Phishing Attacks and Related Techniques: A Survey

M.Sahaya Pretha[1*], Dr.V.Subha[2]
Research Scholar[1*], Assistant Professor[2]
Department of Computer Science and Engineering[1, 2]
Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu.[1, 2]
preethajames9211@gmail.com[1*], subha_velappan@msuniv.ac.in[2]

***Abstract** - Phishing is a kind of cyber attack in which perpetrators use spoofed emails and fraudulent websites to lure unsuspecting online users into giving up personal information. Phishing is a fraudulent trick of stealing victim's personal information by sending messages through SMS, e-mails and social networks via socially engineered messages. Over the past decades, online identity fraud has transformed from being a small scale attack to huge spread syndicated crime as identified in e-mails. Phishing is a cybercrime in which an object is somebody acting like a legitimate organization to bait people into giving delicate information. Phishing is the attempt to get sensitive information such as usernames, passwords, and credit card details, often for malicious reasons. In this survey, we examined phishing attacks and techniques.*

Index terms: Phishing, cybercrime, Uniform Resource Locator, websites, data

I. INTRODUCTION

Cybercrimes can be defined as Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim directly or indirectly, using modern telecommunication networks such as the Internet. Cyber Security refers to a set of techniques used to protect the programs and data from attack. Some examples of cyber crimes include spam, cyber terrorism, fraud, and phishing. A phishing attack is an assortment of a social Engineering. Phishing attacks utilize email, malicious sites or telecall to request individual data by acting as a legitimate site. It may likewise seem to originate from different kinds of links. Phishing can be implemented in different ways such as follows,

- Email-to-email: When someone receives an email requesting sensitive information to be sent to the sender.
- Email-to-website: When someone receives an email embedded with phishing web address.
- Website-to-website: When someone clicks on the phishing website through a search engine or an online advert.
- Browser-to-website: When someone misspelled a legitimate web address on a browser and then referred to a phishing website that has a semantic similarity to the legitimate web address [1].

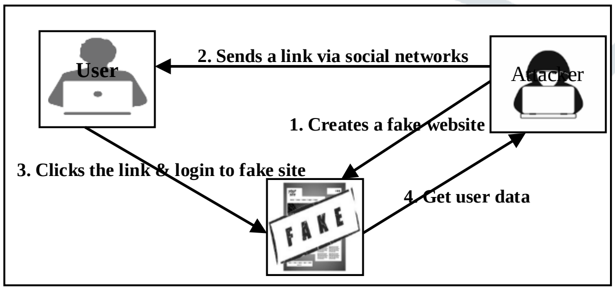
User
2. Sends a link via social networks
Attacker
1. Creates a fake website
3. Clicks the link & login to fake site
4. Get user data
FAKE

Fig 1- Phishing Life Cycle

In the Phishing Life Cycle describes, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

This paper is organized as follows: this section has an introduction. Section II describes the Background and Overview of Phishing attacks. Section III describes the literature on phishing detection techniques. Section IV concludes all the research directions.

II. BACKGROUND AND OVERVIEW OF PHISHING ATTACKS

HP group people have found out a problem and delivered at 1987. It was made the first moves to conduct attacks due to hackers used to communicate with one another via patented software as warez community [2].

According to Internet records, the first time that the term "phishing" was used and recorded was on January 2, 1996. Phishers turned their attention to online payment systems. Although the first attack, which was on E-Gold in June 2001, was not considered to be successful, it planted an important seed. In later 2003, phishers registered dozens of domains that looked like legitimate sites like eBay and PayPal. By the beginning of 2004, phishers were riding a huge wave of success that included attacks on banking sites and their customers. Popup windows were used to acquire sensitive information from victims. Since that time, many other sophisticated methods have been developed. In Table 1 distinguish between traditional and cyber crime techniques.

Table 1: Phishing behind the cybercrime

Traditional Crime techniques	Cyber crime techniques
Burglary: Breaking into a building with the intent to steal.	Hacking: Computer or network Intrusion providing unauthorized access.

Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity Information	Phishing: A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.
Extortion: Illegal use of force or one's official position or powers to obtain property, funds.	Internet extortion: Hacking into and controlling various Industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.
Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.	Internet fraud: A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.
Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.	Identity theft: The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.
Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse	Child exploitation: Using computers and networks to facilitate the criminal victimization of minors.

The above table converse about (GAO) computer interconnectivity has produced enormous benefits but has also enabled criminal activity that exploits this interconnectivity for financial gain and other malicious purposes, such as Internet fraud, child exploitation, identity theft, and terrorism. Cybercrime include activities associated with protecting networks and information, detecting criminal activity, investigating crime, and prosecuting criminals.

