Phishing Detection: Using Machine Learning

Harrison Korodi

15BCN4002

ABSTRACT

Phishing is a type of cybercrime in which spammed messages and fake websites trick people into entering sensitive credentials and data, which the attackers then steal. The purpose of this paper is to investigate how modern-day phishing attacks occur, then to analyze URLs and fake websites for clues and patterns that 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. It builds and tests models using various combinations of settings, compares various machine learning techniques, and measures the precision of a prepared model. Using Neural Network with Adam, SGD, and RMSProp optimizers, I was able to find 26 patterns or odd indicators to show a web application is a phishing website during the current study. The study concludes with a final examination of the changes in results brought about by the Swarm Intelligence Technique with the TDLHBA parameter.

INTRODUCTION

As technology advances, the Internet and email have become an indispensible part of daily life. Unfortunately, the increased flexibility provided by technological advancement has resulted in criminals following the trend. As a result, many issues arise, one of which is identity theft. Phishing, a type of identity theft crime that has recently become a lethal security threat, is primarily targeted at casual email users. Phishing is an illegal activity that involves both social building and specialized deception in order to obtain sensitive secret information (e.g., government managed savings number, email address, passwords, and so on.) and financial record certifications. Phishing includes spam messages disguised as authentic, with a subject or message designed to trick victims into revealing sensitive information.

Phishing is the most dangerous criminal activity in cyberspace. Since most users go online to access government and financial institution services, there has been a significant increase in phishing attacks in recent years. Phishers began to earn money and are now running a successful business. Phishers use a variety of methods to target vulnerable users, including messaging, VOIP, spoofed links, and fake websites. It is very simple to create a counterfeit website that looks exactly like a legitimate website in terms of layout and content. The content of these websites would be identical to that of their legitimate counterparts. The purpose of these websites is to collect personal information from users such as account numbers, login IDs, debit and credit card passwords, and so on. Furthermore, attackers pose security questions for users to answer, posing as a high-level security measure. When users respond to those questions, they are more vulnerable to phishing attacks.

The remainder of this paper is structured as follows. The second section is a review of the literature. Section 3 delves into the social engineering framework, which is the weakest link in the cybersecurity chain. Section 4 provides a theoretical explanation of the various types of phishing attacks. Section 5 then discusses some examples of phishing attacks, and Section 6 investigates a demonstration of a small-scale phishing attack. Section 7 delves into determining whether URLs are safe or malicious. Section 8 discusses existing detection techniques. Section 9 describes the dataset collection process, the model's theory, and the architecture and other details of the neural model, while Section 10 describes the model I used to detect phishing. Finally, section 11 summarizes and concludes the paper.

LITERARY REVIEW

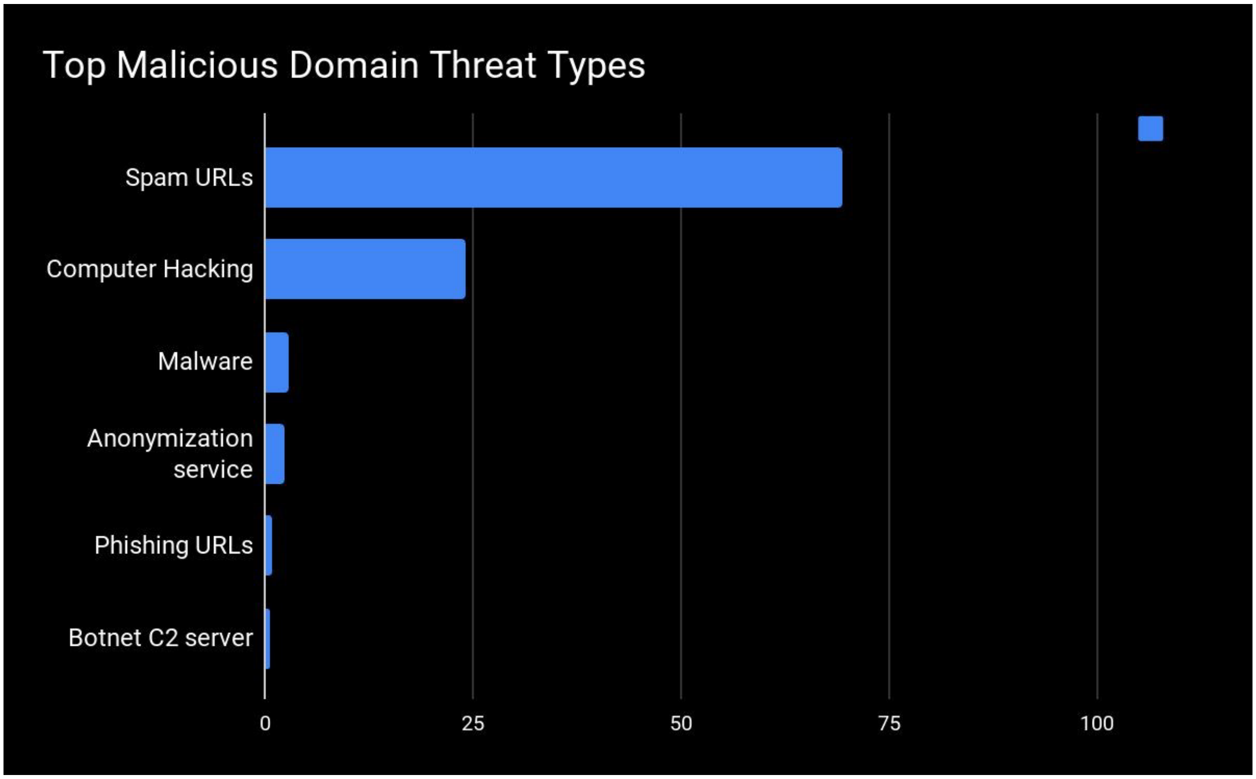
AP Kumar[1] provides us with a broad overview of the world of phishing, including the challenges that phishing presents to users and some general ideas for possible solutions, one of which is being investigated in this paper. Salahdine[10] proposes and investigates the social engineering framework used by attackers, explains existing countermeasures, and encourages the development of new countermeasures. Chauhan[13], Akamai[10], Shankar[19], and Dr. Damodaram[15] all contributed significantly to the idea and development of the study on the types of phishing attacks and examples of phishing attacks that have occurred around the world.

The authors of this paper[3] investigated the accuracy of various machine learning techniques and presented their findings in a simple yet elegant table. This served as the foundation for this study, with promising results encouraging further development of neural networks. Before deciding on convolutional neural network as the final algorithm, random forest[4], support vector machine[7], and recurrent neural network[6], [8] were all considered, but all of them were crutched on the machine to identify a general pattern, which could result in a large number of false positives and false negatives. The swarm intelligence approach was inspired by Fisher's research paper[5], in which the author proposed the idea of how swarms generally perform better in nature, and thus how it can also perform better in machine learning, and provided the algorithm for doing so. Finally, this paper[16] has been a huge help since it's a very detailed paper that discusses everything from the history of phishing attacks to the current challenges and how countermeasures are being developed and how attackers are attempting to circumvent them.

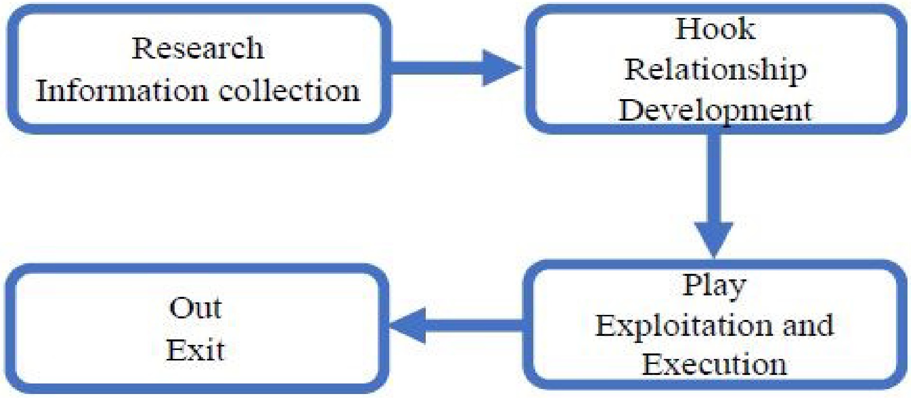
SOCIAL ENGINEERING FRAMEWORK

As previously stated, advances in digital communication technology have made human-to-human communication more accessible and instant. Individual and sensitive data, however, is also available online via social networks and online services that lack the necessary safeguards to protect this information. Communication networks are defenseless and can be infiltrated by malicious clients via social engineering attacks. Social engineering attacks are rapidly spreading in today's organizations, threatening the cybersecurity chain. They target innocent people and organizations in order to obtain vital and sensitive information for cybercriminals. Even the most powerful organizations are vulnerable to social engineering, regardless of the strength of their firewalls, cryptographic methods, intrusion detection frameworks, and antivirus software. Some believe that people are more important than computers or any other technology. As a result, they are the weakest link in the security chain. Malicious activities accomplished through human associations influence an individual's mental state, causing them to divulge sensitive information or interfere with security protocols. Because of these human connections, social engineering attacks are the most innovative attacks because they compromise all frameworks and organizations. They can't be stopped with software or hardware as long as people don't appear to be ready to stop these attacks. Cybercriminals choose these attacks when there is no way to hack into a framework with any technical flaws.

To demonstrate how lethal these attacks are, I conducted some research and used data from the IBM X-Force Threat Intelligence Report and the PurpleSec consulting service. Phishing (31 percent), Scan and Exploit (30 percent), and Stolen Credentials (29 percent) were the top three initial infection vectors seen in X-Force IRIS engagements in 2019. The problem is that social engineering is used in 98% of all attacks. According to Purplesec's recent data breach statistics, 63% of successful attacks originate from internal sources, such as control, errors, or fraud.

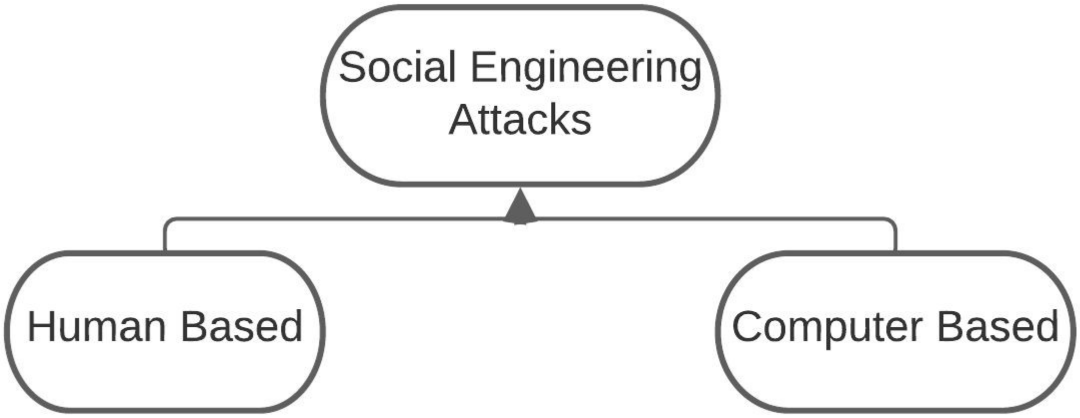


Although social engineering attacks vary from person to person, they all follow a similar pattern with similar phases. The common pattern consists of four phases: (1) gathering information about the target; (2) developing a relationship with the target; (3) exploiting the available information and carrying out the attack; and (4) exiting with no traces. Figure 1 depicts the various stages of a social engineering attack.

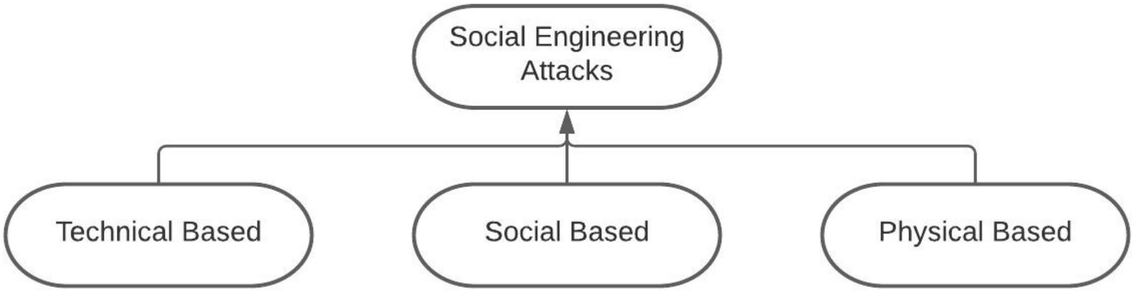


During the research stage, also known as information gathering, the assailant selects a target based on certain requirements. During the hook stage, the attacker begins to gain the target's trust through direct contact or email correspondence. During the play stage, the aggressor emotionally manipulates the target into disclosing sensitive information or committing security breaches. In the final stage, the assailant simply vanishes, leaving no trace.

