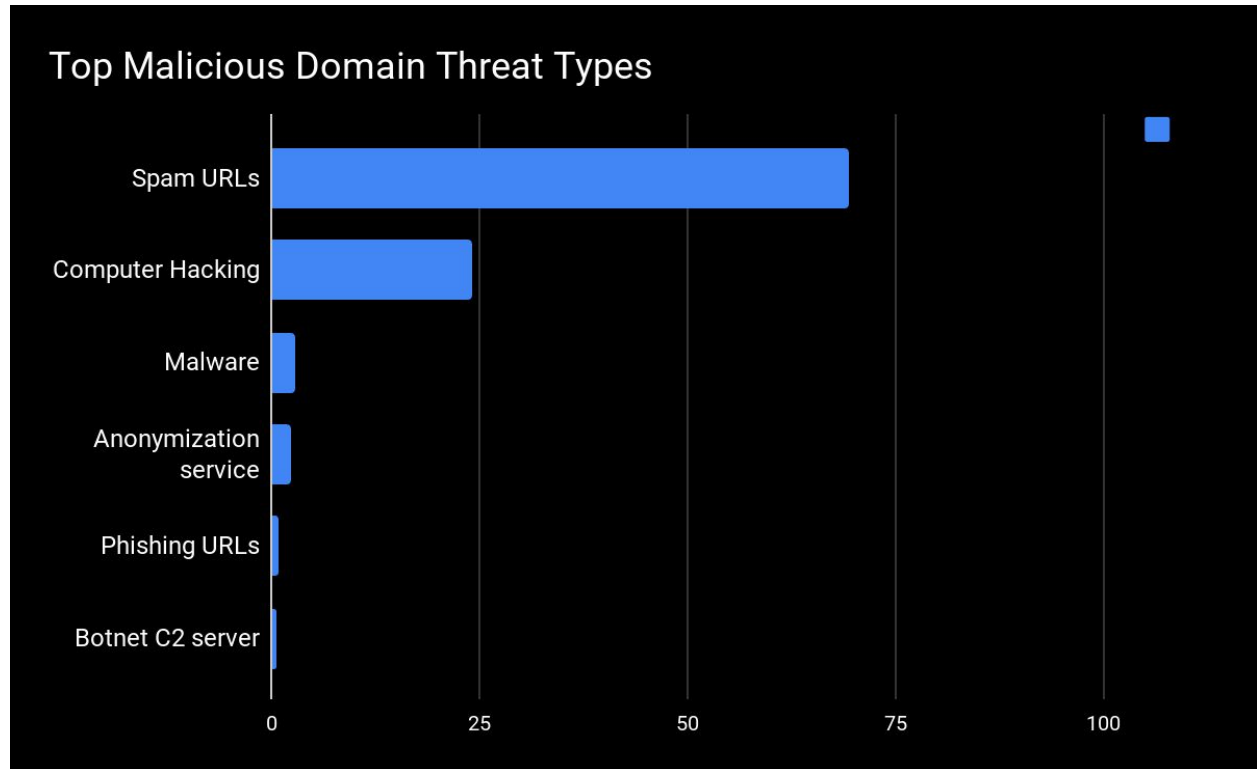
so how it can also perform better in machine learning and has given the algorithm for the same.

Finally, this paper[16] has been a great help as it is a very detailed paper discussing from the history of phishing attacks to the current challenges and how countermeasures are being formed and how the attackers are trying to circumvent them.

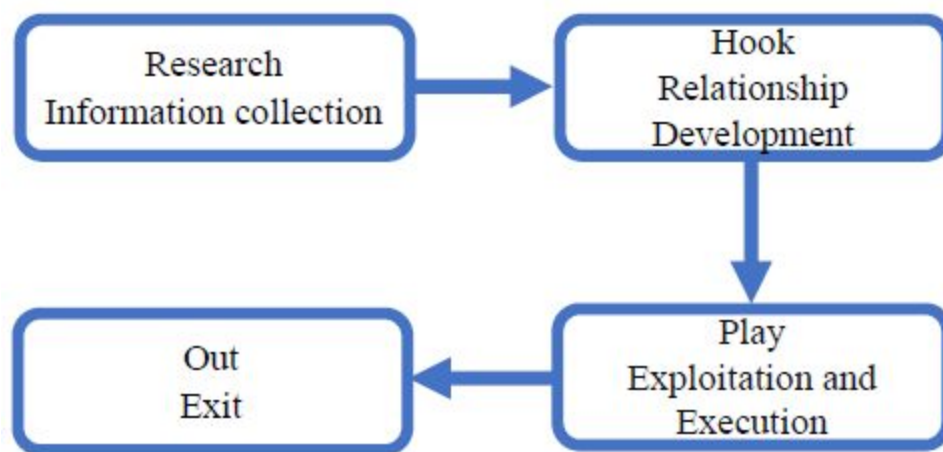
SOCIAL ENGINEERING FRAMEWORK

As mentioned before the advancements in digital communication technology have made communication between humans more accessible and instant. Nonetheless, individual and delicate data is additionally available online through social networks and online services that come up short on the protective measures to shield this information. Communication arrays are powerless and may basically be infiltrated by malignant clients through social engineering attacks. Social engineering attacks are rapidly expanding in the present organizations and are debilitating the cybersecurity chain. They target innocent individuals and organizations to extract essential and delicate information in the interest of cybercriminals. Social engineering is troubling even the biggest of all organizations regardless of the strength of their firewalls, cryptographic methods, intrusion detection frameworks, and antivirus software. People believe people are more contrasted with PCs or any other technology. Consequently, they're the most fragile connection inside the security chain. Malicious activities achieved through human associations impact an individual mentally to give away sensitive information or to interfere with the security protocol. Because of these human associations, social engineering attacks are the most ground-breaking assaults because of how they compromise all the frameworks and organizations. They can't be prevented using software or hardware solutions as long as people don't appear to be prepared to stop these assaults. Cybercriminals select these attacks once there's no passage to hack into a framework with any technical weaknesses.

To prove how deadly these attacks are, I have done some research and have taken data from IBM X-Force Threat Intelligence Report and PurpleSec consulting service. The top three initial infection vectors seen in X-Force IRIS engagements in 2019 were a very close first, second, and third: Phishing (31 percent), Scan and Exploit (30 percent), and Stolen Credentials (29 percent). The thing is 98% of attacks rely on social engineering. According to recent data breach statistics researched by Purplesec, 63% of successful attacks come from internal sources, either control, errors, or fraud.



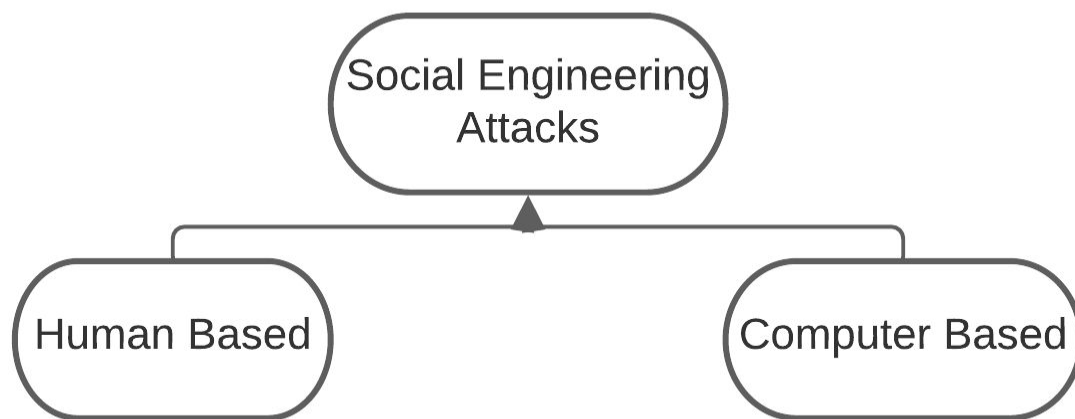
Although social engineering attacks differ from people to people, they have a common pattern with similar phases. The common pattern involves four phases: (1) collect information about the target; (2) develop a relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces. Figure 1 illustrates the different stages of a social engineering attack.



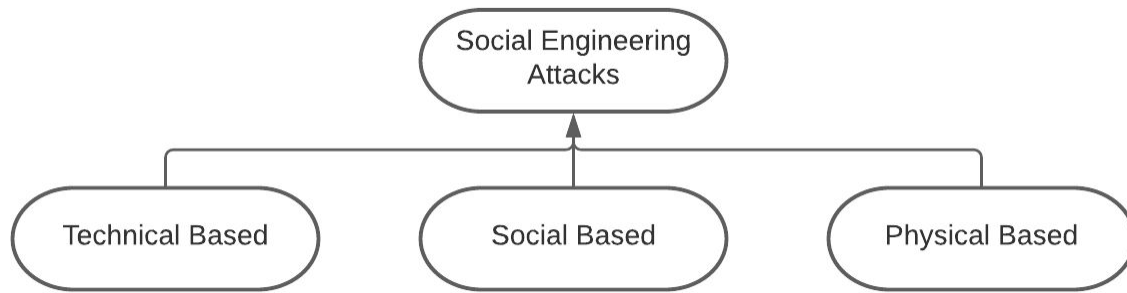
In the research stage, additionally called information gathering, the assailant chooses a

target on the basis of certain prerequisites. In the hook stage, the assailant begins to pick up the trust of the target through direct contact or email correspondence. In the play stage, the aggressor impacts the target emotionally to give sensitive data or perform security botches. In the out stage, the assailant just vanishes without leaving any evidence.