Characteristics of Phishing attacks

- Unusual Urgency
- Poor Design
- Misspellings
- Pop-Up Windows
- Request for submitting personal information
- Generic salutation
- Attachments
- Phony links – the links might show something else but will actually direct to a different location. Phishing emails use various methods to hide the actual URLs.
- Bad grammar and spelling. Phishing websites might look exactly like the original ones, but their URL might be slightly or completely different. Hence, make sure that the URL is the correct one when you visit a website.
- Also, legitimate websites use SSL for protecting your information when entering your data. Make sure that the URL starts with *https://* instead of HTTP:// for pages where you have to submit username/password or other private information.

There are a number of different techniques used to obtain personal information from users. As the cybercrime techniques being used are also more advanced.

2.1 Spear Phishing

While traditional phishing uses a 'spray and prays' approach, by means of mass emails are sent to as many people as possible, spear phishing is a much more targeted attack in which the hacker knows which specific individual or organization they are after.

2.2 Email/Spam

This is the most common phishing technique, the identical emails are sent to millions of users with a request to fill in personal details. These details will be used by the phishers for their illegal activities. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change address details, or verify accounts.

2.3 Web-Based Delivery

Web-based delivery is one of the most sophisticated phishing techniques. Also known as "man-in-the-middle," the hacker is located in between the original website and the phishing website. The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.

2.4 Link Manipulation

Link manipulation is the technique in which the phisher sends a link to a malicious website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link.

2.5 Keyloggers

Keyloggers refer to the malware used to identify inputs from the keyboard. The information is sent to the hackers who will interpret passwords and other types of information. To prevent keyloggers from accessing personal information, secure websites provide options to use mouse clicks to make entries through the virtual keyboard.

2.6 Trojan

A Trojan horse is a type of malware designed to mislead the user with an action that looks legitimate but actually allows unauthorized access to the user account to collect credentials through the local machine. The acquired information is then transmitted to cybercriminals.

2.7 Malvertising

Mal+vertising malicious advertising that contains active scripts designed to download malware or force unwanted content onto your computer. Exploits in Adobe PDF and Flash are the most common methods used in advertisements.

2.8 Session Hijacking

The phisher exploits the web session control mechanism to steal information from the user. In a simple session hacking procedure known as session sniffing, the phisher can use a sniffer to interrupt relevant information so that the man can access the Web server illegally.

2.9 Content Injection

Content injection is the technique where the phisher changes a part of the content on the page of a reliable website. This is done to mislead the user to go a page outside the legitimate website where the user is then asked to enter personal information.

2.10 Phishing through Search Engines

Some phishing scams involve search engines where the user is directed to product sites which may offer low-cost products or services. When the user tries to buy the product by entering the credit card details, it's collected by the phishing site.

2.11 Vishing (Voice Phishing)

In phone phishing, the phisher makes phone calls to the user and asks to dial a number. The purpose is to get personal information of the bank account through the phone. Phone phishing is mostly done with a fake caller ID.

2.12 Smishing (SMS Phishing)

Phishing conducted via Short Message Service (SMS), a telephone-based text messaging service. A smishing text, for example, attempts to attract a victim into revealing personal information via a link that leads to a phishing website.

2.13 Malware

The malware is usually attached to the email sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to downloadable files.

2.14 Ransomware

Ransomware denies access to a device or files until a payment has been paid. Ransomware for PC's is malware that gets installed on a user's workstation using a social engineering attack where the user gets tricked into clicking on a link, opening an attachment, or clicking on Malvertising [3].

III. LITERATURE SURVEY

Currently, various type of research going on the detection of phishing websites. This survey will compare a numeral of detection techniques.

3.1 Taxonomy of Phishing detection schemes

There are 6 related techniques majorly used in phishing detection. Which are classified as a search engine based (SEB), heuristics and machine learning based (HMLB), phishing blacklist and whitelist based (PBWB), visual similarity based (VSB), DNS based (DNSB), and proactive phishing URL detection-based (PPUDB) schemes.

1. *Search engine based*

These techniques extract the features such as text, images, and URLs from websites, then search for them using single or multiple search engines and collect the findings. The legitimate websites typically have a higher index than the phishing website, which remains active for a very short time.

2. *Heuristics and machine learning based*

These techniques extract a set of features like text, image, or URL- specific information from legitimate and phishing websites. A set of heuristics is utilized, and the rules obtained from the learning algorithms. Those are used for Phishing detection.

3. *Phishing blacklist and whitelist based*

The methods in this category utilize the whitelist of legitimate websites and the blacklist containing Phishing websites. The main one is blacklist, is obtained either by user feedback or via reporting by the third parties.