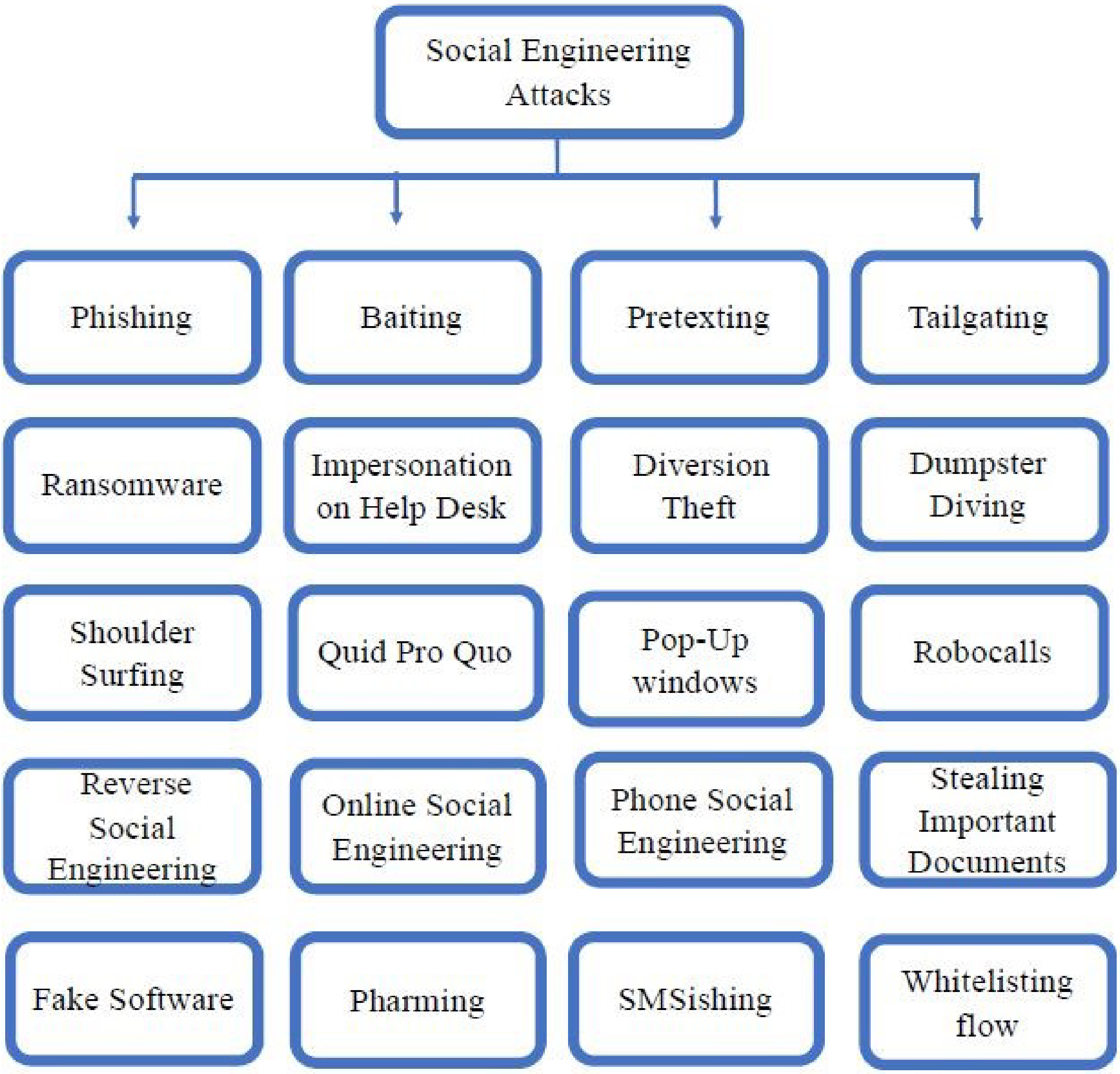
Social design can be divided into two categories: human-based and computer-based.



In human-based attacks, the attacker conducts the attack face to face by communicating with the victim to gather the necessary data. In this way, they can only affect a limited number of victims. One of the computer-based attacks used for spear-phishing messages is the social engineering toolkit (SET). Social engineering attacks are also classified into three types based on how they are carried out: social, technical, and physical-based attacks.



Social-based attacks are carried out by forming associations with the target in order to exploit their psychology and feelings. These are the most dangerous and fruitful attacks because they involve humans. Baiting and spear phishing are examples of these attacks. Technical-based attacks travel the web via social networks and online service sites, collecting data such as passwords, credit card information, and security questions. Physical-based attacks refer to actual activities carried out by the attacker in order to gather information about the target. Such attacks include searching dumpsters for any type of relevant documents, USBs, etc.



TYPES OF PHISHING ATTACKS

Client names, passwords, social security numbers, passport information, credit card numbers, account numbers, PIN numbers, birthdates, mother's family names, and so on are common targets of phishing attacks. Phishers can easily focus on technical expertise and sit in the comfort of their homes or hack workplaces to obtain sensitive data. In this section, I will demonstrate the various types of phishing attacks.

1. Attack by fraud

   In a fraudulent phishing attack, the hacker sends a deceptive email requesting the user to take action, typically referring to a problem with his financial balance, publicizing another service update, or offering a duplicate invoice, and so on. In all of the preceding cases, the client is redirected to a website where personal and sensitive data is extracted. The attacker may use a connection with a domain name that is nearly identical to the original domain name. If the user responds positively and allows the link to open and grants other permissions, malicious programs may be installed on the user's PC, leaving an open backdoor for future attacks.

CEO fraud, smishing (SMS phishing), spear phishing, and whaling are some examples of such attacks.

2. Attack by Infectious software

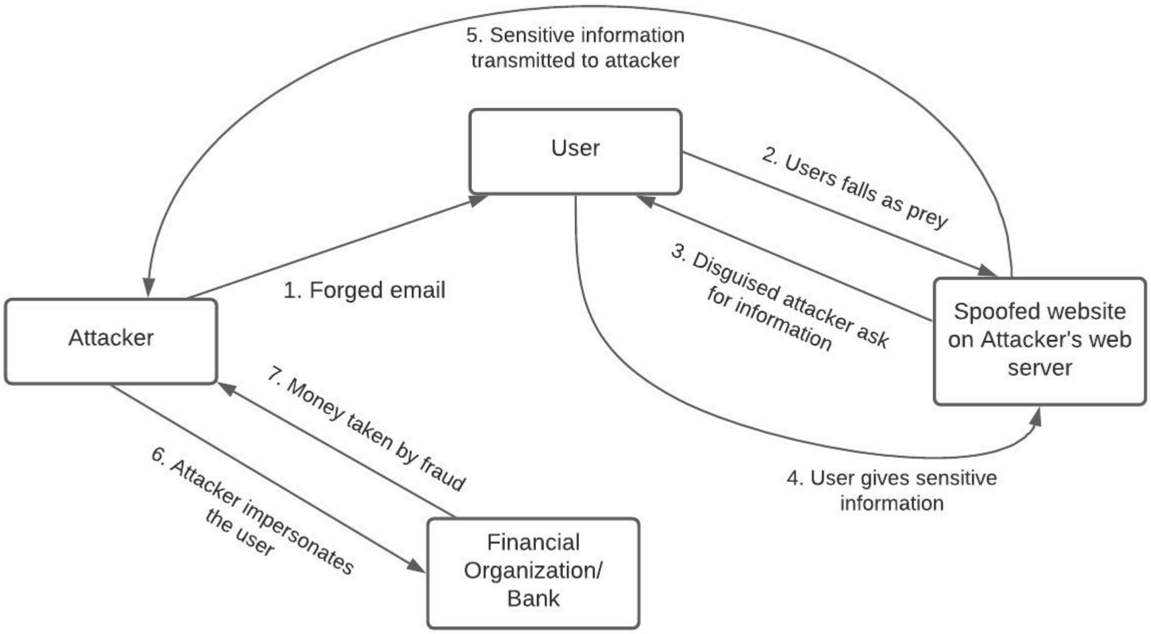
   In a malicious software phishing attack, the attacker takes advantage of security flaws in the PC or operating system. It frequently happens by enticing the user to open an email attachment with the promise of obscene pictures or other intriguing baits. Some open-source or free-to-download programs include malicious programs that are installed alongside the normal one. Keyloggers are covert software or programs that can be installed in an internet browser and/or work as a device driver to capture information entered by the client and upload it to a remote server set up by the attacker. Session hijacking can also occur as a result of a malicious browser component introduced by the attacker. The malware hijacks the session and transfers the user credentials to the hacker as soon as the user successfully logs in and completes a transaction with the website. Web Trojans that pop up to collect client information and send it back to the attacker are also common these days.

3. Attack by DNS Spoofing

   In DNS spoofing phishing attacks, the DNS lookup process is compromised on either the local PC or the DNS server. When a link is clicked or a domain address is entered in the web browser, the host files on a nearby PC are checked first before querying a DNS server to determine the IP address to domain mapping. If this file is compromised and false mapping is entered in the hosts' record by a malicious program, the client can go to the attacker's site and give personal data without realizing it. This was done by a Crowt.D worm attack in 2005. System configuration changes can be used to compromise the DNS server, allowing mapping to be poisoned..

4. Attack by inserting harmful content

   In phishing attacks, the attacker can exploit a server's security flaws by inserting malicious content rather than legitimate safe content, such as the cross-site scripting (XSS) flaw. Outside content, such as a chat message, search, or web email, would be delivered to the guest's internet browser. Such malicious activities can be carried out using the SQL injection vulnerability.


5. Sensitive information transmitted to attacker
User
2. Users falls as prey
3. Disguised attacker ask for information
1. Forged email
Attacker
Spoofed website on Attacker's web server
7. Money taken by fraud
6. Attacker impersonates the user
4. User gives sensitive information
Financial Organization/ Bank

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

   In man-in-the-middle phishing attacks, the attacker intercepts user traffic by placing himself between the user and the web application's server. He employs a proper response forwarding mechanism as the user communicates with the intended site, and he facilitates communication back to the user from the website - all through his computer. As a result, the user would have no reason to suspect traffic monitoring. This category includes clone phishing and evil twin phishing attacks.

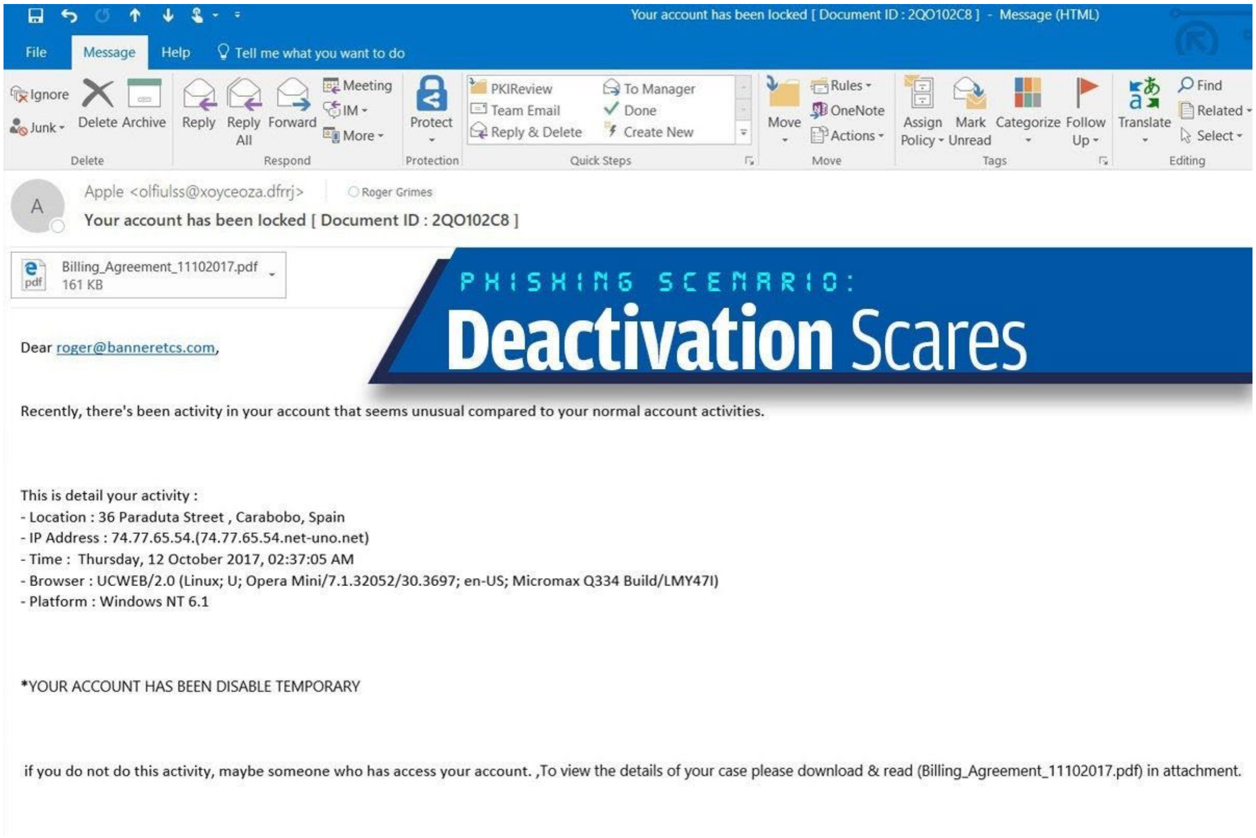
6. Attack by Search Engine Indexing

   In search engine indexing phishing attacks, the attacker creates a genuine-looking website for fake products where he can get users to perform financial transactions and attract users by offering better deals than other websites such as Amazon. This website would then be submitted to search engines for indexing, allowing any user to get a hit on the attacker's webpage. In such a scenario, fraudulent banks with higher interest rates may entice customers to make a cash transfer to the newly created account in the attacker's web trap.