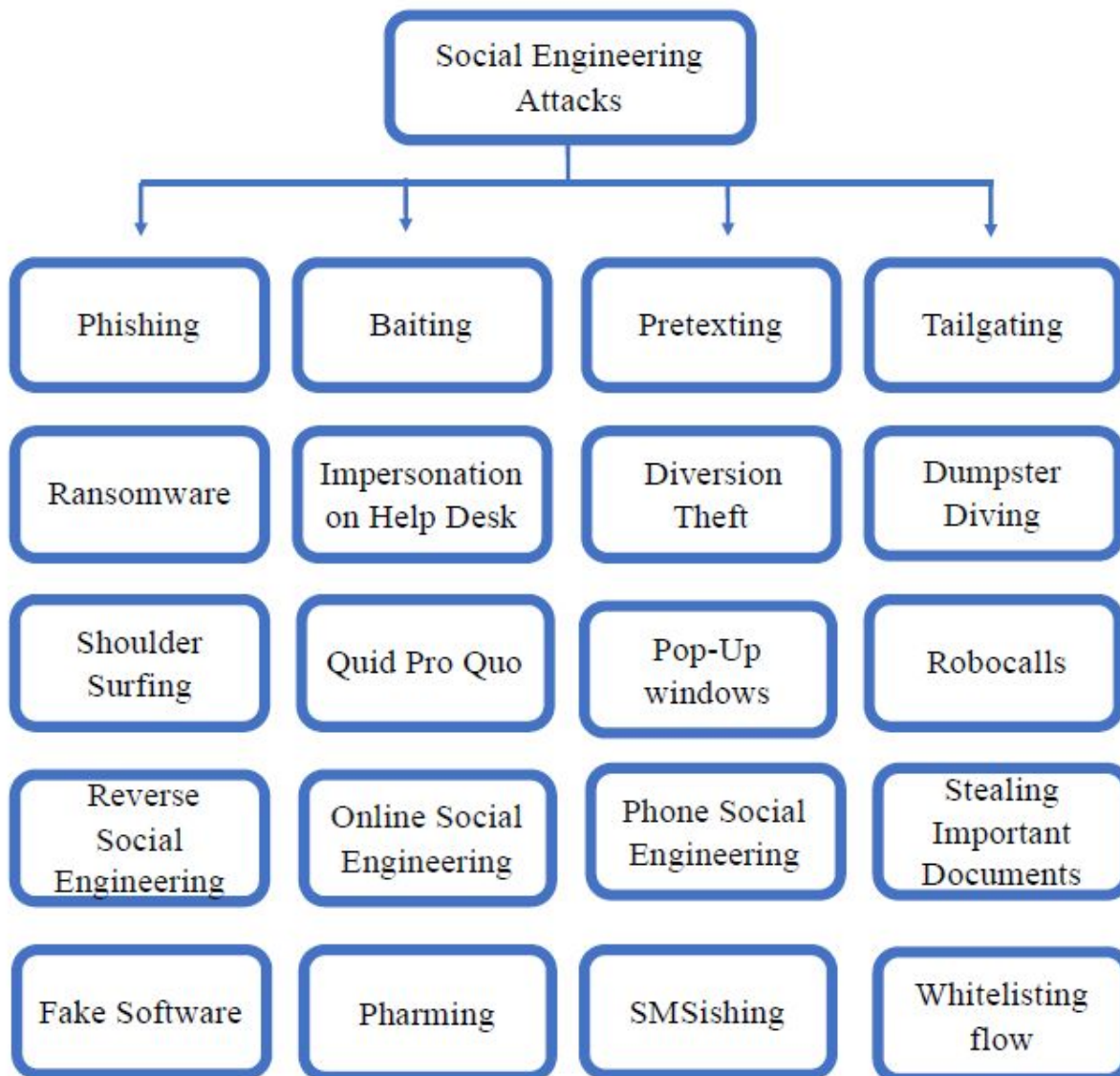
Social designing can be characterized into two classes: human-based and computer-based.



In human-based attacks, the assailant executes the attack face to face by communicating with the victim to assemble the required data. In this manner, they can affect a set number of victims only. Social engineering toolkit(SET) is one of the computer-based attacks used for spear-phishing messages. Social engineering attacks can likewise be characterized into three classes, as per how the attack is carried out: social, technical, and physical-based attacks.



Social-based attacks are performed through associations with the target to play on their psychology and feeling. These attacks are the most hazardous and fruitful attacks as they include human involvement. Instances of these attacks are baiting and spear phishing. Technical-based attacks are led through the web by means of social networks and online services sites and they collect the required data, for example, passwords, credit card data, and security questions. Physical-based attacks allude to actual activities performed by the attacker to gather data about the target. An illustration of such attacks is looking in dumpsters for any kind of relevant documents.



TYPES OF PHISHING ATTACKS

Phishing attacks generally target secret data, for example, client names, passwords, social security numbers(in the case of India, Aadhar Card numbers), passport details, credit card numbers, account numbers, PIN numbers, birthdates, mother's family names, and so forth. Phishers can without much of a stretch focus on technical expertise and sit in the solace of their homes or hack workplaces to get delicate data readily available. In this segment, I am going to show the various types of phishing attacks.

1. Attack by fraud

In a phishing attack by fraud, the hacker sends a deceptive email requesting the user to make some move, ordinarily referring to an issue with his financial balance, publicizing another service update, or offering a duplicate invoice, and so on. In all the above cases, the client is redirected to a website where one's personal and delicate data is being extracted. The attacker may utilize a connection with a domain name that looks fundamentally the same as the original domain name. If the user reacts positively and allows the link to open and gives other permissions, this can prompt malicious programs being installed on the user's PC which leaves an open backdoor for unstoppable access for future attacks.

Some specific types of such attacks include CEO fraud, smishing(SMS phishing), spear phishing, and whaling.

2. Attack by Infectious software

In a phishing attack by malicious software, the attacker exploits security weaknesses within the PC or the operating system. Frequently, it occurs by attracting the user to open an email attachment with the guarantee of obscene pictures or other fascinating baits. Some open-source or free downloadable programs also contain malicious programs that are installed alongside the normal one. Keyloggers are covert software or programs that can be installed into an internet browser and/or potentially work as a device driver that captures the information that is entered in by the client and uploaded to a remote server set up by the attacker. Session hijacking can likewise occur through a malignant browser component that was introduced by the attacker. As soon as the user successfully logs in and completes a transaction with the website, the malware hijacks the session and transfers the user credentials to the hacker. Web Trojans that pop up to gather client details and channel them back to the attacker are also predominant these days.

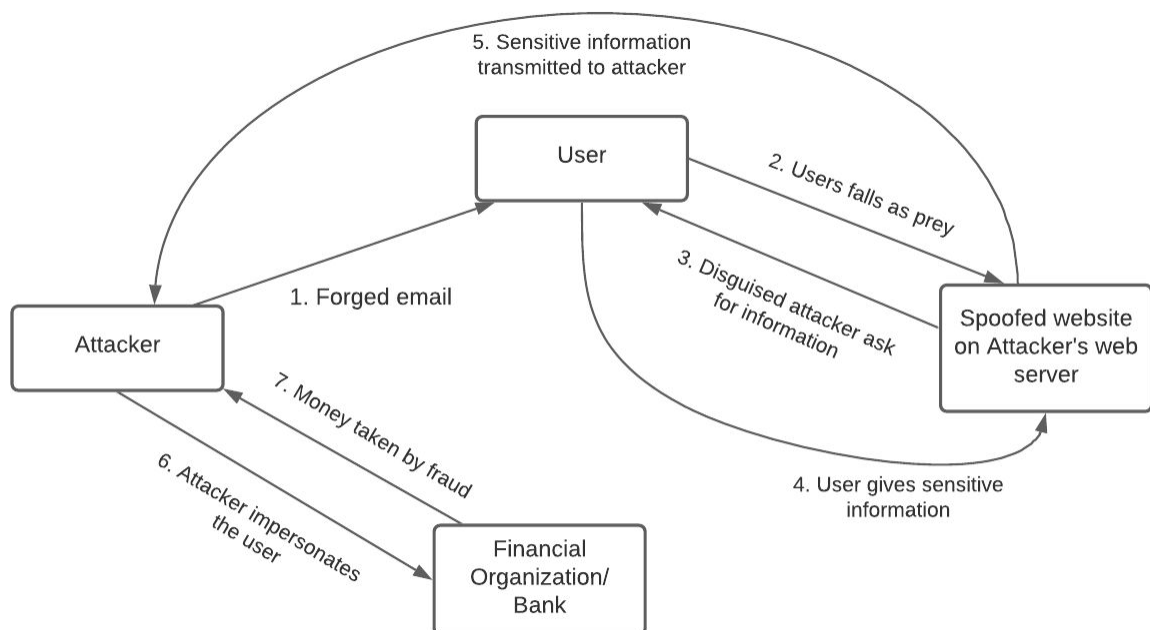
3. Attack by DNS Spoofing

In phishing attacks by DNS spoofing, the DNS lookup process is compromised either on the nearby PC or the DNS server. Host files in a nearby PC is looked into first prior to querying a DNS server to discover the IP address to domain mapping when a link is visited or when a domain address is entered in the web browser.

On the off chance that this file is compromised and false mapping is entered in the hosts' record through a malicious program, the client can go to the attacker's site and give individual data without knowing about it. A Crowt.D worm attack in the year 2005 was doing this. System configuration altering attacks can be done to compromise the DNS server so that the mapping is poisoned.

4. Attack by inserting harmful content

In phishing attacks by inserting harmful content, the attacker can affect a server's security weakness and put a malignant or unsafe content rather than a legitimate safe one, for example, the cross-site scripting (XSS) weakness. Here content coming from outside sources like a chat message, search, or web email would be provided to the guest's internet browser. SQL injection vulnerability can be utilized to perform such malignant activities.



5. Attack by Man-in-the-middle approach

In phishing attacks by man-in-the-middle approach, the attacker intercepts user traffic by coming in between him and the server of the web application. He uses a proper response forwarding mechanism as the user communicates with the intended site and helps communication back to the user from the website – all via his computer. The user thus would not have any suspicion of traffic tapping.

Attacks that come under this category are clone phishing and evil twin phishing.

