International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Effective Measures to Overcome the Fraudulent Phishing

Neha R[1], Sai Sree Reena Reddy L[2], Dr. Gururaj H L[3], Prof Goutham B[4]

[1]Neha R, Student, Vidyavardhaka College of Engineering, Karnataka, India
[2]Sai Sree Reena Reddy L, Student, Vidyavardhaka College of Engineering, Karnataka, India
[3]Dr. Gururaj H L, Prof of Vidyavardhaka college of Engineering, Vidyavardhaka college of Engineering, Karnataka, India
[4]Goutham.B, Prof of Vidyavardhaka college of Engineering, Vidyavardhaka college of Engineering, Karnataka, India

***

Abstract - Social media plays a vital role in an individual's everyday life. The various benefits that an individual can get by using social media apps or websites is enormous where they can keep in touch with their family and friends, make new friends, do online transactions, purchase products and most importantly to share their personal information. Everyday enormous amount of data is generated over these social media sites which can then be used by large companies to generate revenue or can be misused by the attackers to exploit vulnerabilities of these social network platforms. As the usage of these social media platforms are increasing, security threats have also been increasing side-by-side. One such attack is the Phishing attack, where the intention of the attacker is to forge a website to track and steal sensitive information about the victim. Here the attacker sends malicious links or illegal attachments through emails that can capture the victim's personal information such as login credentials, bank account details and many more. Since this kind of unlawful activities are increasing day-by-day, it is important for the victims to protect their data from being vulnerable to the attackers. Hence it is necessary to know about various detection and preventive techniques. This paper presents different types of phishing attacks, detection of phishing attacks and the prevention of the same.

***Key Words*: Phishing, Victim, Strategy, Hacking, Malware**

1. INTRODUCTION

In this modern era it has become a great practice of dealing with each and every information online. All official and unofficial conversations happens on different social media network such as whatsapp, Instagram, linkedIn, e-mails and many more. With the increased rate of usage of online platforms there is an equal balance between the advantages and disadvantages of them. Every minute data is very important and it should be secured as it costs a lot to the individual. Since these platforms is a hub for all the personal and professional data of every individual, the chances of such data being vulnerable for the attackers is very high and dangerous. Out there, is a number of hackers eagerly waiting to steal data in order for their benefits either in terms of money or some other personal grudge. In order to protect our data it is very important to have certain prevention methods. One such troublesome and most popular type of attack is the phishing attack. Most of the time it happens that the attacker sends the email with fake URLs which is almost similar to the original one and the user who is unaware of this will be the direct victim for the attack. In this attack when the user clicks on the URL, he is redirected to a fake 'Sign in' page which is legitimate but fake in nature. The fake page is almost similar to the original one with very few unnoticeable changes may be regarding the alphabets in a word or so. Most of the times, the intention of phishing is to obtain the personal details of the victim such as login credentials, bank account details, credit card details etc., In very few cases there are chances where the attacker sends the pdf attached to the email. Clicking on the pdf or downloading the same may become vulnerable for the victim information. This shows that behind a link or button there could be anything. A phishing scam is well disguised and plays on curiosity as depicted in Figure 1.

Fig 1: Example for a Phishing Scam

The rest of the chapter is structured as follows: Analysis of different Phishing Attacks are depicted in section 2

2. Analysis of Phishing Attacks

Phishing is a threat to all internet users. Phishing can be broadly divided into various categories and is shown in Figure 2.

Fig 2: Categories of Phishing Attacks

2.1 SPOOFING EMAIL

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. By seeing these kinds of mails the victim is forced to believe in the mail and share the important and personal information with the spammer either by clicking the URL's sent in the mail or in worst cases, just by opening the mail by clicking on it. The various entities can be spoofed as depicted in Figure 3.