EXAMPLES OF PHISHING ATTACKS

In this section, we will look at the technical aspects of common phishing attacks. There are four main techniques or classifications: (1) Email Field Manipulation Attack; (2) Email With Image-Only Content Attack; (3) Misdirection and Redirection Attack; and (4) Pop-up Window Attack. There are several different attacks that fall under the first two types, and I'll go over each of them here.

1. DEACTIVATION SCARES



Apple <olfiulss@xoyceoza.dfrrj>   Roger Grimes

Your account has been locked [Document ID : 2QO102C8]

Billing_Agreement_11102017.pdf
161 KB

Dear roger@banneretcs.com,

Recently, there's been activity in your account that seems unusual compared to your normal account activities.

This is detail your activity :
- Location : 36 Paraduta Street , Carabobo, Spain
- IP Address : 74.77.65.54.(74.77.65.54.net-uno.net)
- Time : Thursday, 12 October 2017, 02:37:05 AM
- Browser : UCWEB/2.0 (Linux; U; Opera Mini/7.1.32052/30.3697; en-US; Micromax Q334 Build/LMY47I)
- Platform : Windows NT 6.1

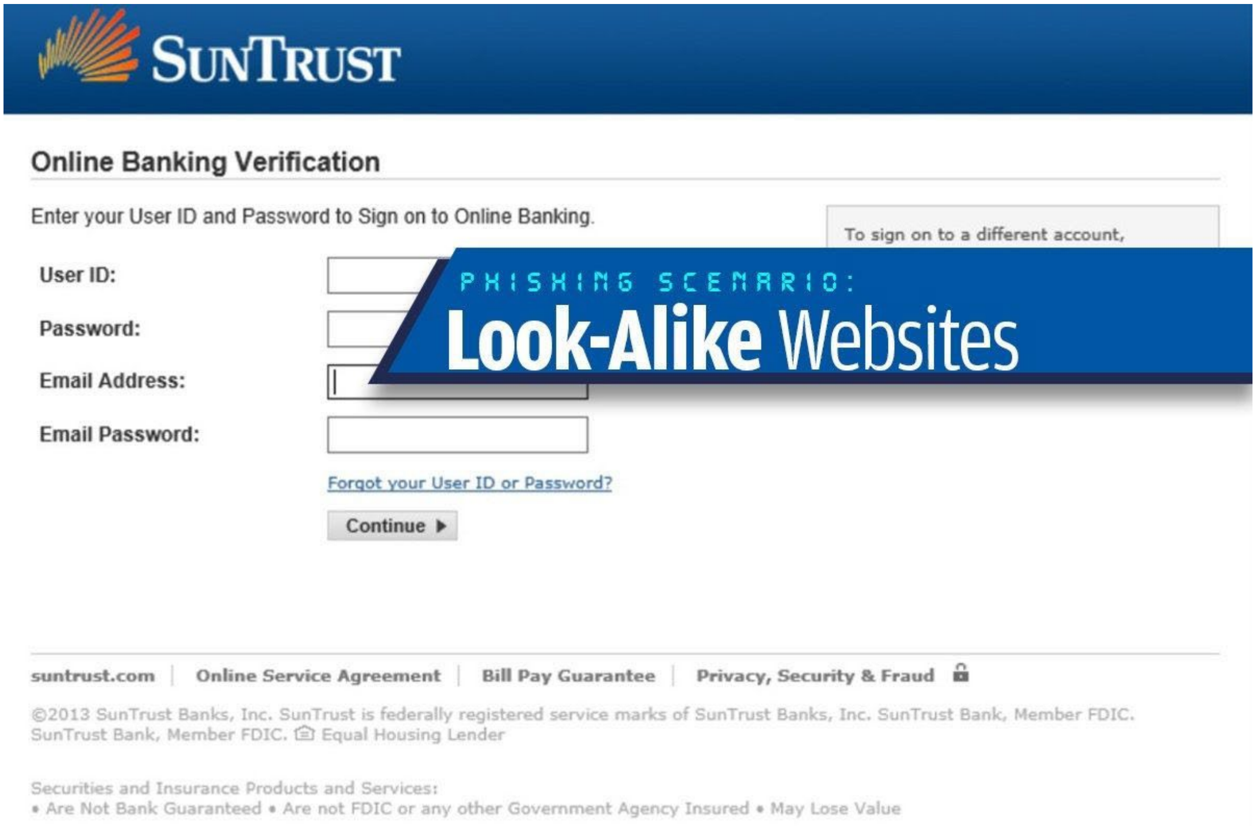
*YOUR ACCOUNT HAS BEEN DISABLE TEMPORARY

if you do not do this activity, maybe someone who has access your account. ,To view the details of your case please download & read (Billing_Agreement_11102017.pdf) in attachment.

DEACTIVATION EXAMPLE [SOURCE: CSOONLINE]

This is a trap that works more frequently than others because nothing scares people into responding as quickly as possible. Rarely a day goes by when an individual does not receive an email purporting to be from an organization with which they may or may not be affiliated. It asserts and guarantees that their account will be deactivated if they don't click a link, enter their login name, password, and secret phrase, and make an immediate move - most likely to update their credit card. These were once easy to identify. In any case, they appear to be exceptionally authentic today. They may include genuine links to the organization from which they claim to be. They may even include "Beware of scammers" warnings or comforting notices like "Examined and Cleaned by AV." It's completely obvious if the phishers claim to be from a company with which an individual has no history. However, if they do have a record, and they have recently moved or canceled any type of card, users can expect the company to put everything back in order by managing this quickly.

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,

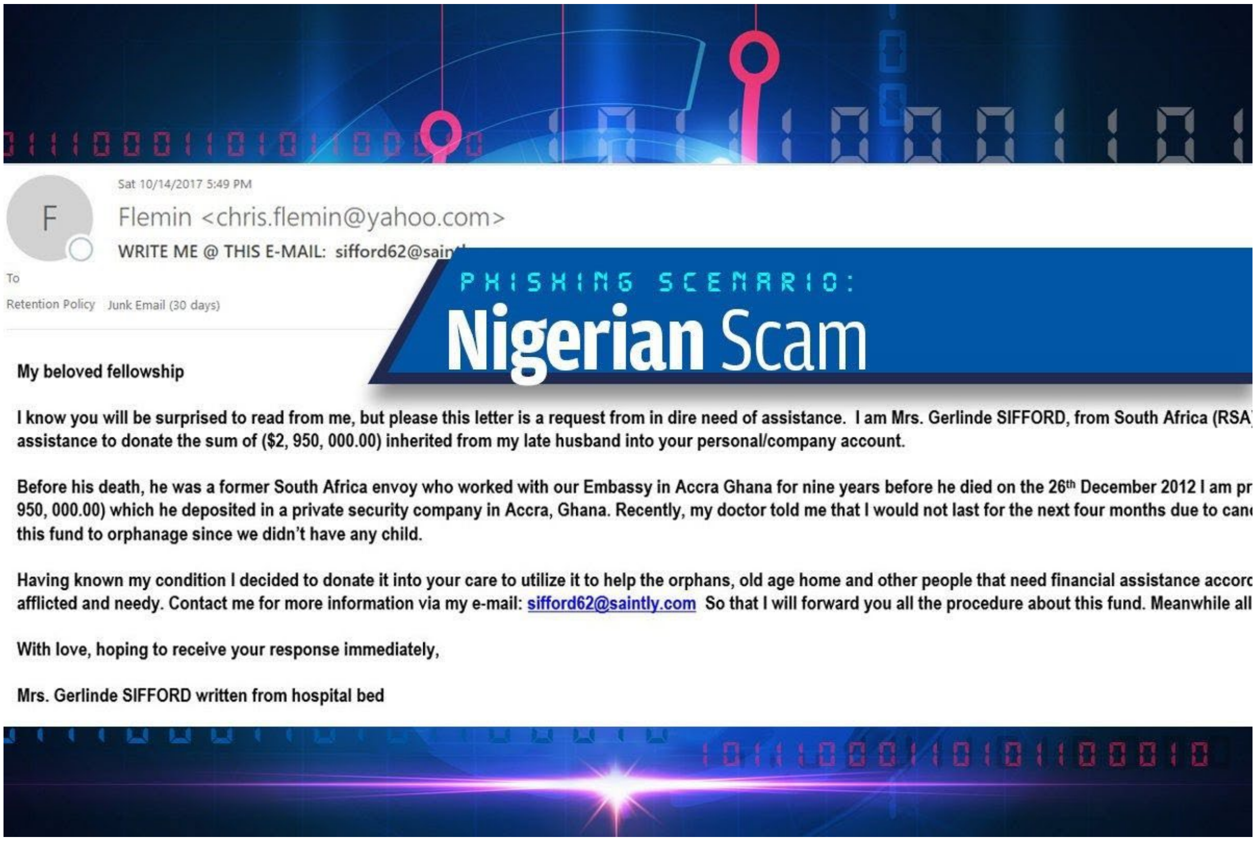
©2013 SunTrust Banks, Inc. SunTrust is federally registered service marks of SunTrust Banks, Inc. SunTrust Bank, Member FDIC. SunTrust Bank, Member FDIC. Equal Housing Lender

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's become difficult to distinguish between a phishing site and a legitimate site. The forgeries are exact replicas with the genuine site's URL as a component of the URL. If you look closely, you will notice that the phishing site redirects to a different domain. However, this is barely noticeable when the site appears to be the genuine article. The screenshot above depicts a phishing email that falsely claims to be from a legitimate bank. Sun Trust clients may fall victim to this phish because the site appears to be familiar, despite the fact that the URL is fake.

3. NIGERIAN SCAMS



Sat 10/14/2017 5:49 PM

Flemin <chris.flemin@yahoo.com>

WRITE ME @ THIS E-MAIL: sifford62@sain

To

Retention Policy Junk Email (30 days)

My beloved fellowship

I know you will be surprised to read from me, but please this letter is a request from in dire need of assistance. I am Mrs. Gerlinde SIFFORD, from South Africa (RSA assistance to donate the sum of ($2, 950, 000.00) inherited from my late husband into your personal/company account.

Before his death, he was a former South Africa envoy who worked with our Embassy in Accra Ghana for nine years before he died on the 26th December 2012 I am pr 950, 000.00) which he deposited in a private security company in Accra, Ghana. Recently, my doctor told me that I would not last for the next four months due to can this fund to orphanage since we didn't have any child.

Having known my condition I decided to donate it into your care to utilize it to help the orphans, old age home and other people that need financial assistance accord afflicted and needy. Contact me for more information via my e-mail: sifford62@saintly.com So that I will forward you all the procedure about this fund. Meanwhile all

With love, hoping to receive your response immediately,

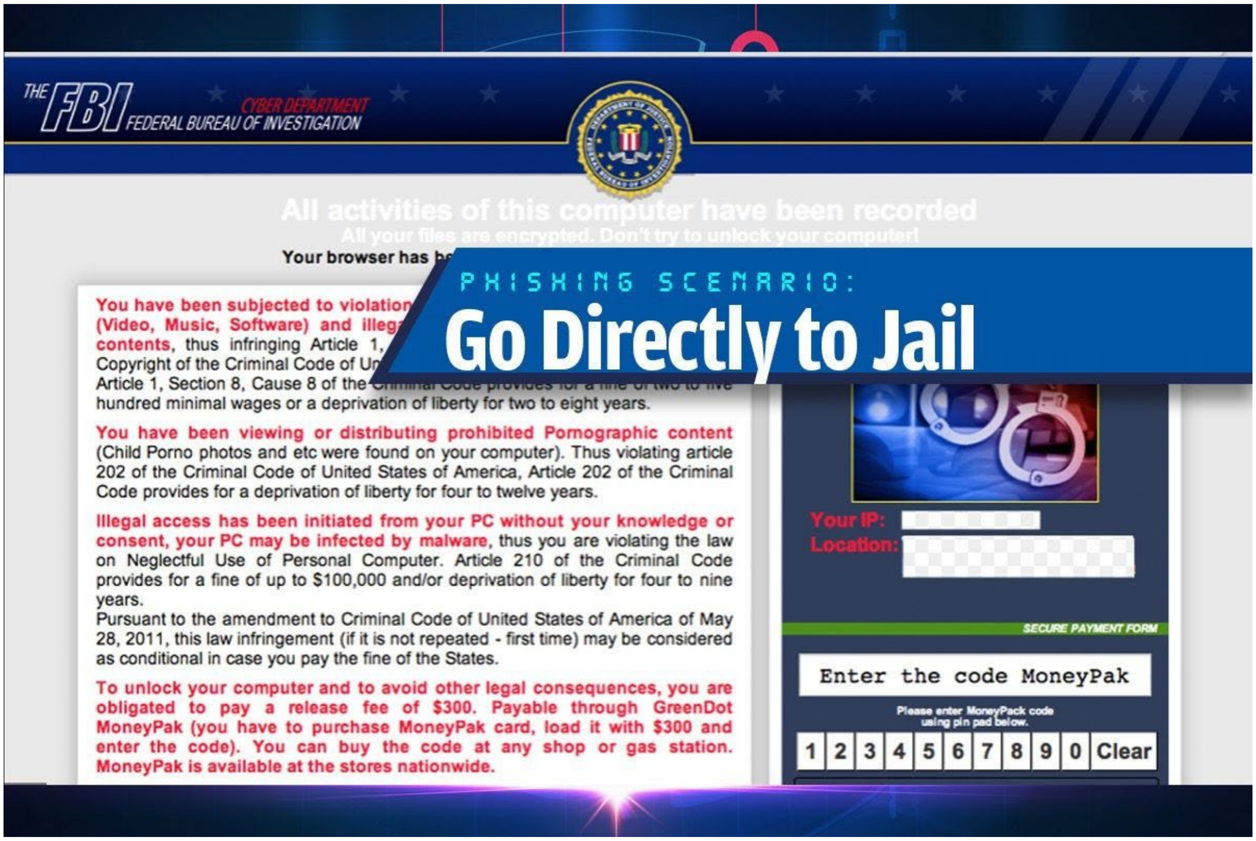
Mrs. Gerlinde SIFFORD written from hospital bed

NIGERIAN SCAM EXAMPLE [SOURCE: CSOONLINE]

This phishing lure, officially known as "advance fee frauds," became known as Nigerian scams decades ago because Nigerian fraudsters appear to attempt them far more frequently than any other country - at least per capita.