6. Attack by Search Engine Indexing

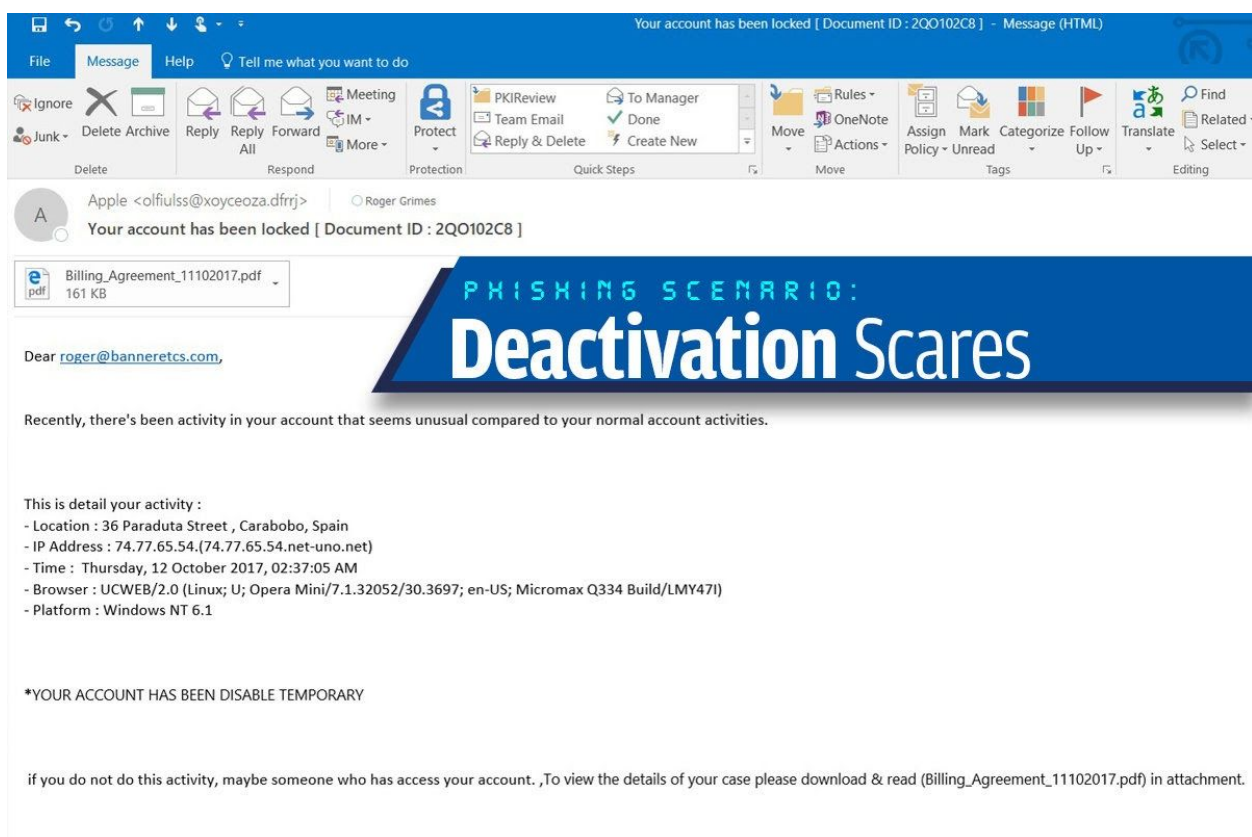
In phishing attacks by search engine indexing, the attacker creates a genuine-looking website for fake products where he can get users to perform financial transactions and attract users because of better offers than other websites like Amazon. This website would then be submitted for indexing by search engines so that any user can get a hit on the attacker's webpage.

Fraudulent banks with higher interest rates can attract customers in such a scenario and make the users perform some cash transfer to the newly created account in the attacker's web trap.

EXAMPLES OF PHISHING ATTACKS

In this section, we explore the technical aspects of typical phishing attacks. There are mainly 4 common techniques or classifications: (1) Email Field Manipulation Attack; (2) Email With Image-only Content Attack; (3) Misdirection and Redirection Attack; (4) Pop-up Window Attack. The several different attacks which fall under the first two types and I would explore each of them here.

1. DEACTIVATION SCARES



DEACTIVATION EXAMPLE[SOURCE: CSOONLINE]

This is a trap that works more often than others as nothing alarms individuals into responding as quickly as conceivable than a deactivation notice. Rarely a day passes by when an individual doesn't get an email pretending to come from an association they may – or might not – have a place with. It makes a claim and guarantees their account will be deactivated on the off chance that they don't follow a link, enter their login name, password, and secret phrase, and make a prompt move – most likely to update their credit card. These were once simple to spot. In any case, today the case is that they look extraordinarily authentic. They may incorporate genuine links to the organization they claim to be from. They presumably even incorporate "Be careful of scammers" warnings or consoling notices like "Examined and Cleaned by AV". It's entirely obvious if the phishes claim to be from an organization that an individual doesn't have a record with only. However, on the off chance that they do have a record, and they have as of late have moved or canceled any type of card, the users may expect the company to put everything in order by managing this rapidly.

2. LOOK-ALIKE WEBSITES



Online Banking Verification

Enter your User ID and Password to Sign on to Online Banking.

To sign on to a different account,

User ID:

Password:

Email Address:

Email Password:

[Forgot your User ID or Password?](#)

Continue ►

PHISHING SCENARIO:

Look-Alike Websites

[suntrust.com](#) | [Online Service Agreement](#) | [Bill Pay Guarantee](#) | [Privacy, Security & Fraud](#)

©2013 SunTrust Banks, Inc. SunTrust is federally registered service marks of SunTrust Banks, Inc. SunTrust Bank, Member FDIC. SunTrust Bank, Member FDIC. Equal Housing Lender

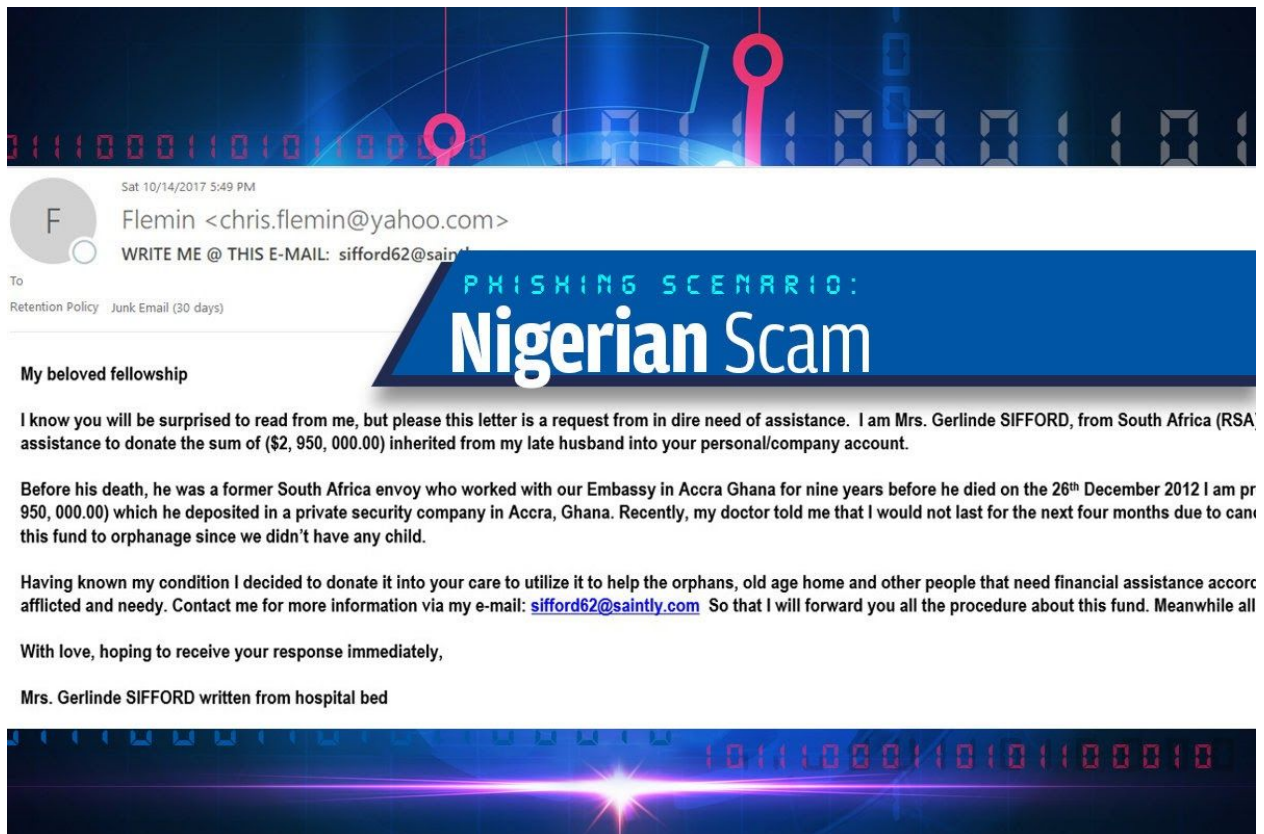
Securities and Insurance Products and Services:

• Are Not Bank Guaranteed • Are not FDIC or any other Government Agency Insured • May Lose Value

LOOKALIKE EXAMPLE[SOURCE:CSOONLINE]

It has gotten hard to differentiate between a phishing site and a genuine site. The fakes are exact duplicates and they contain the genuine site's URL as a component of the URL. On the off chance that you take a gander at it cautiously, you will see that the phishing site redirects to an alternate domain. Yet, this is barely noticeable when the site looks simply like the genuine thing. The screen capture above shows an illustration of a phishing email dishonestly professing to be from a genuine bank. Clients of Sun Trust may well succumb to this phish on the grounds that the site looks comfortably familiar, despite the fact that the URL is fake.

3. NIGERIAN SCAMS



NIGERIAN SCAM EXAMPLE[SOURCE: CSOONLINE]

Officially known as “advance fee frauds”, this phishing lure became known as Nigerian scams decades ago because Nigeria’s fraudsters seem to attempt them far more often than any other country – at least per capita.