4. *Visual similarity based*

This technique utilizes the visual similarity between legitimate pages Vs phishing pages. When phishing websites are matched in terms of their visual characteristics with the legitimate websites, it checks whether the URL is on the legitimate domain URL list. If not, the website is marked as a phishing website.

5. *DNS based*

DNS is used to validate the IP address of a phishing website. For example, DNS will identify whether the IP address is running on the list of legitimate website IPs. If it is not, the website is marked as phishing. DNS can also be utilized by these techniques in other ways, based on the needs of the user.

6. *Proactive phishing URL detection based*

This scheme detects probable phishing URLs by generating different combinatorial URLs from existing legitimate URLs. Whether they stay alive and are involved in phishing related activities on the web [4].

Sujata Garera et al. focused on the structure of URLs engaged in various phishing attacks. URL belongs to a phishing attack without requiring any knowledge of the corresponding page data. The several features that can be used to distinguish a phishing URL from a legitimate websites. These features are used to generate a model using logistic regression technique that is efficient and high accuracy [5].

Maher Aburrous et al. proposed a model is based on Fuzzy Logic operators which are used to characterize the phishing website factors, indicators, variables, measures and size with a layer structure. Experimental results showed the significance and importance of the phishing website criteria. URL & Domain Identity represented by layers and the final phishing website rate is assigned by weight of variable on phishing layers [6].

Shreeram et al. acknowledged a rule that can be explained as an IP address of the URL in e-mail and it does not match the defined Rule Set for White List then the received mail is a phishing mail. It provides the feature of malicious status notification before the user reads the mail. A genetic algorithm is proposed, this algorithm is used to develop rules that are used to differentiate phishing link from a legitimate link. The parameters like evaluation function, crossover and mutation [7].

Islam et al. suggested the Decision Tree (DT) algorithm is a simple algorithm that is based on a set of rules which is advantageous owing to the sequential structure of the decision tree branches. The significant conditions and actions are inter-linked directly, supplementary conditions and actions if needed. However, insignificant conditions and actions are ignored. The boosting method constructs a highly accurate classification rule by combining various simple and moderately accurate hypotheses [8].

Likarish et al. used TF-IDF which uses unique keywords to identify a specific page. This technique is often used in search engines to find relevant pages. This algorithm is used to identify the website and keywords. Those keywords are sent to a search engine such as Google and the top URLs are identified. If the site is located in the top search results then the site is considered legitimate. Otherwise, the site is labeled as phishing because most likely the phishing site will not have a high ranking on the search engine results [9].

Jeeva et al. focused on the significant features that discriminate between legitimate and phishing URLs. These features are subjected to associative rule mining and developed one model using apriori and predictive apriori. The rules obtained the features that are more prevalent in phishing URLs. The results obtained from rule mining features in the phished URLs set. The model to produce high accuracy and classified whether the website is legitimate or phishing based on features [10].

Jain et al. Developed Phishing Detection Algorithm to protecting against phishing attacks at the client side and is to perform fast access time and high detection rate using auto-updated white-list [11].

Mustafa Gaytan et al. used ELM method to provide good generalization performance in phishing detection procedure faster than other techniques [12].

Waleed Ali et al. recommended BPNN, RBFN, SVM, NB, C4.5, kNN and RF used to find phishing websites via wrapper-based features selection methods PCA and IG. Those combining feature selection with classification techniques are produce high classification accuracy [13].

Andrew j park et al. developed an authoritative extension for web browsers. The extension embedded by Phishing-Detective framework model. It detects phishing websites in real-time while users browse web. If any phishing site will be detected, then that site will be blocked before receiving an alert [14].

Ramana et al. suggested DT, RF, NB, IBK are used to identify the phishing URLs. The best two techniques are fused by generating a hybrid model based on the classification results. The hybrid model is detect phishing websites absolutely and produce high accuracy and less error rate [15].