You might chuckle at the terrible language structure and absurd situations proposed, wondering, "What rational individual would fall for such a trickery?" However, those elements serve as a global filter. Every day, the average Nigerian scammer sends out a large number of deceptive messages. Furthermore, the majority of them are blocked and dumped by email users or their antimalware software. However, the average email user is not the target audience for this scam. This bait is designed to attract more vulnerable targets. For some people, carelessness and mistakes are not a hindrance, which is the prize that this phisherman is after.

4. GO DIRECTLY TO JAIL


THE FBI FEDERAL BUREAU OF INVESTIGATION
CYBER DEPARTMENT
PHISHING SCENARIO:
Go Directly to Jail
Your IP:
Location:
SECURE PAYMENT FORM
Enter the code MoneyPak
Please enter MoneyPack code using pin pad below.
1 2 3 4 5 6 7 8 9 0 Clear

All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has be

You have been subjected to violation (Video, Music, Software) and illeg contents, thus infringing Article 1, Copyright of the Criminal Code of Un Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.

Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

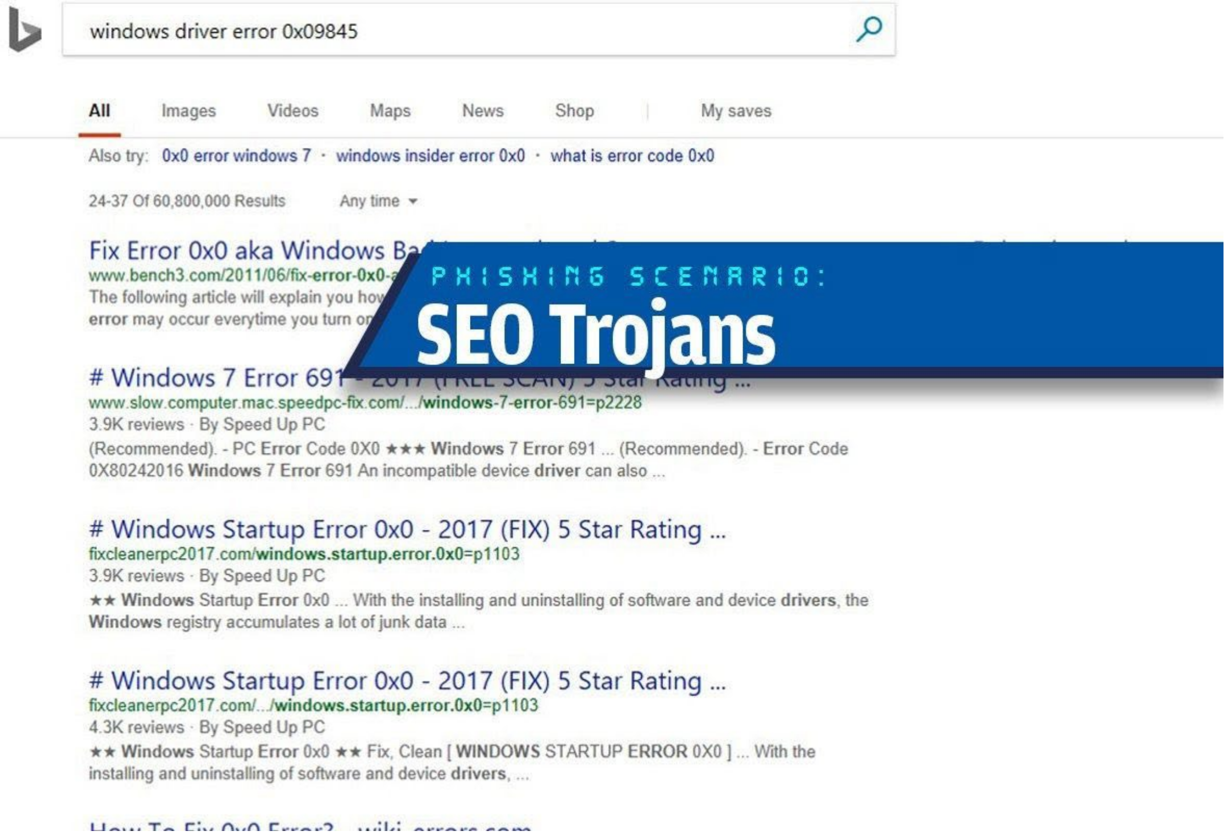
To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

GO TO JAIL EXAMPLE [SOURCE:CSOONLINE]

This is classified as a popup phishing attack. Phishers understand that everyone feels guilty inside and use it to catch us off guard. Even if the thing you're regretting isn't illegal, you can easily be misled into worrying that you've been caught. Furthermore, nothing motivates people to act quickly and absurdly more than the threat of imprisonment. As a result, in the United States, phishing scams that use forged FBI warnings to encourage illegal music downloading or pornographic viewing take the lead. Counterfeit IRS threats for tax return issues are also extremely effective. These baits are frequently delivered by phone, which may be intended to create and heighten the sense of urgency.

Many people pay even though they know they did not cheat their taxes, watch porn, or download music. They simply want the warning to go away - which it will not - or they expect another member of the family to be responsible. Unfortunately, phony punishment warnings sent via email frequently contain ransomware, which will completely lock down your PC until you pay.

5. SEO TROJANS



Also try: 0x0 error windows 7 · windows insider error 0x0 · what is error code 0x0

24-37 Of 60,800,000 Results Any time

Fix Error 0x0 aka Windows Ba
www.bench3.com/2011/06/fix-error-0x0-a
The following article will explain you how
error may occur everytime you turn on

Windows 7 Error 691
www.slow.computer.mac.speedpc-fix.com/.../windows-7-error-691=p2228
3.9K reviews · By Speed Up PC
(Recommended). - PC Error Code 0X0 ★★★ Windows 7 Error 691 ... (Recommended). - Error Code 0X80242016 Windows 7 Error 691 An incompatible device driver can also ...

Windows Startup Error 0x0 - 2017 (FIX) 5 Star Rating ...
fixcleanerpc2017.com/windows.startup.error.0x0=p1103
3.9K reviews · By Speed Up PC
★★ Windows Startup Error 0x0 ... With the installing and uninstalling of software and device drivers, the Windows registry accumulates a lot of junk data ...

Windows Startup Error 0x0 - 2017 (FIX) 5 Star Rating ...
fixcleanerpc2017.com/.../windows.startup.error.0x0=p1103
4.3K reviews · By Speed Up PC
★★ Windows Startup Error 0x0 ★★ Fix, Clean [WINDOWS STARTUP ERROR 0X0] ... With the installing and uninstalling of software and device drivers, ...

How To Fix 0x0 Error? - wiki.errors.com

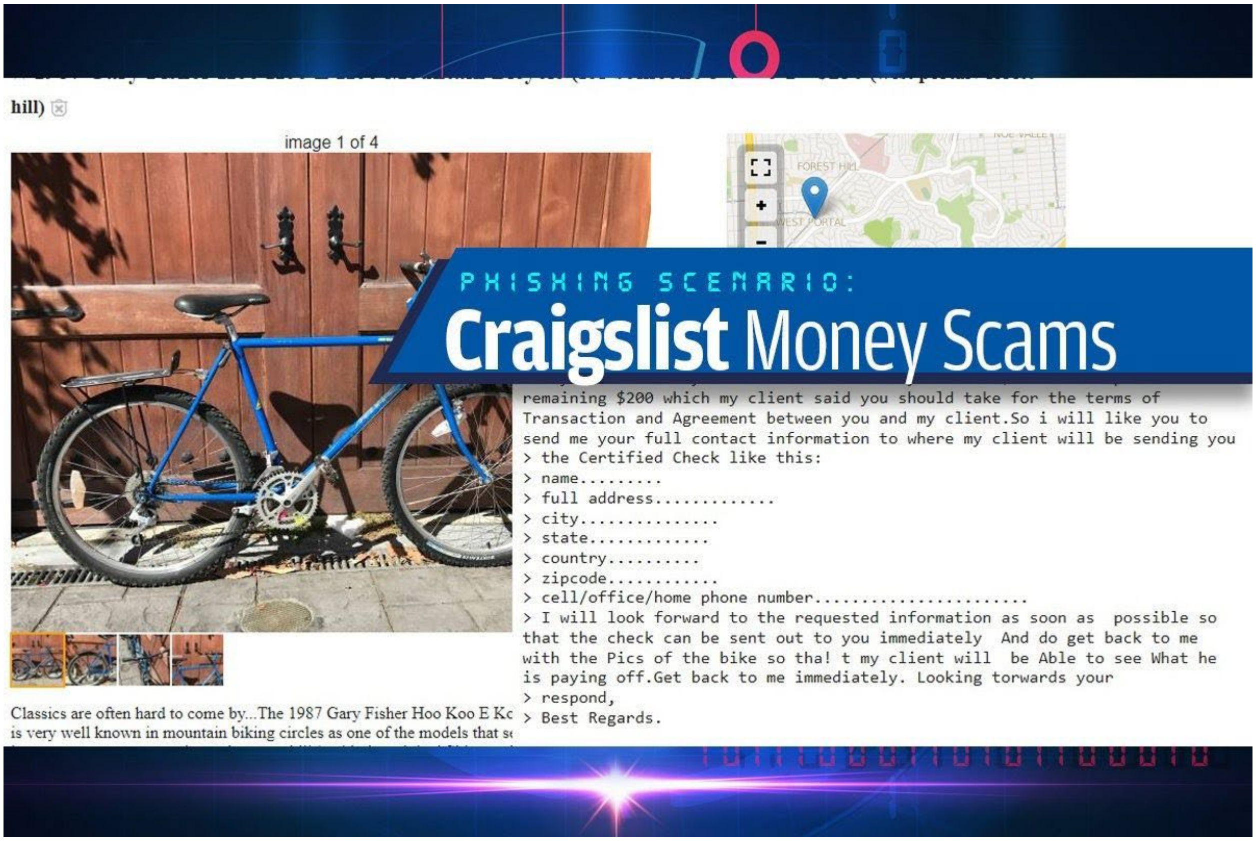
SEO TROJAN EXAMPLE [SOURCE:CSOONLINE]

By appearing at the top of your search results, one common phishing scam tricks you into installing malicious software directly from the web. This is known as Search Engine Optimization (SEO) poisoning.

It works in the following way: You have a technical problem and immediately assume that it is caused by a bug in a device driver. Or perhaps you received an error message and looked it up on Google to figure out what was wrong. These are viable approaches to finding a solution. But every now and then, you come across a website that appears genuine and promises a quick solution. All you have to do is download and install the software. The issue this time is that the code is malicious.

In this screenshot, I looked for an error code that didn't exist. The search engine returned its best match, which includes websites willing to sell me "fix-it" software. In this case, I know there's nothing to fix and that this error code doesn't exist. Some of the links in this example may not be malicious in the strictest sense. These are simply what computer technicians refer to as "pest" software.

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



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

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 tha! t my client will be Able to see What he
is paying off.Get back to me immediately. Looking torwards your
> respond,
> Best Regards.

CRAIGSLIST FRAUD EXAMPLE [SOURCE:CSOONLINE]

Fraudsters adore scouring personal advertisements and auction websites for victims. By far their most popular fishing hole is now Craigslist worldwide and OLX in India. This isn't because these websites are evil or anything. This is because people appear at them, ready to click and visit links and exchange personal information and money.