You may chuckle at the terrible language structure and preposterous situations proposed and wonder, "What rational individual would fall for such a trickery?" But those elements are an international filter. The normal Nigerian scammer sends out a huge number of deceitful messages per day. Furthermore, the greater part of them is obstructed and dumped by email users or their antimalware program. Be that as it may, the normal email user isn't the fish this scam is attempting to get. This bait is intended to target the more susceptible targets. For certain individuals, the senselessness and slip-ups are essentially not a hindrance. And that is the prize this phisherman exactly is looking out for.

4. GO DIRECTLY TO JAIL



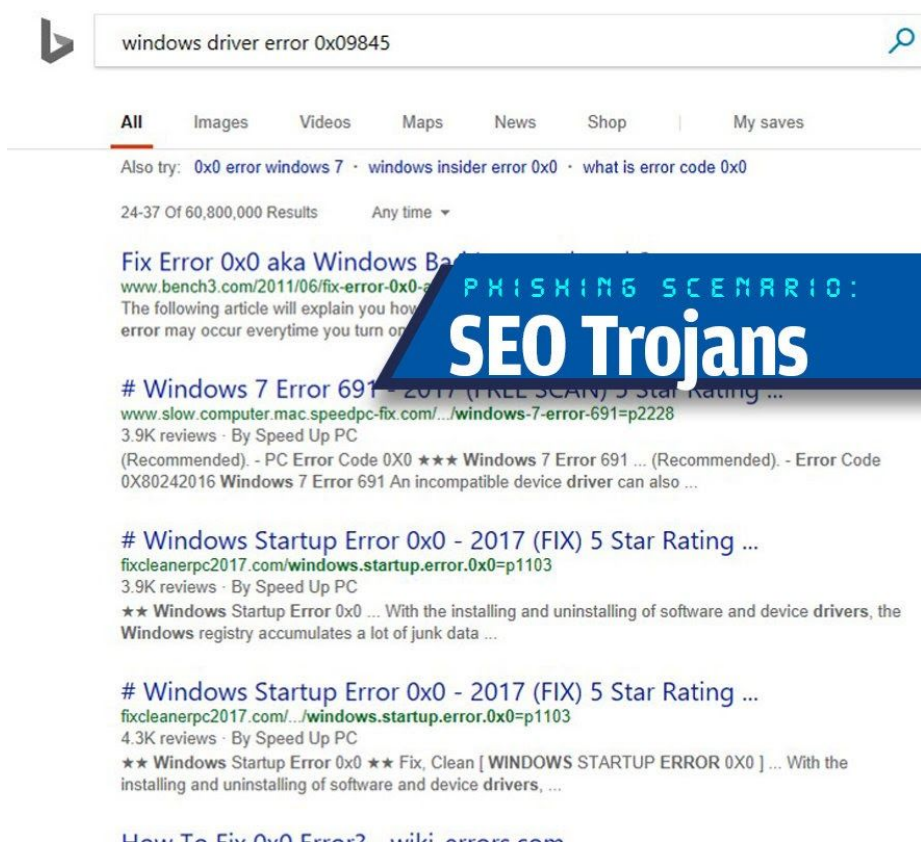
GO TO JAIL EXAMPLE[SOURCE:CSOONLINE]

This falls under the popup phishing attack category. Phishers realize that everyone has a feeling of guilt inside and use it to catch us off-guard. Regardless of whether the thing you feel regretful about isn't illegal, you can easily be fooled into stressing that you have been caught. Furthermore, nothing spurs somebody to react promptly and with absolute absurdity than the danger of being put in prison. Therefore, in the United States, phishing scams that utilize counterfeit FBI warnings for illegal music downloading or watching pornography lead the way. Counterfeit threats from the IRS for tax return issues are also exceptionally successful. These baits frequently come via telephone — may be to create and heighten the sense of urgency.

Many people pay even when they knew that they did not cheat their taxes, watch pornography, or download music. They simply need the warning to disappear – it won't! – or expect another person in the family is the guilty party. Unfortunately, the phony punishment warnings that come in by means of email frequently carry

ransomware too, which will totally lock up your PC until you pay.

5. SEO TROJANS



SEO TROJAN EXAMPLE[SOURCE:CSOONLINE]

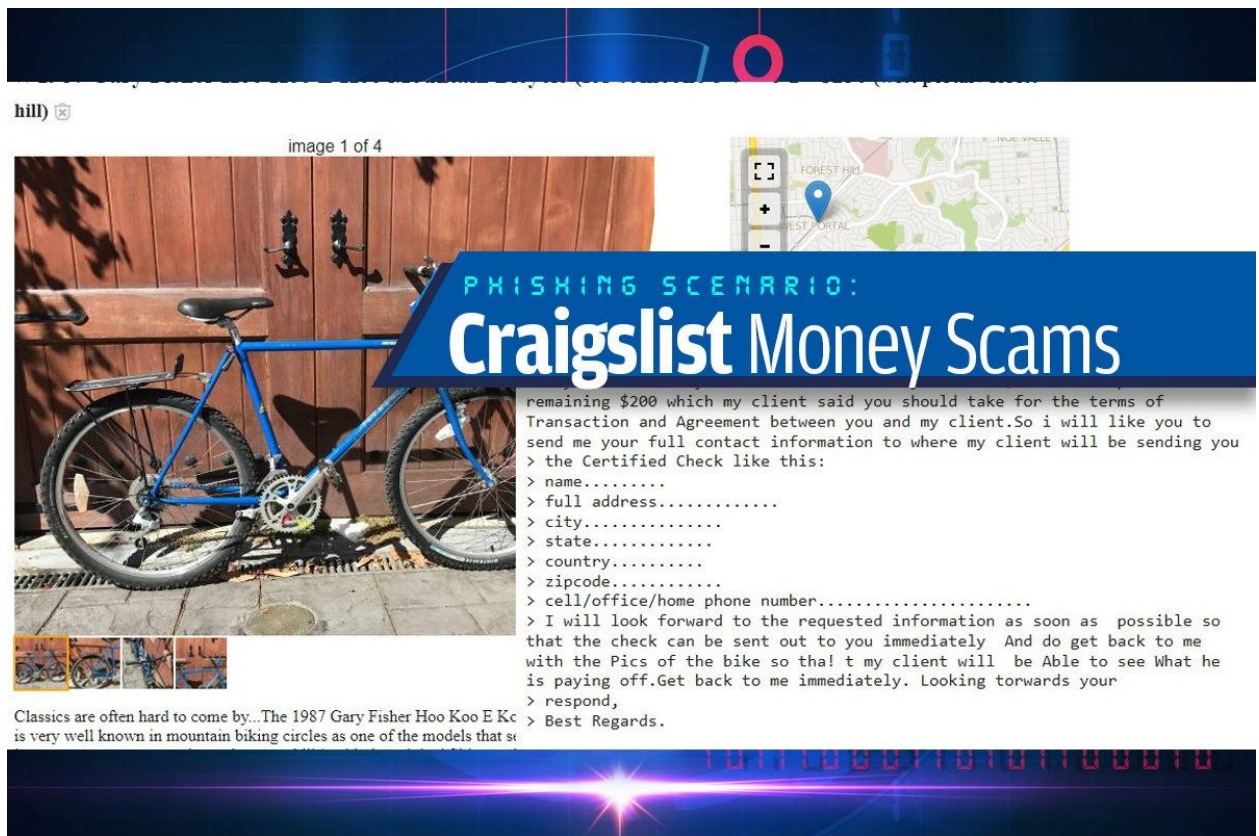
One very common phishing scam tricks you into installing malicious software directly from the web by showing up at the top of your search results. This lure is called Search Engine Optimization (SEO) poisoning.

It works in the following manner: You are having a technical issue and assume, just like that, that the problem is a bug in a device driver. Or maybe you got an error message and searched Google with its wording to decipher what's wrong. These are good approaches to a solution. But once in a while, you wound up at a site that looks authentic and promises a quick solution. All you have to do is install the software it offers. The problem is that, this time, the code is malicious.

In this screenshot, I searched for a non-existent error code. The search engine returned its best match, which includes sites that will gladly sell me "fix-it" software. In this case, I know I have nothing to fix. Some of the links in this example might not be – in the strictest sense – malicious. Some are merely what

people who fix computers for a living call “pest” software.

6. CRAIGSLIST/EBAY/OLX/GOOGLE PAY/PHONEPE MONEY SCAMS



hill) image 1 of 4

PHISHING SCENARIO:
Craigslist Money Scams

remaining \$200 which my client said you should take for the terms of Transaction and Agreement between you and my client. So I will like you to send me your full contact information to where my client will be sending you the Certified Check like this:

- > name.....
- > full address.....
- > city.....
- > state.....
- > country.....
- > zipcode.....
- > cell/office/home phone number.....

> I will look forward to the requested information as soon as possible so that the check can be sent out to you immediately. And do get back to me with the Pics of the bike so that my client will be able to see what he is paying off. Get back to me immediately. Looking forwards your

> respond,
> Best Regards.

Classics are often hard to come by...The 1987 Gary Fisher Hoo Koo E Kc is very well known in mountain biking circles as one of the models that s

CRAIGSLIST FRAUD EXAMPLE[SOURCE:CSOONLINE]

Fraudsters just love scouting for victims in personal advertisements and auction websites. Now by a wide margin, their number one fishing hole is Craigslist all around the world and OLX in India. This isn't on the grounds that these websites are evil or something. This is on the grounds that individuals appear at them, ready to click and visit links and trade personal information and money.