3.3 Phishing Features

Phishing websites are identified based on several features from the URL [16]. The features are given in Table 2

Table 2-Phishing Features

Sl.No	Attribute	Rules	Values
1.	having_IP_Address	*Rule*: IF$\begin{cases}\text{If The Domain Part has an IP Address} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
2.	URL_Length	*Rule:* IF$\begin{cases} URL\ length < 54 \rightarrow feature = \text{Legitimate} \\ else\ if\ URL\ length \geq 54\ and\ \leq 75 \rightarrow feature = Suspicious \\ otherwise \rightarrow feature = \text{Phishing}\end{cases}$	{ 1,0,-1 }
3.	Shortining_Service	*Rule*: IF$\begin{cases}\text{TinyURL} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
4.	having_@_Symbol	Rule: IF $\begin{cases}\text{Url Having @ Symbol} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
5.	double_slash_redirecting	Rule: IF $\begin{cases}\text{the position of the Last Occurrence of "//" in the URL} > 7 \rightarrow Phishing \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
6.	Prefix_Suffix	Rule: IF $\begin{cases}\text{Domain Name Part Includes } (-) \text{ Symbol} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ -1,0,1 }
7.	having_Sub_Domain	Rule: IF $\begin{cases}\text{Dots In Domain Part} = 1 \rightarrow \text{Legitimate} \\ \text{Dots In Domain Part} = 2 \rightarrow \text{Suspicious} \\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ -1,0,1 }
8.	SSL_final_State	Rule: IF $\begin{cases}\text{Use https and Issuer Is Trusted } and\ Age\ of\ Certificate \geq 1 \text{ Years} \rightarrow \text{Legitimate} \\ \text{Using https and Issuer Is Not Trusted} \rightarrow \text{Suspicious} \\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ -1,1,0 }
9.	Domain_registeration_length	Rule: IF$\begin{cases}\text{Domains Expire on} \leq 1 \text{ years} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1,-1 }
10.	Favicon	Rule: IF$\begin{cases}\text{Favicon Loaded From External Domain} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
11.	port	Rule: IF$\begin{cases}\text{Port \# is of the Preferred Status} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
12.	HTTPS_token	Rule: IF$\begin{cases}\text{Using HTTP Token in Domain Part of The URL} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
13.	Request_URL	Rule: IF $\begin{cases}\text{\% of Request URL} < 22\% \rightarrow Legitimate \\ \text{\%of Request URL} \geq 22\% \text{ and } 61\% \rightarrow \text{Suspicious} \\ \text{Otherwise} \rightarrow \text{feature} = \text{Phishing}\end{cases}$	{ 1,-1 }
14.	URL_of_Anchor	*Rule*: IF$\begin{cases}\text{\% of URL Of Anchor} < 31\% \rightarrow Legitimate \\ \text{\% of URL Of Anchor} \geq 31\% \text{ And} \leq 67\% \rightarrow \text{Suspicious} \\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ -1,0,1 }
15.	Links_in_tags	Rule: IF$\begin{cases}\text{\% of Links in "} < Meta > \text{","} < Script > \text{" } and \text{ "} < \text{Link>"} < 17\% \\ \rightarrow Legitimate \\ \text{\% of Links in } < Meta >, < Script > \text{ and } < \text{Link>"} \geq 17\% \text{ And} \leq 81\% \\ \rightarrow \text{Suspicious} \\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ 1,-1,0 }
16.	SFH	Rule: IF$\begin{cases}\text{SFH is "about blank" Or Is Empty} \rightarrow \text{Phishing} \\ \text{SFH Refers To A Different Domain} \rightarrow \text{Suspicious} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ -1,1 }
17.	Submitting_to_email	Rule: IF$\begin{cases}\text{Using "mail()" or "mailto:" Function to Submit User Information} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
18.	Abnormal_URL	Rule: IF $\begin{cases}\text{The Host Name Is Not Included In URL} \rightarrow \text{Phishing} \\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
19.	Redirect	Rule: IF $\begin{cases}\text{ofRedirect Page} \leq 1 \rightarrow \text{Legitimate} \\ \text{of Redirect Page} \geq 2\ And < 4 \rightarrow Suspicious \\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ 0,1 }

20.	on_mouseover	Rule: IF$\begin{cases}\text{onMouseOver Changes Status Bar} \rightarrow \text{Phishing}\\ \text{It Does't Change Status Bar} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
21.	RightClick	Rule: IF$\begin{cases}\text{Right Click Disabled} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
22.	popUpWidnow	Rule: IF $\begin{cases}\text{Popup Window Contains Text Fields} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
23.	Iframe	Rule: IF $\begin{cases}\text{Using iframe} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 0,1 }
24.	age_of_domain	Rule: IF $\begin{cases}\text{Age of Domain} \geq 6 \text{ months} \rightarrow \text{Legitimate}\\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ -1,0,1 }
25.	DNSRecord	Rule: IF$\begin{cases}\text{no DNS Record For The Domain} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
26.	web_traffic	Rule: IF$\begin{cases}\text{Website Rank} < 100{,}000 \rightarrow \text{Legitimate}\\ \text{Website Rank} > 100{,}000 \rightarrow \mathit{Suspicious}\\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ -1,0,1 }
27.	Page_Rank	Rule: IF$\begin{cases}\text{PageRank} < 0.2 \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ -1,0,1 }
28.	Google_Index	Rule: IF$\begin{cases}\text{Webpage Indexed by Google} \rightarrow \text{Legitimate}\\ \text{Otherwise} \rightarrow \text{Phishing}\end{cases}$	{ 0,1 }
29.	Links_pointing_to_page	Rule: IF $\begin{cases}\text{Of Link Pointing to The Webpage} = 0 \rightarrow \text{Phishing}\\ \text{Of Link Pointing to The Web page} > 0 \text{ and} \leq 2 \rightarrow \mathit{Suspici}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0,-1 }
30.	Statistical_report	Rule: IF$\begin{cases}\text{Host Belongs to Top Phishing IPs or Top Phishing Domains} \rightarrow \text{Phishing}\\ \text{Otherwise} \rightarrow \text{Legitimate}\end{cases}$	{ 1,0 }
31.	Result	1- Phishing, -1 – Legitimate	{ 1,-1 }