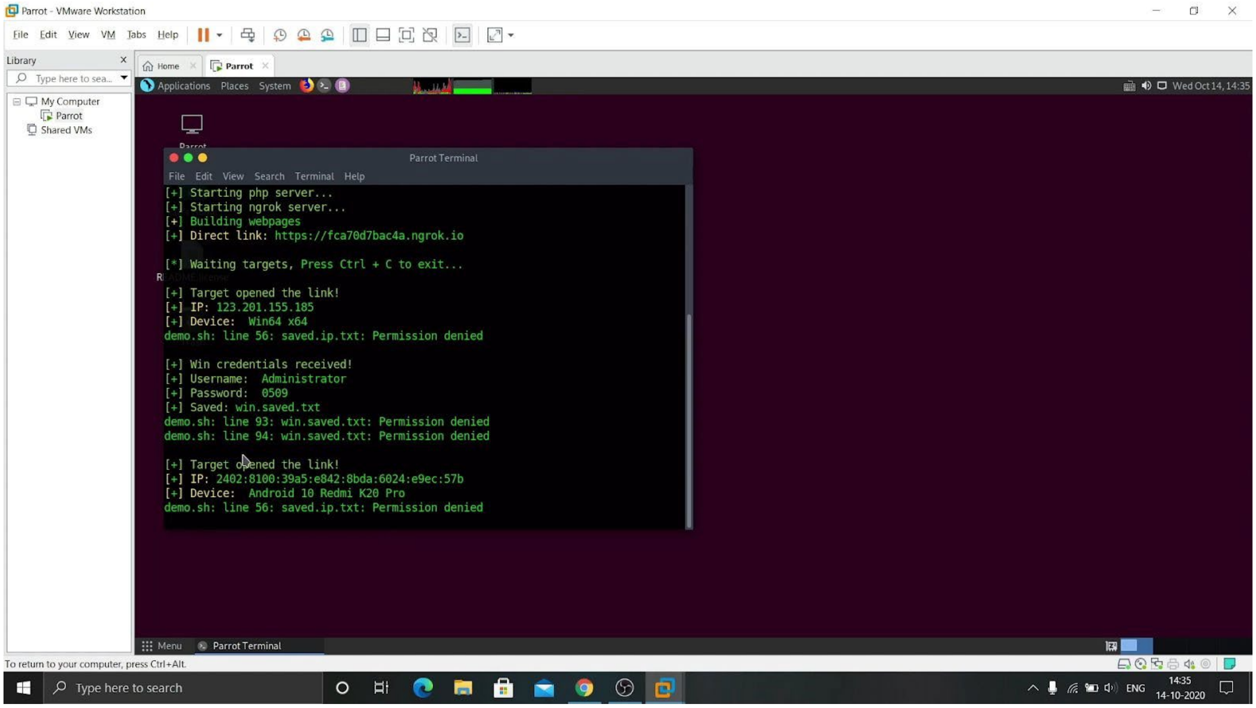
Money scams on Craigslist can take many forms. The most common one occurs when you go there to sell. To your delight, a buyer arrives quickly and offers to pay your full price - including shipping! That was simple. But wait, there's more. They confidently offer to overpay if you use their independent, trusted intermediary to handle payment and delivery costs. They offer a large sum of money in exchange for this. They ask that you remove your portion and forward the remainder to their intermediary.

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

You are currently liable for the fraudulent funds you transferred to the intermediary. Do not make the mistake of assuming that your bank will verify your check when you deposit it. They will not.

SMALL-SCALE PHISHING DEMONSTRATION

To demonstrate how phishing works on a small scale, I created a shell script that uses ngrok and a simple redirection to a webpage. The shell script basically generates a URL that can be shortened using a URL shortener service. That can be sent to anyone we want, and when the target opens the URL, it redirects them to their device's lookalike lock screen and forces them to enter the password captured on our screen.