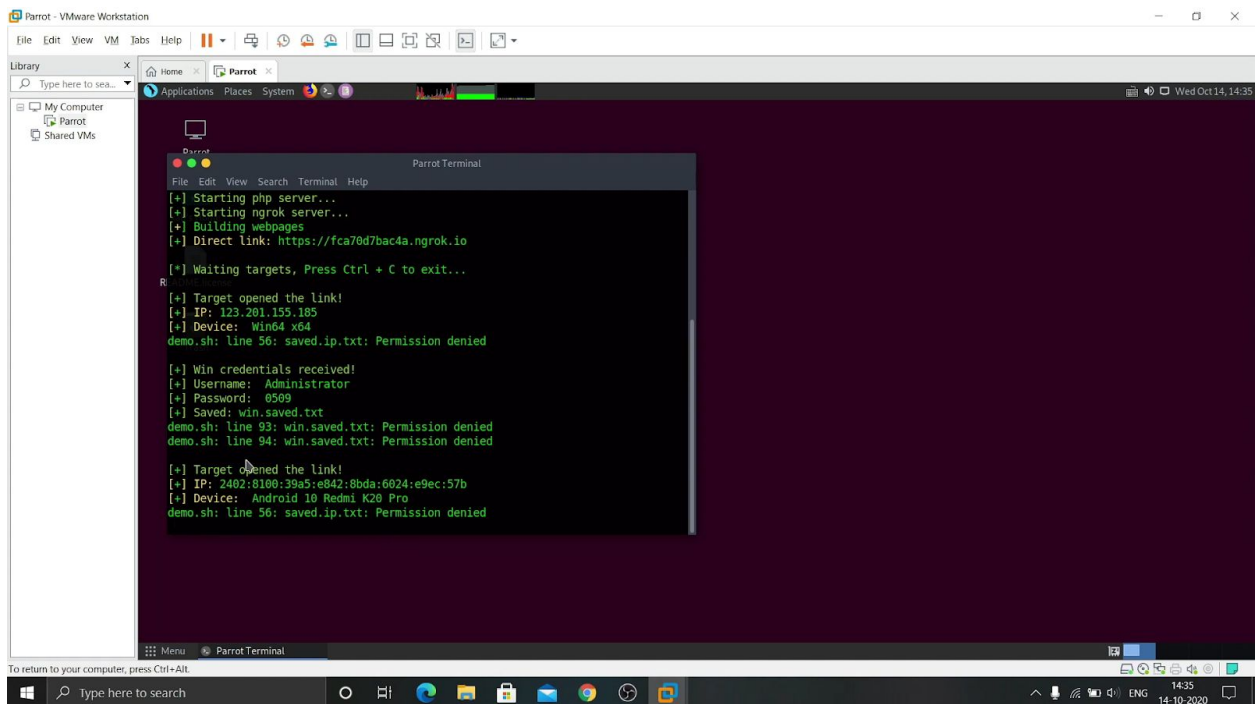
On Craigslist, money scams occur in a variety of ways. However, the most common one happens when you go there to sell. To your delight, a purchaser shows up quickly, offers to pay your full-cost – and the delivery price too! That was easy. But wait, it gets better. They trustingly offer to overpay in the event that you will utilize their independent, trusted intermediary to handle the payment and delivery costs. For this, they offer a mammoth check. They request that you eliminate your portion and forward the rest to their intermediary.

After two days, your bank returns the check your purchaser sent since it's fake.

Presently you are on the hook for the fraudulent funds you shipped off to the intermediary. Do not make the mistake to assume that your bank would verify the check when you deposited it. It doesn't.

SMALL-SCALE PHISHING DEMONSTRATION

To demonstrate how phishing works on a small scale, I have developed a shell script that works with ngrok and straightforward redirection to a webpage. Basically, the shell script generates an URL that can be shortened using an URL shortener service. That can be sent to anyone we want and once the target decides to open the URL, it redirects the target to their devices' lookalike lock screen and forces them to enter the password which is captured on our screen. The demonstration of the entire mini-project can be seen using the given link: <https://youtu.be/07aq26vsokc>



The screenshot shows a Parrot VM terminal window with a dark purple background. The terminal output displays the following sequence of events:

```
Parrot - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Parrot
Shared VMs
Applications Places System
Wed Oct 14, 14:35

Parrot Terminal
File Edit View Search Terminal Help
[+] Starting php server...
[+] Starting ngrok server...
[+] Building webpages
[+] Direct link: https://fca70d7bac4a.ngrok.io
[+] Waiting targets, Press Ctrl + C to exit...
R
[+] Target opened the link!
[+] IP: 123.201.155.105
[+] Device: Win64 x64
demo.sh: line 56: saved.ip.txt: Permission denied

[+] Win credentials received!
[+] Username: Administrator
[+] Password: 0509
[+] Saved: win.saved.txt
demo.sh: line 93: win.saved.txt: Permission denied
demo.sh: line 94: win.saved.txt: Permission denied

[+] Target opened the link!
[+] IP: 2402:8100:39a5:e842:8bda:6024:e9ec:57b
[+] Device: Android 10 Redmi K20 Pro
demo.sh: line 56: saved.ip.txt: Permission denied
```

DETECTING PHISHING URLs FEATURES

One of the biggest difficulties that come into defending against phishing attacks is that people are not even aware that they are being phished. Thus I aim to shed some light on the important features that have proved to be sound and effective in predicting phishing websites manually. In addition, I propose some other features too that I believe are

signatures to phishing URLs.

1.1 ADDRESS BAR BASED FEATURES

1.1.1 Using the IP address

If an IP address is used in place of the domain name in the URL, such as “<http://129.91.9.193/fake.html>”, users can be sure that someone is trying to steal their personal data. Sometimes, the IP address is even transformed into hexadecimal code as shown in the following link <http://0x5E.0xAA.0xCA.0x69/2/paypal.ca/index.html>”.

1.1.2 Long URL to Hide the Suspicious Part

Phishers can use a long URL to concede the suspicious part in the address bar. For example:

http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=_home&dispatch=11004d58f5b74f8dc1e7c2e8dh4105e811004d58f5b74f8dc1e7c2e8dd4105e8@phishing.website.html

To ensure the accuracy of our study, we calculated the length of URLs in the dataset and produced an average URL length. The results showed that if the length of the URL is greater than or equal to 54 characters then the URL is classified as phishing. By reviewing our dataset we were able to find 1220 URLs lengths equals 54 or more which constitute 48.8% of the total dataset size.

I propose that if we use a method based on frequency then we can improve the accuracy of the algorithm.

1.1.3 Using URL shortening services “Tiny URL/Bitly”

URL shortening is a method on the “World Wide Web” in which a URL can be converted to a shorter length and yet, redirect to the required web page. This is accomplished by means of an “HTTP Redirect” on a domain name that is short, which links to the webpage that has a long URL. For example, the URL “<http://www.vitap.ac.in/>” can be shortened to “bit.ly/19DXSk4”.

1.1.4 URLs having “@” symbol

Using the “@” symbol in the URL leads the browser to ignore everything preceding the “@” symbol and the real address often follows the “@” symbol.

1.1.5 Redirecting using “//”

The existence of “//” within the URL path means that the user will be redirected to another website. An example of such URL’s is:

“<http://www.legitimate.com//http://www.phishing.com>”. We examine the location where the “//” appears. We find that if the URL starts with “HTTP”, that means the “//” should appear in the sixth position. However, if the URL employs “HTTPS” then the “//” should appear in the seventh position.

1.1.6 Adding Prefix or Suffix Separated by (-) to the Domain

The dash symbol is almost never used in legitimate URLs. Phishers tend to add prefixes or suffixes separated by (-) to the domain name so that users feel that they are dealing with a legitimate website. For example

<http://www.Confirme-paypal.com/>.

1.1.7 Sub Domain and Multi Sub Domain

Let us assume we have the following link: <http://www.vitap.ac.in/students/>. A domain name might include the country-code top-level domains (ccTLD), which in our example is “in”. The “ac” part is shorthand for “academic”, the combined “ac.in” is called a second-level domain (SLD) and “vitap” is the actual name of the domain. To produce a rule for extracting this feature, we first have to omit the (www.) from the URL which is in fact a subdomain in itself. Then, we have to remove the (ccTLD) if it exists. Finally, we count the remaining dots. If the number of dots is greater than one, then the URL is classified as “Suspicious” since it has one subdomain. However, if the dots are greater than two, it is classified as “Phishing” since it will have multiple subdomains. Otherwise, if the URL has no subdomains, we will assign “Legitimate” to the feature.

1.1.8 HTTPS and Certificate

The existence of HTTPS is very important in giving the impression of website legitimacy, but this is clearly not enough. I suggest checking the certificate assigned with HTTPS including the extent of the trust certificate issuer, and the certificate age. Certificate Authorities that are consistently listed among the top trustworthy names include: “GeoTrust, GoDaddy, Network Solutions, Thawte, Comodo, Doster, and VeriSign”. Furthermore, from a literary review of other research papers, I found that the minimum age of a reputable certificate is two years.

1.1.9 Domain Registration Length

Based on the fact that a phishing website lives quite briefly, we believe that trustworthy domains are regularly paid for several years in advance. From research, ***I observed that the longest fraudulent domains have been used usually for a maximum period of one year or so.***

1.1.10 Favicon

A favicon is a graphic image (icon) associated with a specific webpage. Many existing user agents such as graphical browsers and newsreaders show favicon as a visual reminder of the website identity in the address bar. If the favicon is loaded from a domain other than that shown in the address bar, then the webpage is likely to be considered a phishing attempt.

1.1.11 Using a non-standard port

This feature is useful in validating if a particular service (e.g. HTTP) is up or down on a specific server. With the aim of controlling intrusions, it is much better to merely open ports that you need. Several firewalls, Proxy and Network Address Translation (NAT) servers will, by default, block all or most of the ports and only open the ones selected. If all ports are open, phishers can run almost any service they want and as a result, user information is threatened.

1.1.12 Existence of “HTTPS” token in the Domain part of URL

The phishers may add the “HTTPS” token to the domain part of a URL in order to trick users. For example,

<http://https-www-paypal-it-webapps-mpp-home.soft-hair.com/>

1.2 ABNORMAL BASED FEATURES

1.2.1 Request URL

Request URL examines whether the external objects contained within a webpage such as images, videos, and sounds are loaded from another domain. In legitimate webpages, the webpage address and most of the objects embedded within the webpage are sharing the same domain.