3.4 APWG Report

In Anti Phishing Work Group several reports related to the phishing environment have been taken from the year 2005 to 2017. All the phishing data collected are given in the following table 3. Today, phishing has reached epidemic levels as, according to statistics published by APWG[17].

Table 3-APWG report from 2005 to 2017

Total number of unique phishing reports (campaigns) received, according to APWG[43]													
Year	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**	**Total**
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244	173063
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787	268126
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683	327814
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187	335965
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897	412392
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020	313517
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979	284445
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195	320081
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489	491399
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765	704178
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421	194499	105233	80548	1413978
2016	99384	229315	229265	121028	96490	98006	93160	66166	69925	89232	118928	69533	1380432
2017	96,148	100,932	121,860	87,453	93,285	92,657	99,024	99,172	98,012	61322	86,547	85,744	1122156

IV. CONCLUSION

Phishing originated sometime around the year 1995. These type of fraudulent activities were not commonly known by everyday people until nearly ten years later. It has been approximately 30 years since the phishing problem was acknowledged. But, still, it is used to steal personal information, online documentation and credit card details. There are diverse solutions offered, but whenever a result is proposed to overcome these attacks, phishers come up with the vulnerabilities of that solution to maintain with such an attack.

REFERENCES

[1]. http://www.phishing.org

[2]. Felix, Jerry and Hauck, Chris (September 1987). "System Security: A Hacker's Perspective". 1987 Interex Proceedings 1: 6.

[3]. http://www.thewindowsclub.com

[4]. Gaurav Varshney et al. "A survey and classification of web phishing detection schemes" SECURITY AND COMMUNICATION NETWORKS, Vol-9 Pages-6266–6284, 2016

[5]. Sujata Garera, Niels Provos, Monica Chew, Aviel D. Rubin "A Framework for Detection and Measurement of Phishing Attacks" ACM WORM'07, November 2, 2007.

[6]. Maher Aburrous et al. Intelligent Phishing Website Detection System using Fuzzy Techniques, Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008.

[7]. V.Shreeram, M.Suban, P.Shanthi, K.Manjula, "Anti-phishing detection of phishing attacks using Genetic Algorithm" 978-1-4244-7770-8/10/ ©2010 IEEE.

[8]. Islam, Md Rafiqul & Xiang, Yang. (2010). Email classification using data reduction method. 1 - 5. 10.4108/chinacom.2010.59.

[9]. Likarish, P., Jung, E., Dunbar, D., Hansen T., and Hourcade, J.P. B-APT: Bayesian Anti-Phishing Toolbar. In Communications, 2008. ICC '08. IEEE international conference on Communications, pages 1745-1749, 2008.

[10]. S. Carolin Jeeva1 and Elijah Blessing Rajsingh, Intelligent phishing URL detection using association rule mining, Hum. Cent. Comput. Inf. Sci. (2016) 6:10

[11]. Jain and Gupta, A novel approach to protect against phishing attacks at client side using auto-updated white-list, EURASIP Journal on Information Security (2016), Springer Publisher

[12]. Effective Classification of phishing web pages based on New rules by using Extreme learning machines, Anatolian Journal of Computer Sciences (2017)

[13]. Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection, International Journal of Advanced Computer Science and Applications (2017)

[14]. Phishing Website Detection Framework Through Web Scraping and Data Mining, IEEE 2017

[15]. Detection of Phishing Websites Using Hybrid Model, Journal of advancement in Engineering and technology (2018).

[16]. Rami M. Mohammad "Phishing Websites Features" 2015.

[17]. "APWG Phishing Attack Trends Reports". Retrieved October 17, 2017.