Parrot - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Parrot
Shared VMs
Home
Parrot
Applications Places System
Wed Oct 14, 14:35
Parrot Terminal
File Edit View Search Terminal Help
Menu
Parrot Terminal
To return to your computer, press Ctrl+Alt.
Type here to search
ENG
14:35
14-10-2020

```
[+] Starting php server...
[+] Starting ngrok server...
[+] Building webpages
[+] Direct link: https://fca70d7bac4a.ngrok.io

[*] Waiting targets, Press Ctrl + C to exit...

[+] Target opened the link!
[+] IP: 123.201.155.185
[+] 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 most difficult aspects of defending against phishing attacks is that people are unaware they are being phished. As a result, I intend to shed some light on the key features that have proven to be sound and effective in manually predicting phishing websites. In addition, I propose some other features that I believe are phishing URL signatures.

1.1 ADDRESS BAR BASED FEATURES

1.1.1 Using the IP address

If an IP address is used in the URL instead of a domain name, such as "http://129.91.9.193/fake.html", users can be certain that someone is attempting to steal their personal information. As shown in the following link, the IP address is sometimes converted into hexadecimal code: "http://0x5E.0xAA.0xCA.0x69/2/paypal.ca/index.html".

1.1.2 Long URL to Hide the Suspicious Part

Phishers can use a lengthy URL to conceal the suspicious portion in the address bar. As an example:
http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=home&amp;dispatch=11004d58f5b74f8dc1e7c2e8dh4105e811004d58f5b74f8dc1e7c2e8dd4105e8@phishing.website.html

We calculated the length of URLs in the dataset and produced an average URL length to ensure the accuracy of our study. The results revealed that if the URL is longer than or equal to 54 characters, it is classified as phishing. By reviewing our dataset, we discovered 1220 URLs with lengths of 54 or more, accounting for 48.8% of the total dataset size. I propose that by using a frequency-based method, we can improve the algorithm's accuracy.

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 reduced in length while still redirecting to the desired web page. This is accomplished by using a "HTTP Redirect" on a short domain name, which links to a webpage with a long URL. The URL "http://www.vitap.ac.in/" can, for example, be shortened to "bit.ly/19DXSk4".

1.1.4 URLs having “@” symbol

When the "@" symbol is used in a URL, the browser ignores everything preceding the "@" symbol, and the true address frequently follows the "@" symbol.

1.1.5 Redirecting using “//”

If there is a "//" in the URL path, the user will be redirected to another website. "http://www.legitimate.com//http://www.phishing.com" is an example of such a URL. We look at the place where the "//" appears. We discovered that if the URL begins with "HTTP", the "//" should appear in the sixth position. If the URL contains "HTTPS," the "//" should appear in the seventh position.

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

In legitimate URLs, the dash symbol is almost never used. Phishers frequently add prefixes or suffixes separated by (-) to domain names in order to give users the impression that they are dealing with a legitimate website. For instance, see http://www.confirme-paypal.com/.

1.1.7 Sub Domain and Multi Sub Domain

Assume we have access to the following URL: http://www.vitap.ac.in/students/. A domain name may include a country-code top-level domain (ccTLD), such as "in" in our example. The "ac" part stands for "academic," the combined "ac.in" is known as a second-level domain (SLD), and "vitap" is the domain's actual name. To create a rule for extracting this feature, we must first remove the (www.) from the URL, which is a subdomain in and of itself. Then, if the (ccTLD) exists, it must be removed. We then count the remaining dots. Because the URL has one subdomain, it is classified as "Suspicious" if the number of dots is greater than one. However, if the number of dots is greater than two, it’s classified as "Phishing" because it will have multiple subdomains. If the URL does not have any subdomains, we will assign "Legitimate" to the feature.

1.1.8 HTTPS and Certificate

The presence of HTTPS is critical in conveying the legitimacy of a website, but it is clearly insufficient. I recommend verifying the HTTPS certificate, including the scope of the trust certificate issuer and the certificate age. Certificate Authorities such as "GeoTrust, GoDaddy, Network Solutions, Thawte, Comodo, Doster, and VeriSign" are consistently listed among the most trustworthy names. In addition, based on a review of other research papers, I discovered that the minimum age of a reputable certificate is two years.

1.1.9 Domain Registration Length

Given the short lifespan of a phishing website, we believe that trustworthy domains are frequently paid for several years in advance. According to my research, the longest fraudulent domains have been used for a maximum of one year or so.

1.1.10 Favicon

A favicon is a graphic image (icon) that is associated with a particular webpage. Many existing user agents, such as graphical browsers and newsreaders, display favicons in the address bar as a visual reminder of the website's identity. If the favicon is loaded from a domain other than the one shown in the address bar, the webpage is most likely a phishing attempt.

1.1.11 Using a non-standard port

This feature is useful for determining whether a specific service (e.g., HTTP) is available or unavailable on a specific server. To control intrusions, it is far better to simply open the ports that are required. Several firewalls, proxy servers, and Network Address Translation (NAT) servers will, by default, block all or most of the ports and only allow access to those that are explicitly allowed. If all ports are open, phishers can run almost any service they want, putting user information at risk.

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

In order to trick users, phishers may add the "HTTPS" token to the domain part of a URL. As an example, http://https-www-paypal-it-webapps-mpp-home.soft-hair.com/

1.2 ABNORMAL BASED FEATURES

1.2.1 Request URL

Request URL determines whether external objects such as images, videos, and sounds contained within a webpage are loaded from another domain. The webpage address and the majority of the objects embedded within the webpage share the same domain in legitimate webpages.

1.2.2 URL of Anchor

The <a> tag defines an anchor as an element. This feature is treated exactly like the "Request URL" feature. 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. < a href="#">

   B. < a href="#content">

   C. < a href="#skip">

   D. < a href="JavaScript ::void(0)">

1.2.3 Server Form Handler (SFH)

SFHs with an empty string or "about:blank" are considered suspicious because action should be taken based on the submitted information. Furthermore, if the domain name in SFHs differs from the domain name of the webpage, this indicates that the webpage is suspect because submitted information is rarely handled by external domains. So, if SFH is empty, it is almost certainly a phishing site, and if it redirects to a different domain, it’s still suspicious.

1.2.4 Submitting Information as forms or via email

A web form enables a user to submit personal information, which is then routed to a server for processing. A phisher may send the user's information to his personal email address. To that end, a server-side scripting language, such as PHP's "mail()" function, could be used. The "mailto:" function is another client-side function that could be used for this purpose.

1.3 HTML AND JAVASCRIPT BASED FEATURES

1.3.1 Website Forwarding

The number of times a website has been redirected is the fine line that separates phishing websites from legitimate ones. Phishing websites have been observed to redirect at least three times.

1.3.2 Status Bar Customization

Phishers may use JavaScript to display a bogus URL in the status bar. To extract this feature, we must examine the webpage source code, specifically the "onMouseOver" event, and see if it changes the status bar.

1.3.3 Disabling Right Click

Phishers typically use JavaScript to disable the right-click function, preventing users from viewing and saving the webpage source code. This feature is exactly the same as "Using onMouseOver to hide the Link." Nonetheless, for this feature, we will search the webpage source code for the event "event.button==2" and see if the right-click is disabled.

1.3.4 Using Pop-Up Window

It's unusual to find a legitimate website that requests personal information from users via a pop-up window. This feature, on the other hand, has been used in some legitimate websites, and its main goal is to warn users about fraudulent activities or to broadcast a welcome announcement, even though no personal information was requested through these pop-up windows.