1.2.2 URL of Anchor

An anchor is an element defined by the <a> tag. This feature is treated exactly as “Request URL”. However, for this feature we examine:

1. If the <a> tags and the website have different domain names. This is similar to the request URL feature.
2. If the anchor does not link to any webpage, e.g.:
 - A.
 - B.
 - C.
 - D.

1.2.3 Server Form Handler(SFH)

SFHs that contain an empty string or “about:blank” is considered doubtful because action should be taken upon the submitted information. In addition, if the domain name in SFHs is different from the domain name of the webpage, this reveals that the webpage is suspicious because the submitted information is rarely handled by external domains. So if SFH is empty then it is guaranteed a phishing site, and if it is redirecting to a different domain, it is still under suspicion.

1.2.4 Submitting Information as forms or via email

Web form allows a user to submit his personal information that is directed to a server for processing. A phisher might redirect the user’s information to his personal email. To that end, a server-side script language might be used such as “mail()” function in PHP. One more client-side function that might be used for this purpose is the “mailto:” function.

1.3 HTML AND JAVASCRIPT BASED FEATURES

1.3.1 Website Forwarding

The fine line that distinguishes phishing websites from legitimate ones is how many times a website has been redirected. ***Phishing websites have been observed to redirect more than 3 times at least.***

1.3.2 Status Bar Customization

Phishers may use JavaScript to show a fake URL in the status bar to users. To extract this feature, we must dig-out the webpage source code, particularly the “onMouseOver” event, and check if it makes any changes to the status bar.

1.3.3 Disabling Right Click

Generally, phishers use JavaScript to disable the right-click function so that users cannot view and save the webpage source code. This feature is treated exactly as “Using onMouseOver to hide the Link”. Nonetheless, for this feature, we will search for the event “event.button==2” in the webpage source code and check if the right-click is disabled.

1.3.4 Using Pop-Up Window

It is unusual to find a legitimate website asking users to submit their personal information through a pop-up window. On the other hand, this feature has been used in some legitimate websites and its main goal is to warn users about fraudulent activities or broadcast a welcome announcement, though no personal information was asked to be filled in through these pop-up windows.

1.3.5 IFrame Redirection

IFrame is an HTML tag used to display an additional webpage into one that is currently shown. Phishers can make use of the “iframe” tag and make it invisible i.e. without frame borders. In this regard, phishers make use of the “frameBorder” attribute which causes the browser to render a visual delineation.

1.4 DOMAIN BASED FEATURES

1.4.1 Age of Domain

This feature can be extracted from the WHOIS database. Most phishing websites live for a short period of time. ***The minimum age of a legitimate website is 6 months.***

1.4.2 DNS Record

For phishing websites, either the claimed identity is not recognized by the WHOIS database or no records found for the hostname. If the DNS record is empty or not found then the website is classified as “Phishing”, otherwise it is classified as

“Legitimate”.

1.4.3 Website Traffic

This feature measures the popularity of the website by determining the number of visitors and the number of pages they visit. However, since phishing websites live for a short period of time, they may not be recognized by the Alexa database. I observed that in the worst scenarios, legitimate websites ranked among the top 100,000. Furthermore, if the domain has no traffic or is not recognized by the Alexa database, it is classified as “Phishing”. Otherwise, it is classified as “Suspicious”.

1.4.4 Pagerank

PageRank is a value ranging from “0” to “1”. PageRank aims to measure how important a webpage is on the Internet. The greater the PageRank value the more important the webpage. ***Most of the phishing websites do not have any PageRank whatsoever.***

1.4.5 Number of Links Pointing to Page

The number of links pointing to the webpage indicates its legitimacy level, even if some links are of the same domain. ***Due to its short life span, we find that 98% of phishing dataset items have no links pointing to them.*** On the other hand, legitimate websites have at least 2 external links pointing to them

EXISTING PHISHING DETECTION TECHNIQUES

1. TRADITIONAL METHODS FOR PHISHING DETECTION

This method has further two categories, namely authentication protection and network security.

Network-level security contains two types of filters, white-list filter, and black-list filter which in turn works by blocking IP address and domain from the given network. Apart from this, there is also a rule-based filter and pattern-matching filter.

- Black-list Filter

This provides protection at the network layer of the OSI model by classifying email DNS address, IP address, and sender address from the email header and comparing them to the predefined list. If the data hits a match, then the email is rejected.

- White-list Filter

In this technique, the email data is compared with a predefined list containing IP addresses and static IP addresses of legitimate domain. Here only the emails which give a hit are allowed access.

- Pattern-matching Filter

This is used to decide whether the email is spam or not by searching the email in a pattern list and if the email has more than a certain amount of banned text, then the email is decided as spam.

- Email verification

Email confirmation is a client-level verification system. The system requires confirmation from the sender and receiver.

2. AUTOMATED METHODS

- Logistic Regression

This algorithm applies a linear model to predict binary data i.e. 0 or 1. It is easy to interpret and understand and gives quite good results over some data. But it is quite simple and thus, attackers have come up with several other ways to overcome the same.

- Decision Trees Filter(DT)

Decision tree algorithm is based on a node and arrow model and it initializes from the root node. If-then rules are applied to every node in the network to filter out the spam emails using every possible condition.

- Support Vector Machine(SVM)

SVM has been in use for quite a long time in different fields like healthcare for diagnosis of diseases, text recognition, classification of images, and

other purposes. Basically what SVM does is that it partitions the data into two categories using fixed rules, quadratic equation, and statistics. SVM used to give the best solution to the problem but the problem is that it fails to analyze big data.

PROPOSED APPROACH TO DETECT PHISHING USING NEURAL NETWORKS

As we can see machine learning techniques have already been used to detect phishing websites but they come with their own cons. The approach I propose is based on the research performed as shown till now:

1. Preprocess the information to evacuate any kind of unnecessary data like null values
2. Use the feature extraction based on the research on phishing URLs and convert English content to numerical data which is understandable by the computer
3. Find out the general information about the dataset such as the summary and the number of safe and unsafe rows
4. Partition the newly formed numerical dataset into two distinct sets into training and testing set
5. Define callback function to monitor loss and adjust learning rates accordingly and to stop the model once it reaches a certain average accuracy rate
6. Train and test numerous models for various optimizers namely, Adam, RMSProp, and SGD with 3 hidden layers, two with 512 nodes, and the last one with 256 nodes and Sigmoid activation function
7. Evaluate model to gauge loss and accuracy of the prepared model for all the optimizers and compare them
8. Train and test again with the same optimizers but now with the first two hidden layers with 512 nodes only but the last hidden node having 1024 nodes, and Sigmoid activation function. Loss function in both the cases is “binary cross-entropy” as it is perfect for binary classification
9. Evaluate and compare the result generated from both the models for the specific optimizers
10. Finally, enhance the result using Swarm Intelligence/TDLHBA technique

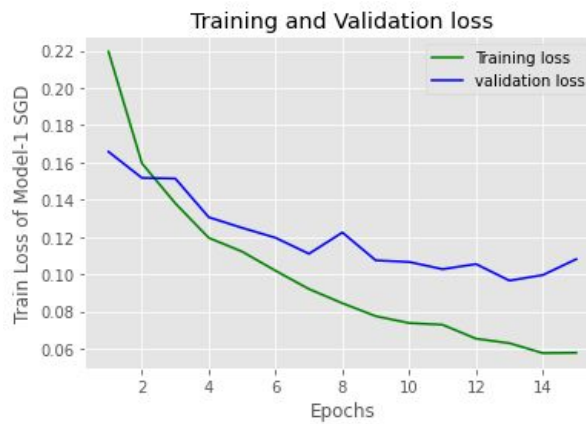
EXPERIMENTAL RESULTS

This section demonstrates the comparison of experimental results between the models,

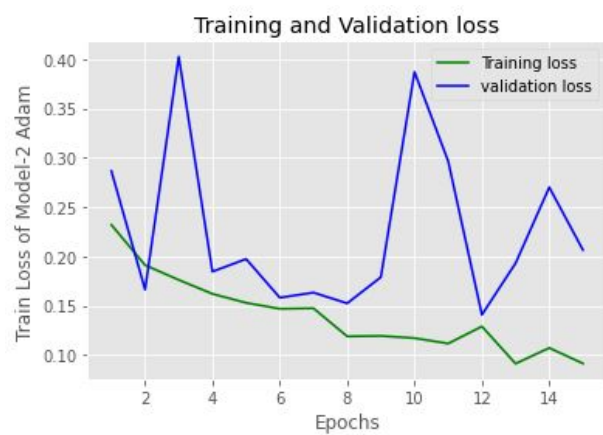
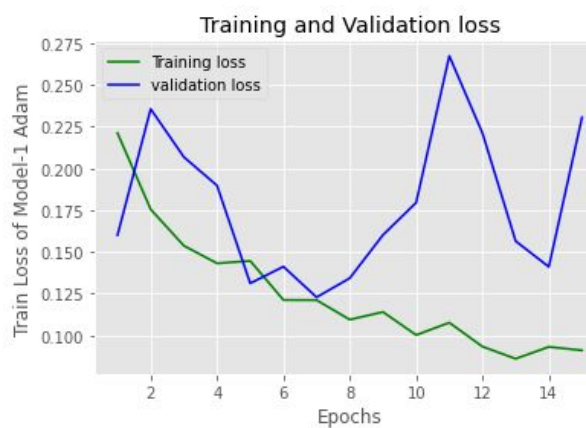
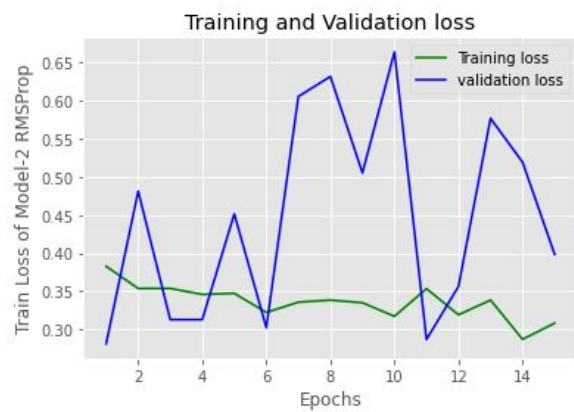
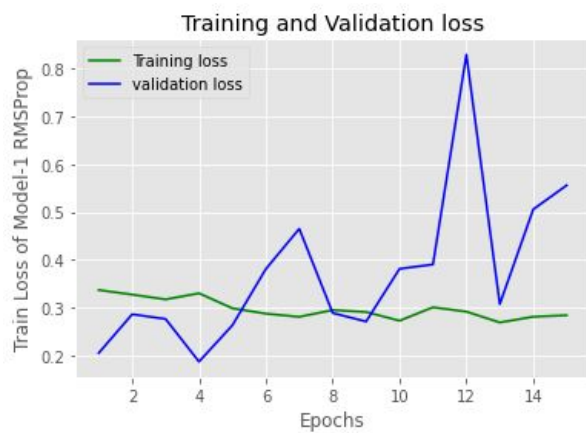
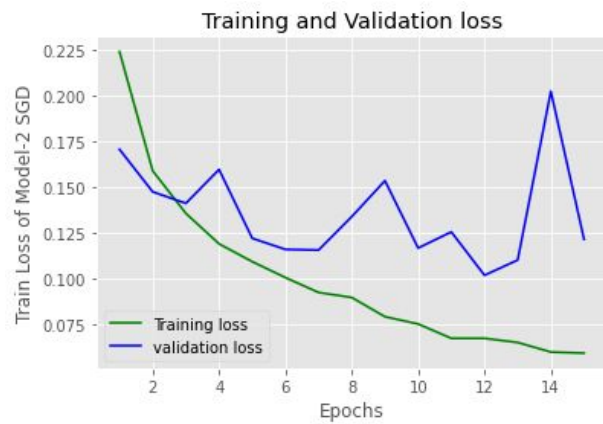
comparison between the loss and accuracy of the same.