1.3.5 IFrame Redirection

IFrame is an HTML tag that displays another webpage within the one that is currently displayed. Phishers can use the "iframe" tag to make the frame invisible, i.e. without frame borders. Phishers use the "frameBorder" attribute to cause the browser to render a visual delineation.

1.4 DOMAIN BASED FEATURES

1.4.1 Age of Domain

This information can be obtained from the WHOIS database. Most phishing websites only exist for a short time. ***The minimum age of a legitimate website is 6 months.***

1.4.2 DNS Record

In the case of phishing websites, either the claimed identity is not recognized by the WHOIS database or no records for the hostname are found. If the DNS record is empty or not found, the website is considered "Phishing," otherwise it is considered "Legitimate."

1.4.3 Website Traffic

This feature assesses the popularity of a website by counting the number of visitors and the pages they visit. However, because phishing websites only exist for a short time, the Alexa database may not recognize them. In the worst-case scenarios, legitimate websites ranked among the top 100,000. Furthermore, if the domain receives no traffic or is not recognized by the Alexa database, it is labeled "Phishing." Otherwise, it’s classified as "Suspicious".

1.4.4 Pagerank

PageRank is a number that ranges from "0" to "1". PageRank attempts to determine the importance of a webpage on the Internet. The higher the PageRank value, the more significant the webpage. ***Most phishing websites do not have any PageRank whatsoever.***

1.4.5 Number of Links Pointing to Page

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

EXISTING PHISHING DETECTION TECHNIQUES

1. TRADITIONAL METHODS FOR PHISHING DETECTION

This method is further divided into two categories: authentication protection and network security.

Network-level security includes two types of filters: white-list filters and black-list filters, which work by blocking IP addresses and domains from a given network. There is also a rule-based filter and a pattern-matching filter.

- Black-list Filter

  This protects the network layer of the OSI model by classifying email DNS addresses, IP addresses, and sender addresses and comparing them to a predefined list. If the data matches, the email is rejected.

- White-list Filter

  The email data is compared to a predefined list of IP addresses and static IP addresses of legitimate domains in this technique. Only emails with a hit are allowed access here.

- Pattern-matching Filter

  This is used to determine whether an email is spam or not by searching the email in a pattern list and determining whether the email contains more than a certain amount of banned text.

- Email verification

  A client-level verification system is email confirmation. The system necessitates confirmation from both the sender and the receiver.

2. AUTOMATED METHODS
    - Logistic Regression

      This algorithm predicts binary data, i.e. 0 or 1, using a linear model. It is simple to interpret and understand, and it produces good results with some data. However, it's quite simple, and as a result, attackers have devised a number of other methods to circumvent it.

    - Decision Trees Filter(DT)

      The decision tree algorithm is built on a node and arrow model and starts at the root node. To filter out spam emails, if-then rules are applied to every node in the network using every possible condition.

    - Support Vector Machine(SVM)

      SVM has been used for a long time in various fields such as healthcare for disease diagnosis, text recognition, image classification, and other purposes. SVM divides data into two categories by using fixed rules, quadratic equations, and statistics. SVM used to provide the best solution to a problem, but it fails to analyze large amounts of data.

DATASET COLLECTION AND THEORY BEHIND THE NEURAL MODEL USED

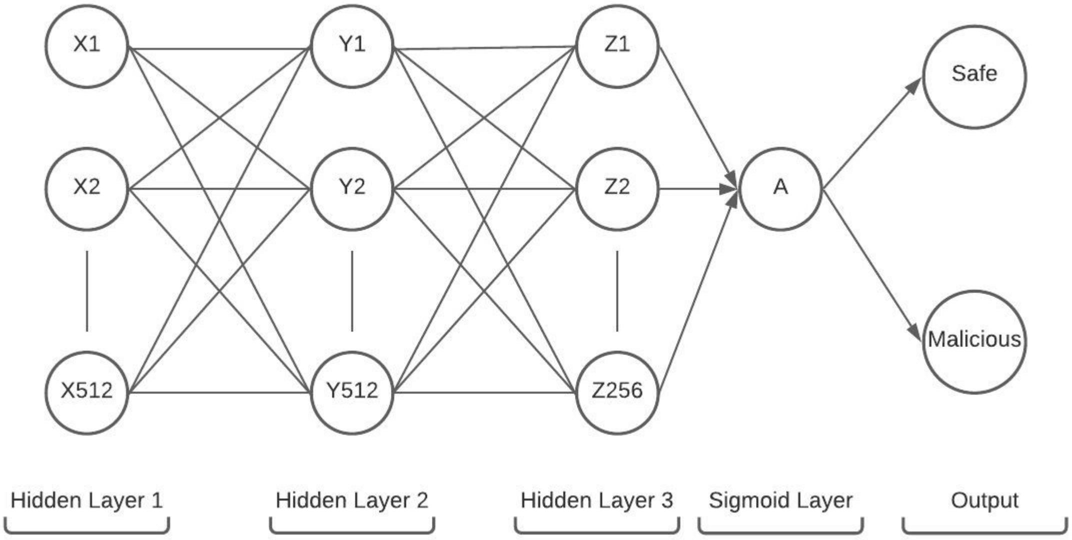
Dataset collection is a critical component of any project involving data analysis and machine learning. The main sources for finding datasets for any project on the Internet are Kaggle, UCI Machine Learning Repository, and Github. However, conducting a literary review provides a unique perspective on dataset selection. Following a review of various papers, I identified three potential datasets that could be used for the project:

1. UCI Phishing Dataset(https://archive.ics.uci.edu/ml/datasets/phishing+websites)
2. Phishstorm Dataset(https://research.aalto.fi/en/datasets/phishstorm-phishing-legitimate-url-dataset)
3. Phishtank Dataset(https://machinelearning.inginf.units.it/data-and-tools/hidden-fraudulent-urls-dataset)

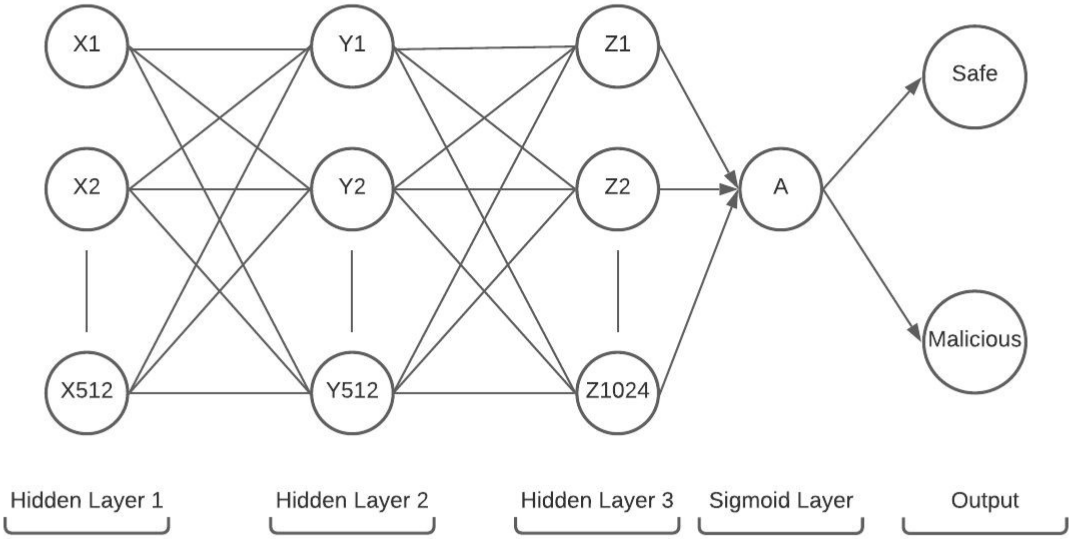
Finally, I decided to work with the UCI Phishing Dataset because, of the three, I concluded it to be the most trustworthy and reliable due to its creation from the PhishTank archive, the MillerSmiles archive, Google's searching operators, and the large number of papers written with it as the foundation.
After deciding on a dataset, research on various algorithms began. The paper[3] research assisted in determining that from other machine learning algorithms such as linear regression, Naive Bayes, kNN, Random Forest, and neural networks. The neural network showed the most promise of all of them and was thus chosen for this project.

A neural network is a set of algorithms that attempts to recognize underlying relationships in a set of data using a process similar to how the human brain works. In other words, we are attempting to assist the machine in making decisions on its own. The Sequential API in Keras is extremely powerful for creating layered neural networks. We are aware that sequential API is slightly less useful than functional API, but because we are not concerned with multiple inputs, there is no need to increase the project's complexity; however, we will demonstrate in the Swarm Intelligence demonstration that functional API produces more accurate results.

Since we want a fully connected neural network architecture, we use the Dense Layer, which works by each neuron receiving input from all neurons in the previous layer. When we first start the model, we have the input layer with 512 nodes and a ReLu activation function, then hidden layer 1 with 512 nodes and a ReLu activation function, hidden layer 2 with 256 nodes and a Sigmoid activation function, and finally the output layer with 1 node and a Sigmoid activation function.



The second model we trained had a minor change. In the hidden layer 2, instead of 256 nodes, we have 1024 nodes to see if increasing the number of nodes in the model improves the output.



In this experiment, we are experimenting with three different types of optimizers: the original basic SGD, or Stochastic Gradient Descent; an adaptive learning optimizer RMSProp; and an algorithm derived from both, the Adam optimizer.

The main advantage of SGD is that we only have to calculate the cost of one example for each step, which greatly speeds up the neural network. SGD is typically noisier than standard gradient descent and may require more iterations to reach the minima due to its randomness in descent, but it is computationally less expensive, which is what we want if we want to use an algorithm in a browser. However, when compared to the newer algorithm, it converges slower and has issues with being stuck in a local minimum.

The RMSprop optimizer works in the same way as the gradient descent algorithm with momentum. It dampens vertical oscillations during descent. As a result, we can boost the learning rate and make our algorithm converge faster in the horizontal.

The Adam optimizer is an SGD extension. The primary distinction between Adam and SGD is that SGD uses a single learning rate for all weight updates. Adam, on the other hand, maintains a per-parameter learning rate with sparse gradients (from AdaGrad) and online and non-stationary problems (from RMSProp). It is computationally efficient and requires very little memory.

Finally, there’s Swarm Intelligence. Swarm intelligence, a branch of artificial intelligence that studies the collective behavior of complex and decentralized systems with social structure, was coined in 2009 by two researchers, Michael and Konstantinos. In other words, it attempts to mimic the colonial nature of ants or bird flock patterns. In this case, we take inspiration from the paper[5] and employ the "Bat Algorithm," which attempts to mimic the behavior of bats, according to the author. The main steps in the Bat Algorithm are as follows:

1. Initialization: A starting population is created.
2. New solution generation: Bats use physical rules of echolocation to find new solutions and move within the search space.

3. Local Search Step: Using random walk-based heuristics, the best solution is improved.
4. New solution evaluation: The new solution is being evaluated.
5. Conditional best solution saving: The new best solution is saved with a certain probability.
6. Identifying the best solution

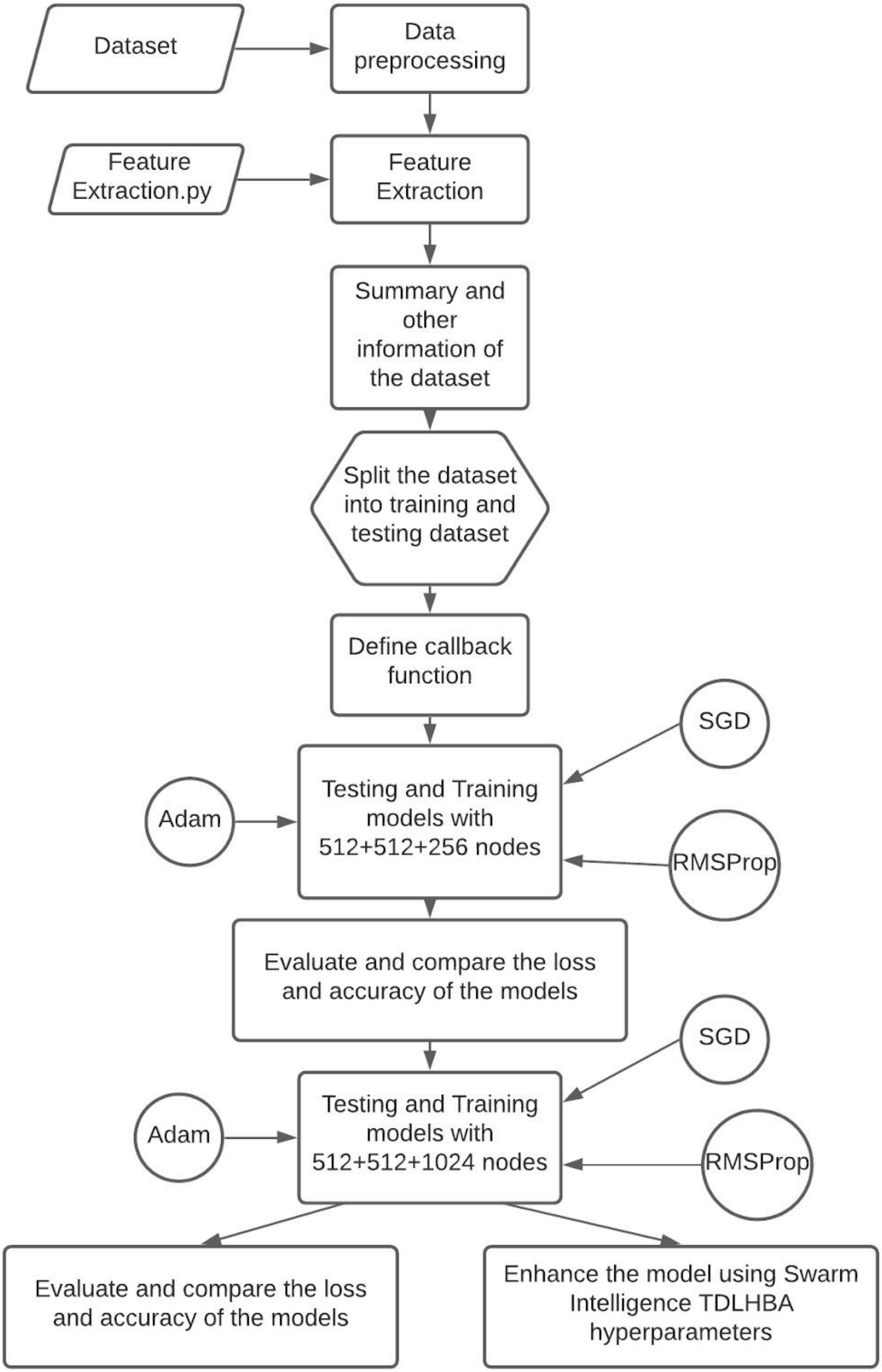
This method can now be applied to neural networks as well, using the Feed-Forward neural network, a component of the Recurrent Neural Network (RNN) that contains feedback connections from neurons in subsequent layers to neutrons in preceding layers. This implies that the output of such a neural network is also dependent on the network's state in the previous training iteration. The proposed method here is a modified bat algorithm named TDLHBA, which is an optimizer for finding the optimal neural network parameter settings.

For the purposes of the experiment, we define a feed-forward NN with two fully connected hidden layers and a single neuron in the output layer. The first layer has 40 neurons and the second layer has 30. The activation function ReLu is used by both hidden layers, while sigmoid is used by the output layer. Finally, based on the preceding research, Adam as the optimizer function.

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 have their own set of drawbacks. The approach I propose is based on the research presented thus far:

1. Preprocess the data to remove any unnecessary data, such as null values.
2. Use feature extraction based on phishing URL research to convert English content to numerical data that the computer can understand.
3. Determine the dataset's general information, such as the summary and the number of safe and unsafe rows.
4. Divide the newly created numerical dataset into two distinct sets: training and testing.
5. Create a callback function to monitor loss and adjust learning rates as needed, as well as to stop the model once it reaches a certain average accuracy rate.
6. Train and test a variety of models for various optimizers, including Adam, RMSProp, and SGD, each with three hidden layers, two with 512 nodes and one with 256 nodes and Sigmoid activation function.
7. Evaluate the model to determine the loss and accuracy of the prepared model for each optimizer and compare them.
8. Retrain and test with the same optimizers, but this time the first two hidden layers have only 512 nodes while the last hidden node has 1024 nodes and Sigmoid activation function. The loss function is "binary cross-entropy" in both cases because it is ideal for binary classification.
9. Compare and evaluate the results generated by both models for the specific optimizers.
10. Finally, use Swarm Intelligence/TDLHBA to improve the outcome.


Dataset
Data preprocessing
Feature Extraction.py
Feature Extraction
Summary and other information of the dataset
Split the dataset into training and testing dataset
Define callback function
SGD
Adam
Testing and Training models with 512+512+256 nodes
RMSProp
Evaluate and compare the loss and accuracy of the models
SGD
Adam
Testing and Training models with 512+512+1024 nodes
RMSProp
Evaluate and compare the loss and accuracy of the models
Enhance the model using Swarm Intelligence TDLHBA hyperparameters

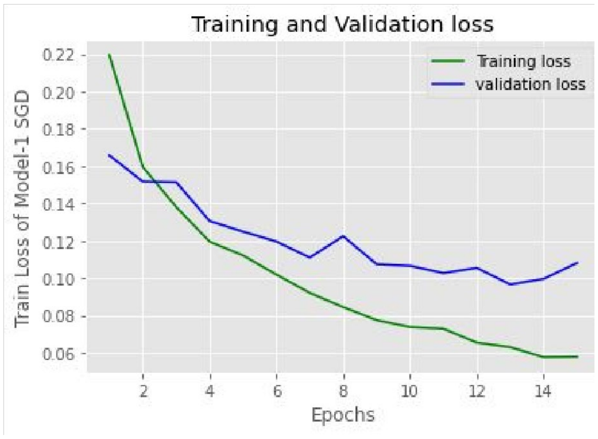
EXPERIMENTAL RESULTS

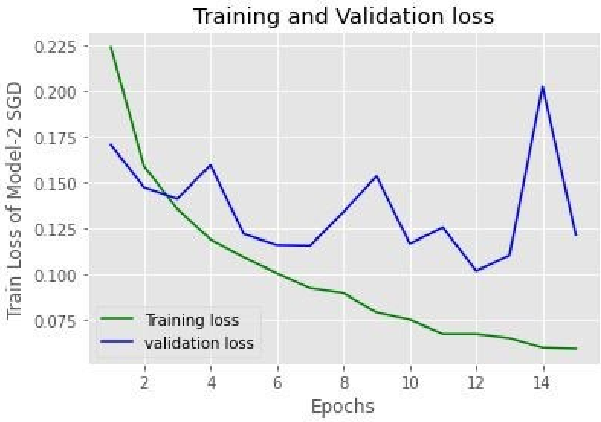
This section shows the comparison of experimental results between models, as well as the loss and accuracy of the same.

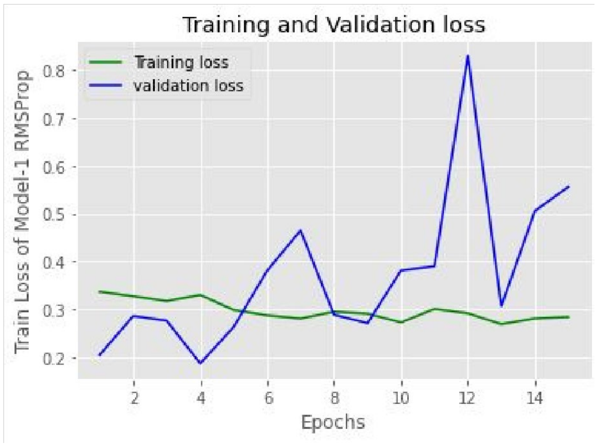
LOSS COMPARISON

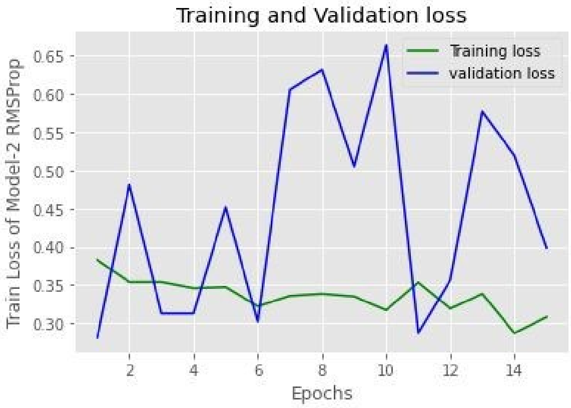
MODEL-1

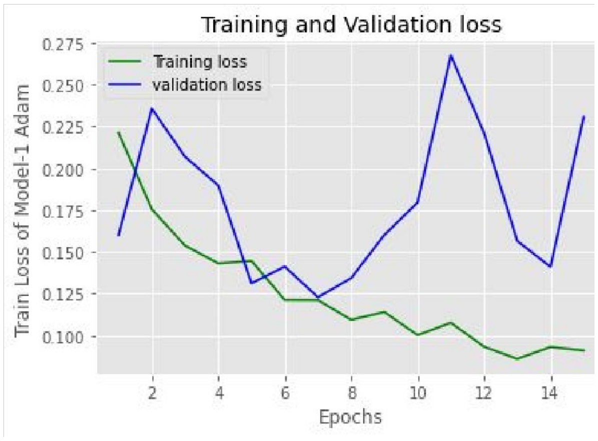
MODEL-2

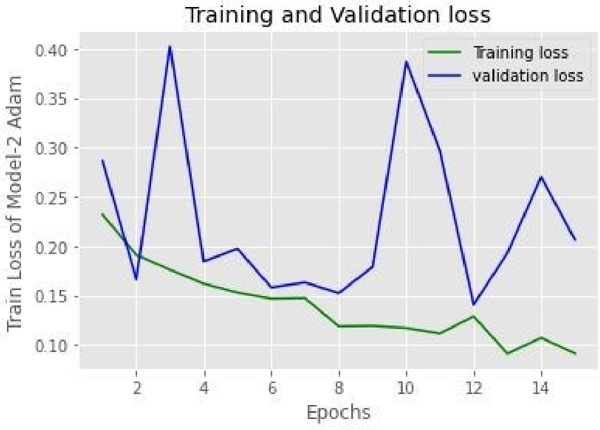










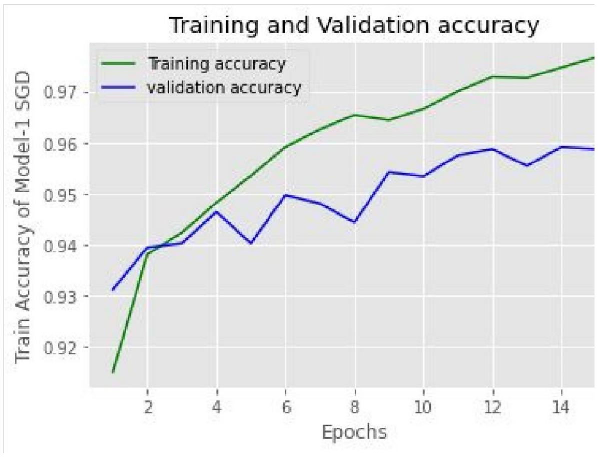


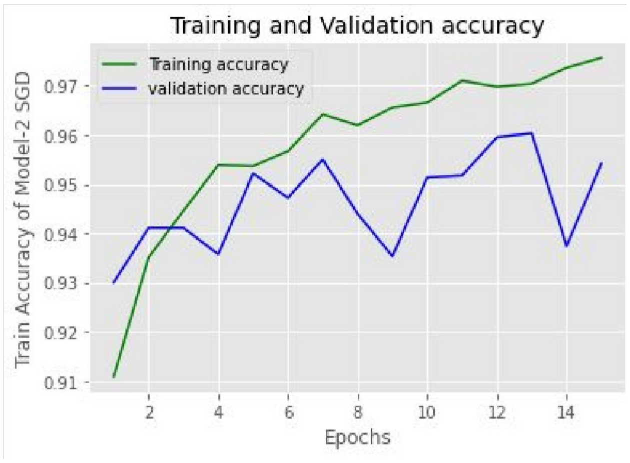
We can see from the graphs above where the loss occurred during model training and validation that the second model outperforms the first by a minuscule margin. The reason for this is that the number of nodes in the hidden layers has increased, implying that the algorithm learns and fits better. And, on average, Stochastic Gradient Descent (SGD) outperforms the other two optimizers.

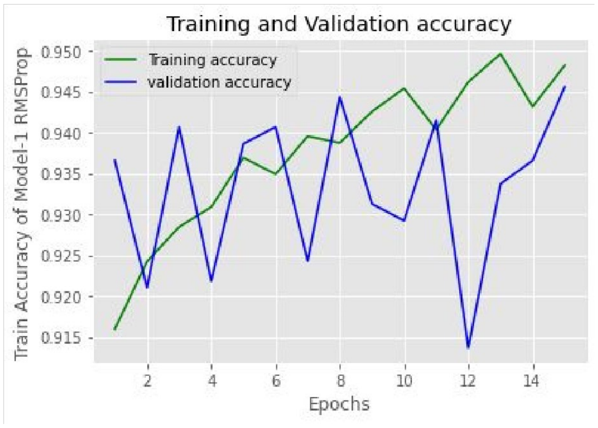
ACCURACY COMPARISON

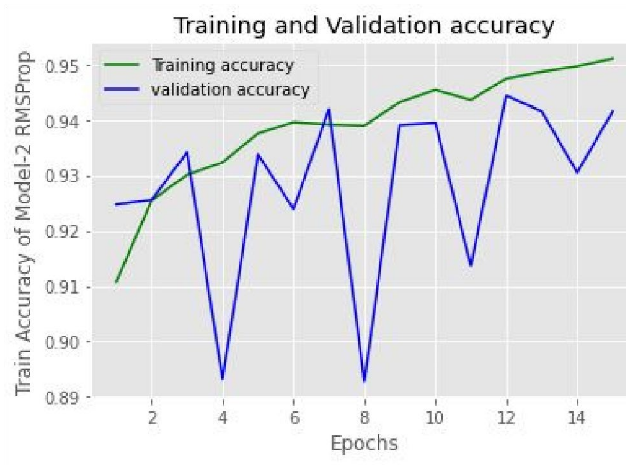
MODEL-1

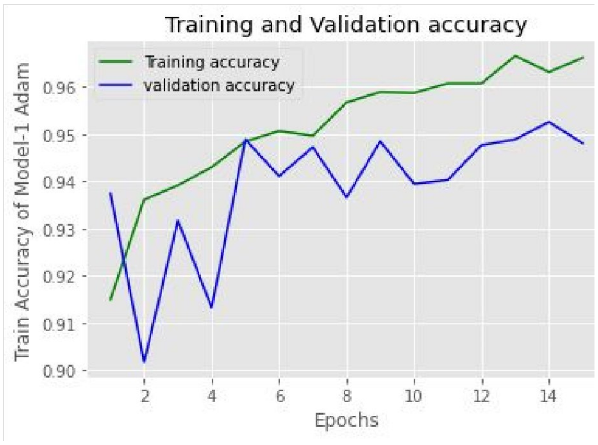
MODEL-2

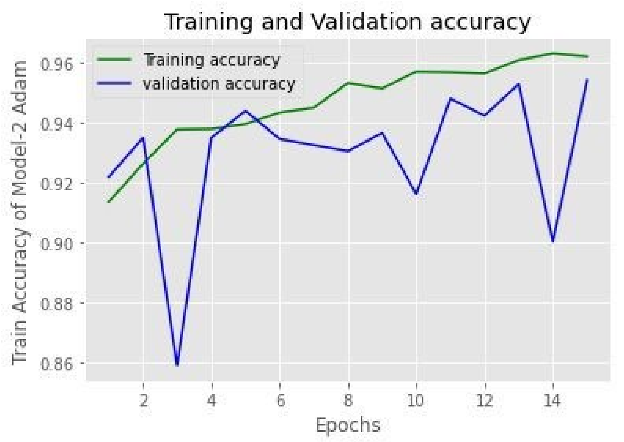




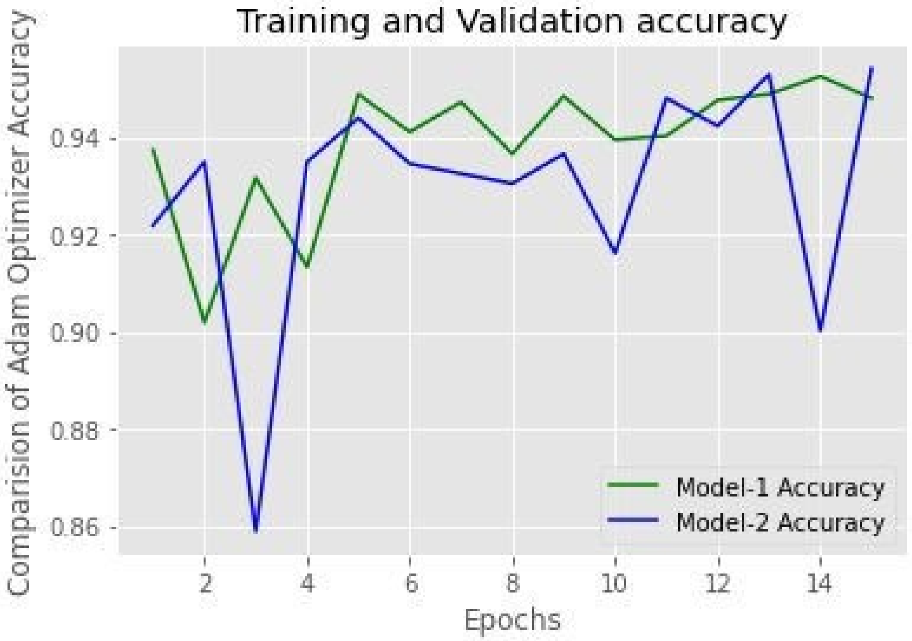


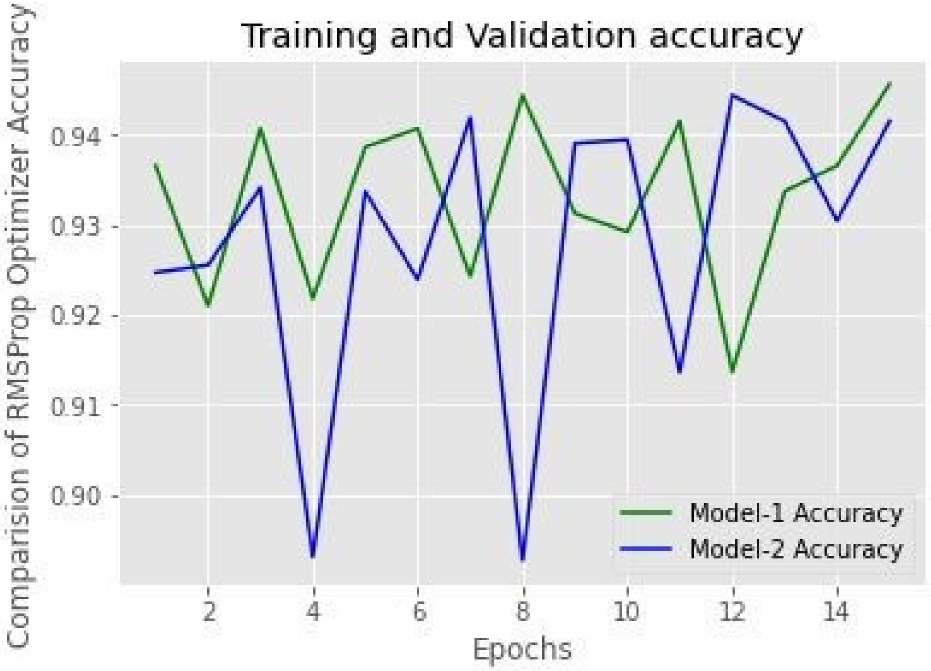


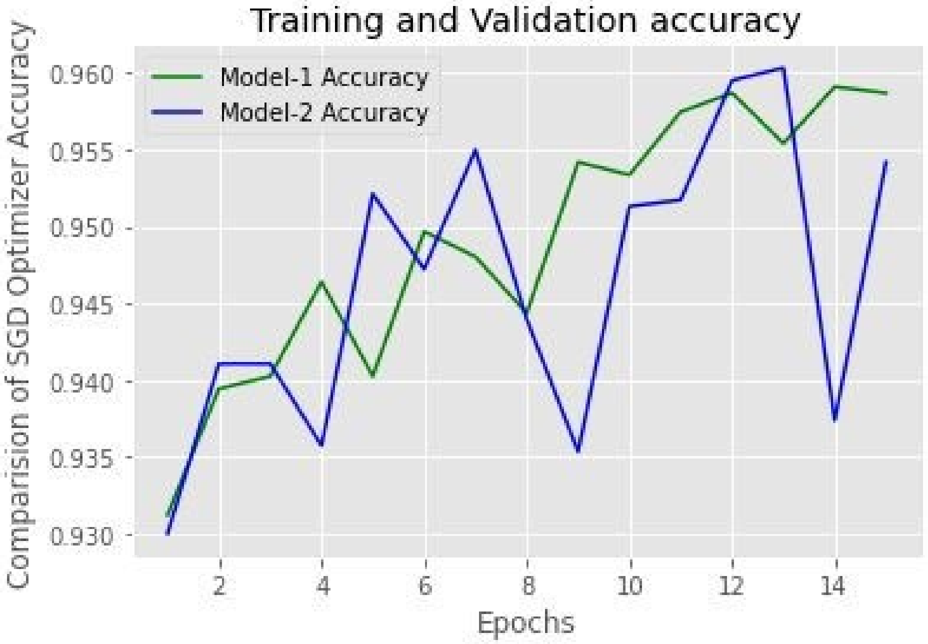




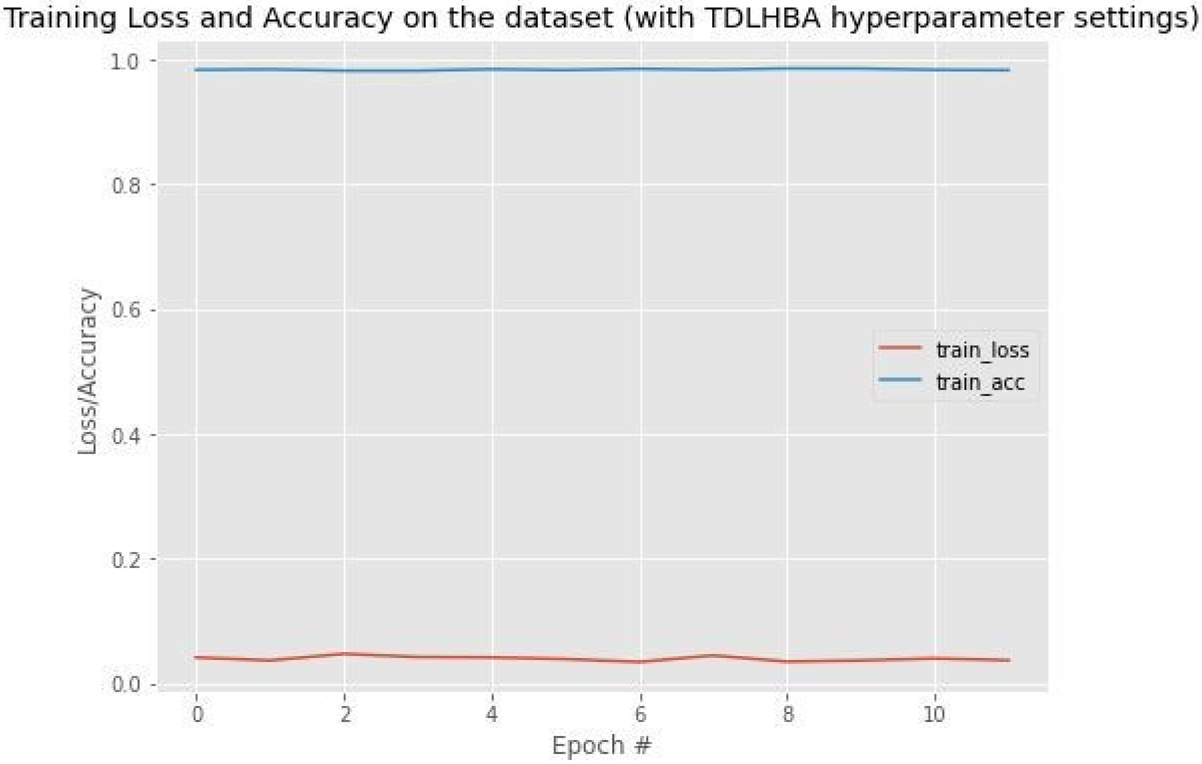
When we compare the accuracy in the above graphs, we see that there isn't much of a difference between the two models. However, Stochastic Gradient Descent (SGD) outperforms the other two in determining accuracy by a minuscule margin.







When we compare the accuracy of each optimizer in both models, we can see that, with the exception of the Adam optimizer, model-1 performed better, despite the fact that the second model had more nodes. Overfitting is the cause of this. As the number of nodes increased, so did the amount of noise and detail, as well as the size of the dataset.



Finally, the neural network with the TDLHBA technique is the result to be on the lookout for. It has an extremely high accuracy of 94.93% on average and a very low loss of less than 0.1%.

CONCLUSION AND FUTURE SCOPE

CONCLUSION

This study suggests a better framework for machine learning systems to address the growing phishing problem. To obtain conclusive and accurate average results, a model was developed and tested four times on Google Collaboratory. The GPU in Google Collaboratory provided a significant upgrade to the model when compared to the Jupyter Notebook running on RAM, which took approximately 60 seconds as opposed to the GPU in Collab, which took approximately 15 seconds, indicating a significant improvement and indicating the complexity of the algorithm. We can conclude from all of the experimental results that the "swarm intelligence approach" is superior to traditional neural network models in every way.

FUTURE SCOPE

As I write this report, attackers are coming up with new ways to defraud people on the Internet and finding new holes in the system. As a result, feature selection will need to be constantly improved and updated as attackers upgrade themselves. Another future goal is to develop an endpoint API that can be used as a plugin or a web application to allow users to interact with and use this phishing detection algorithm.

REFERENCES

1. Kumar, A. P. (2018). Phishing: Challenges and solutions
2. Higbi, J., Bellani, A., & Greaux, F. (2013). Collaborative phishing attack detection. U.S. Patent No. 8,386,958
3. Kiruthiga, K., & Akila, R. (2019). Phishing websites detection using machine learning. International Journal of Research in Technology and Engineering, 8(2S11), 41-49

4. Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. Hindawi Journal of Computer Engineering, 2014, 1-9

5. Fister, I., & Podgorelec, V. (2018, June). Swarm intelligence approaches for parameter setting of deep learning neural network: Case study on phishing websites classification. In The 2018 International Conference on Web Intelligence, Mining and Semantics (pp. 300-307). IEEE
6. Wang, Y., Zhang, S., & Luo, J. (2019). PDRCNN: Precise phishing detection with recurrent convolutional neural networks. Hindawi Wireless Communications and Mobile Computing, 2019, 1-11
7. Patil, M. S., Shetye, S. V., & Shendage, V. P. (2020). Detecting phishing websites using machine learning. International Research Journal of Engineering and Technology (IRJET), 7(2), 775-781
8. Ganesh, J. (2018). DeepAnti-PhishNet: Applying Deep Neural Networks for Phishing Email Detection. In International Workshop on Security in Privacy Preserving Ad Hoc and Wireless Networks (pp. 104-110). Springer, Cham

9. Csirtg (2018). Phishing predictions with deep learning and TensorFlow
10. Akamai (2018). A new era in phishing: Games, social, and prizes
11. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. MDPI Future Internet, 11(4), 76
12. Schuetzler, B. R. (2011). Trends in phishing attacks: Suggestion for future research. University of Nebraska-Lincoln
13. Chauhan, P., Kumar, P., Jyot, & Jain, M. (2020). Phishing attack. International Journal of Future Generation Communication and Networking, 13(4), 620-628
14. Das, R., Kim, C., Tingle, D., & Nippert-Eng, C. (2020). All about phishing: Exploring user research through a systematic literature review. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1-30
15. Damodaram, T. (2016). Study on phishing attacks and antiphishing tools. International Research Journal of Engineering and Technology (IRJET), 3(1), 165-171
16. Gupta, B. B., Arachchige, P. S., & Psannis, K. E. (2019). Defending against phishing attacks: Taxonomy of methods, current issues, and future directions. IEEE Communications Surveys & Tutorials, 21(4), 3664-3690
17. Kumar Jain, A., & Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity-based approaches. Hindawi Security and Privacy, 2017, 1-13
18. Shankar, K. S., Shetty, A. K., & Nath, K. (2019). A review on phishing attacks. International Journal of Advanced Engineering Research, 14(9), 172-180