LOSS COMPARISON

MODEL-1



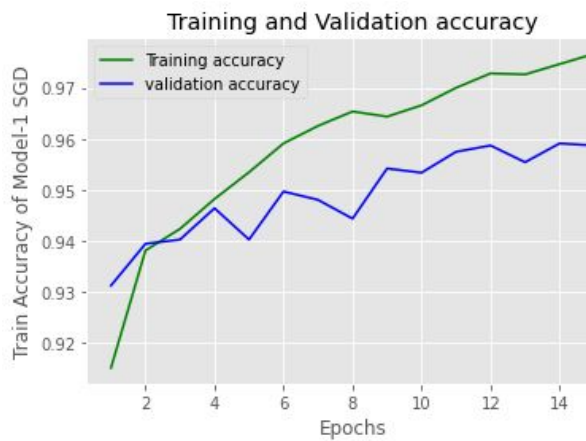
MODEL-2



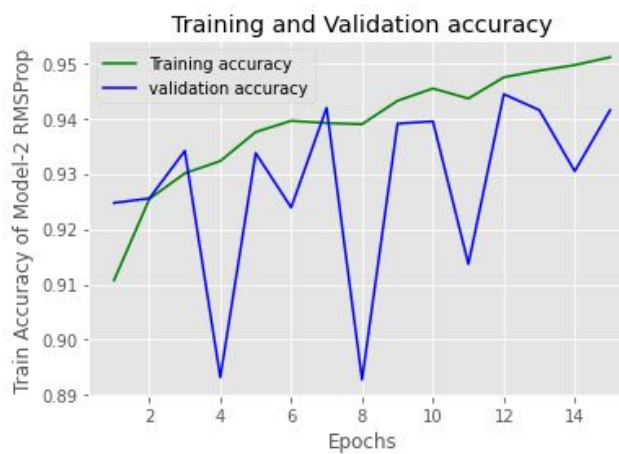
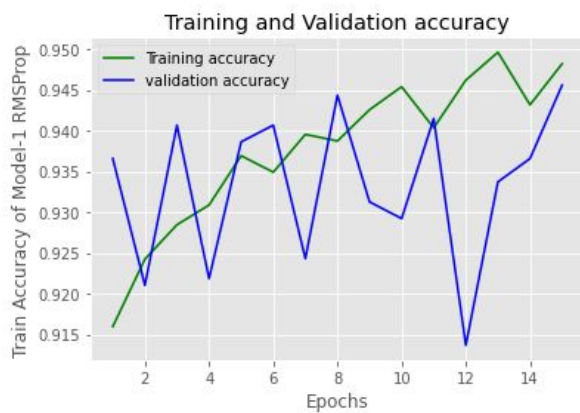
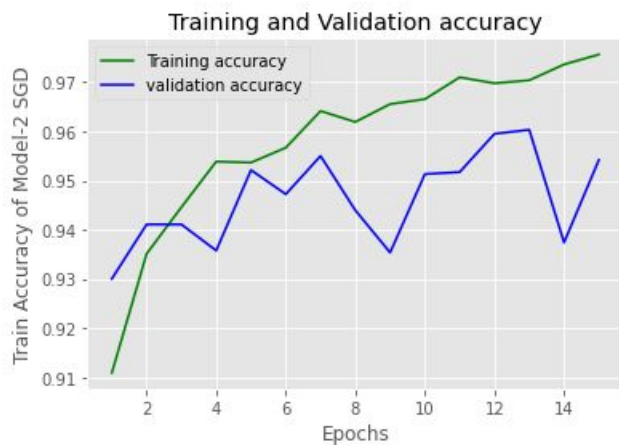
From the above graphs where the loss occurred during the training and validation of models, we can observe that the second model is performing better than the first by a minuscule mark. The reason behind this is that the number of nodes in the hidden layers has increased which means that the algorithm learns better and fits more properly. And of the three optimizers, on average Stochastic Gradient Descent(SGD) outperforms the other two.

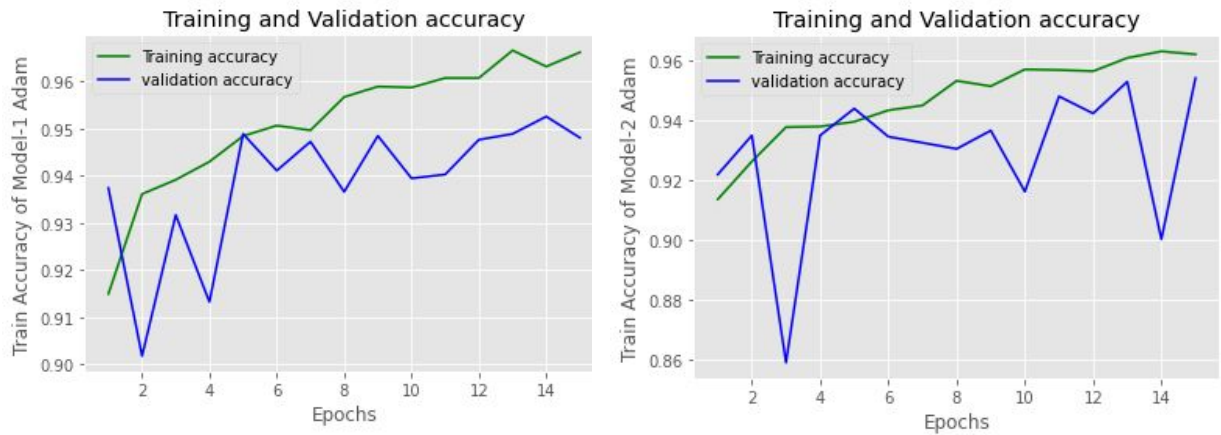
ACCURACY COMPARISON

MODEL-1

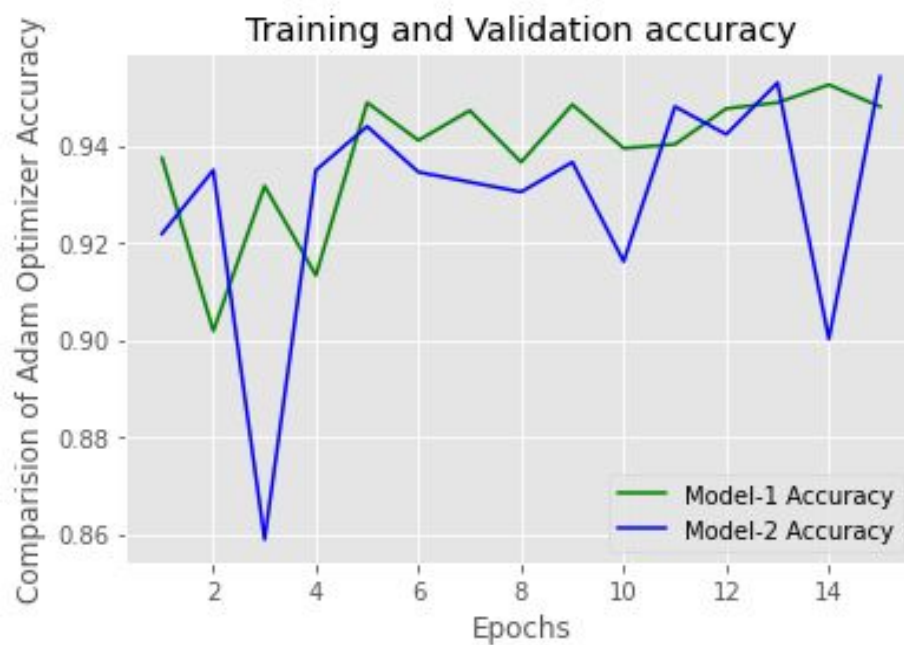


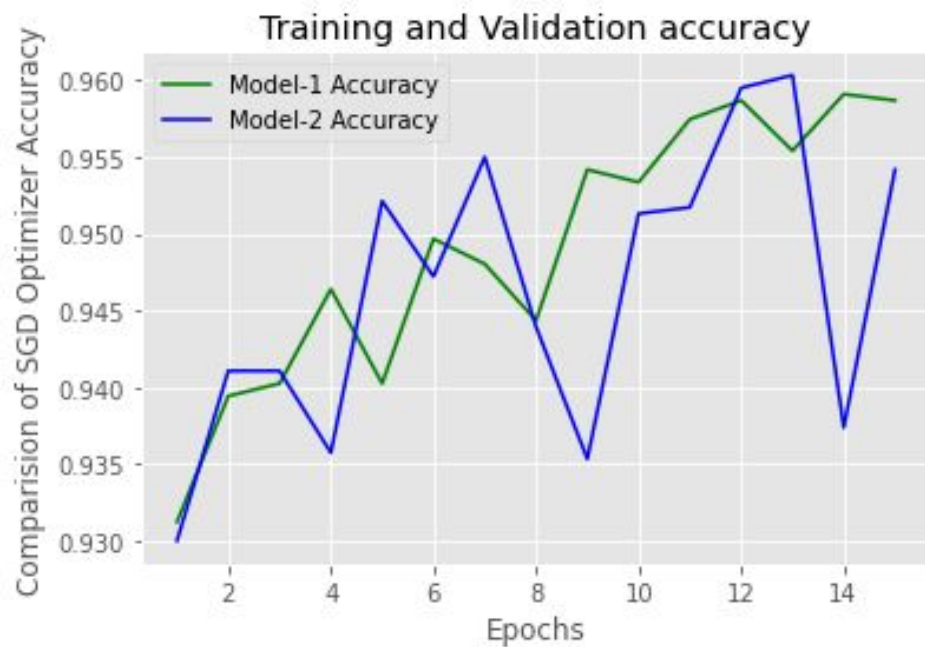
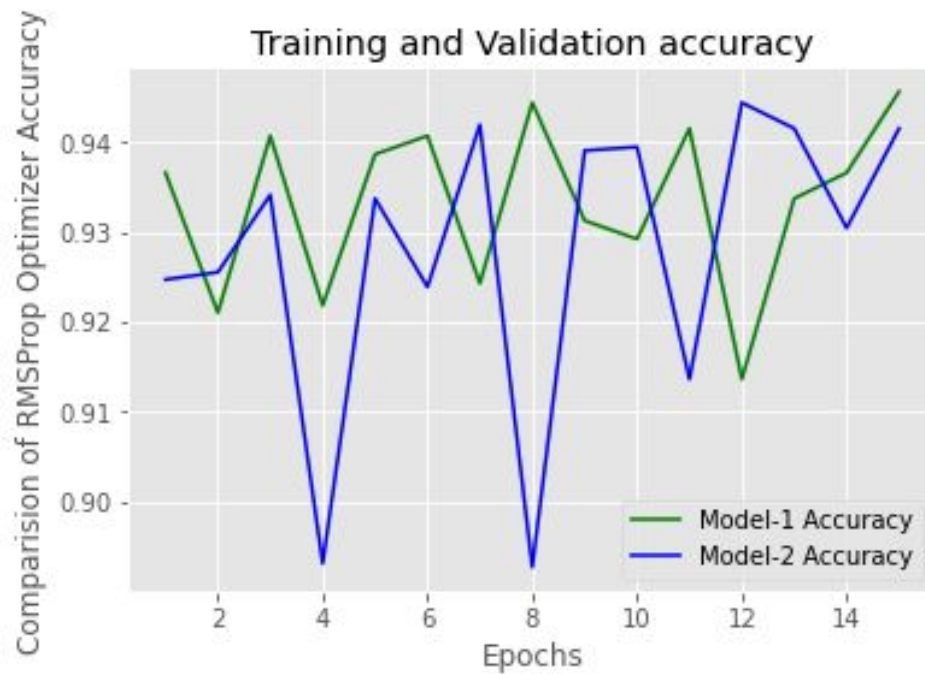
MODEL-2





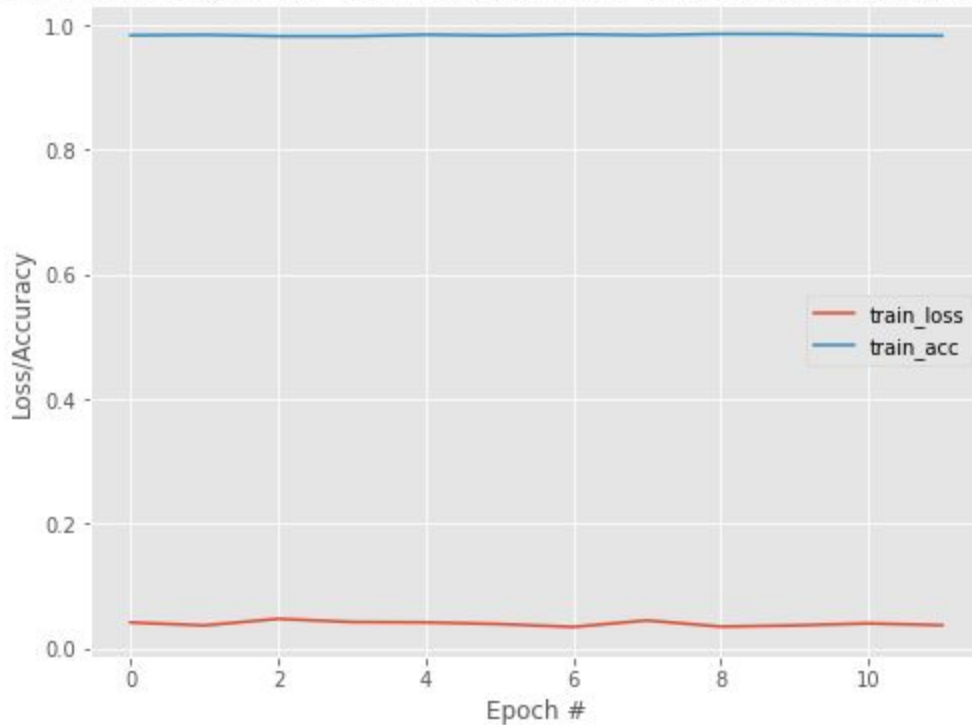
Now when we compare the accuracy in the above graphs, there is not much difference between both the models. But we can see Stochastic Gradient Descent(SGD) again outperforming the other two in determining the accuracy by a minuscule level.





Comparing the accuracy of each optimizer in both the models, we can see that other than the Adam optimizer, model-1 performed in a better way even though the second model had more number of nodes in it. The reason behind this is overfitting. As the number of nodes increased, it took in the noise and the detail and the large size of the dataset.

Training Loss and Accuracy on the dataset (with TDLHBA hyperparameter settings)



Finally, the result we have to actually watch out for is the neural network with the TDLHBA technique. It has extremely high accuracy, an average of **94.93%**, and a very minimal loss, approximately below **0.1%**.

CONCLUSION AND FUTURE SCOPE

CONCLUSION

This research proposes a better framework for machine learning systems to address increasing phishing issues. A model was developed and tested on Google Colaboratory for a total of **4 times** to get conclusive and accurate average results. GPU in Google Colaboratory provided a huge upgrade to the model as compared to the Jupyter Notebook running on RAM, which took approximately **60 seconds** as compared to the GPU of Colab which took approximately **15 seconds**, suggesting a drastic improvement and indicating towards the complexity of the algorithm. From all the experimental results, we can conclusively determine that the “swarm intelligence approach” is more preferable in all ways than the orthodox neural network models.

FUTURE SCOPE

As I am preparing this report, attackers are finding new ways to con the people on the Internet and finding new holes in the system. Thus, feature selection will be needed to be continuously improved and updated as the attackers upgrade themselves. Another future scope is to create an endpoint API which can be used as a plugin or a web application for users to easily interact and make use of this phishing detection algorithm.

REFERENCES

1. A.P. Kumar, "Phishing - Challenges and Solutions", January 2018
2. Higbi, Bellani, Greaux, "Collaborative Phishing Attack Detection", Google Patents, February 2013
3. Kiruthiga, Akila, "Phishing Websites Detection using Machine Learning", IJRTE, Vol. 8 Iss. 2S11, September 2019
4. Akinyelu, Adewumi, "Classification of Phishing Email using Random Forest Machine Learning Technique", Hindawi, Vol. 2014, April 2014
5. Fister, Podgorelec, "Swarm Intelligence Approaches for Parameter Setting of Deep Learning Neural Network: Case Study on Phishing Websites Classification", WIMS 2018, June 2018
6. Wang, Zhang, Luo, "PDRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks", Hindawi, Vol. 2019, October 2019
7. Patil, Shetye, Shendage. "Detecting Phishing Websites Using Machine Learning", IRJET, Vol. 7 Iss. 2, February 2020
8. Ganesh, Arnket Solutions, "DeepAnti-PhishNet: Applying Deep Neural Networks for Phishing Email Detection", IWSPA-2018
9. Csirtg, "Phishing Predictions with Deep Learning and Tensorflow", 2018
10. Akamai, "A New Era in Phishing - Games, Social, and Prizes", May 2018
11. Salahdine, Kaabouch, "Social Engineering Attacks: A Survey", MDPI FutureInternet, April 2019
12. Schuetzler, "Trends in Phishing Attacks: Suggestion For Future Research", University of Nebraska, August 2011
13. Chauhan, Kumar, Jyot, Dr. Jain, "Phishing Attack", International Journal of Future Generation Communication and Networking Vol. 13, No. 4, August 2020
14. Das, Kim, Tingle, Nippert-Eng, "All About Phishing Exploring User Research

through a Systematic Literature Review”, Indiana University Bloomington

15. Dr. Damodaram, “STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS”, IRJET, Vol. 03 Iss. 01, January 2016
16. Gupta, Arachilage, Psannis, “Defending against Phishing Attacks: Taxonomy of Methods, Current Issues, and Future Directions”, NIT Kurukshetra, University of New South Wales and University of Macedonia
17. Kumar Jain, Gupta, “Phishing Detection: Analysis of Visual Similarity-Based Approaches”, Hindawi, January 2017
18. Shankar, Shetty, K. Nath, “A Review on Phishing Attacks”, IJAER, Vol. 14 Iss. 9, 2019