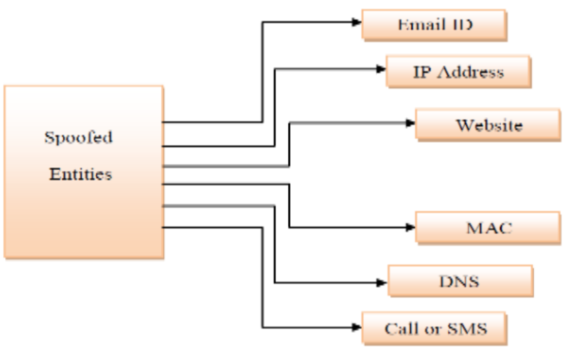

Fig 3: Spoofed entities

2.2 FAKE SOCIAL NETWORK ACCOUNTS

As we all know that social media has become a major and integral part of every individual in this modern era social network acts like an open door for the attackers to make use of innocents by their unethical skills. In this type of phishing we commonly come across the incidents where the attackers create fake accounts or profiles in popular social media platforms and establish a superficial trustworthy relationship with the victims who is not very much aware of the dark side of them. This innocent behavior of the victims pushes them to believe in the fake profiles and worst of all they also tend to share their personal information including financial matters. This type of phishing is mainly done by creating fake profiles by impersonating the celebrities in various fields such as movies, sports and famous business icons. The details of statistics with respect to year is depicted in Figure 4.

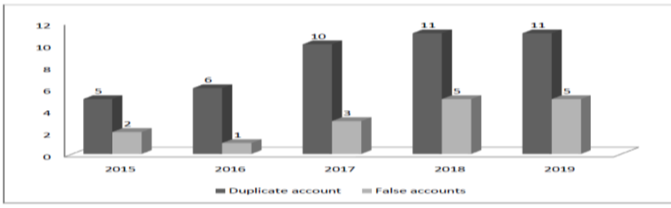

Fig 4: Statistics of Duplicate and False Accounts in Social Media

2.3 HACKING

Hacking is performed by the technically skilled attackers where they access the system resources by various methods in order to rob the data for profit or sometimes just for fun. They use different techniques for hacking such as:

2.3.1 DICTIONARY ATTACK:

As the name itself portraits the Dictionary attack is done by cracking the password of a protected computer in a systematic way by entering every word from a dictionary as the password.

2.3.2 BRUTEFORCE ATTACK:

Brute force attack is a type of hacking which is mainly based on trial and error method where the attacker checks the different combinations in order to find the victim's username and personal identification number. Usually an automated software is used to predict a large number of combinations as per the value of the desired data.

2.3.3 PASSWORD CRACKING:

Password cracking is a technique which is carried out by recovering different combinations of stored or transmitted passwords. Here the passwords are guessed usually through a computer algorithm where the algorithm tries a large number of combinations until the discovery of the correct password and is depicted in Figure 5.

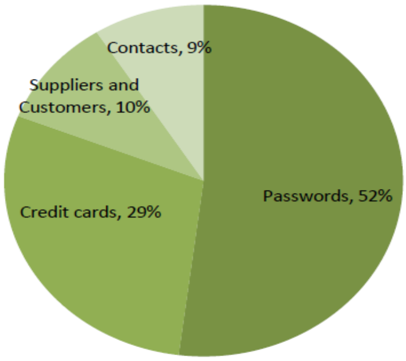

Fig 5: Percentage of hacking in different media

2.4 TROJAN HORSE

This type of phishing is mainly affected by the victims when they download files containing harmful executable programs which makes their system data vulnerable. In extreme cases the TROJAN can take over the complete control of the victim's system making it available to the hackers very easily. The types of different downloading platforms affected are depicted in Figure 6.

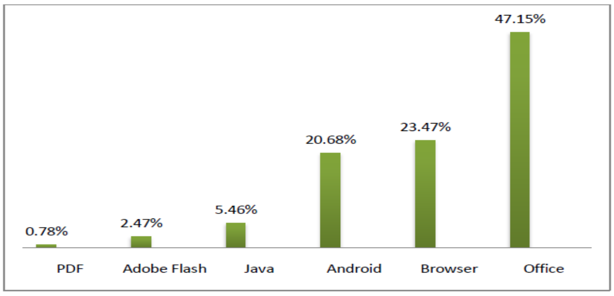

Fig 6: Percentage of attack on different downloading platforms

2.5 DECEPTIVE PHISHING

This is the most common type of phishing where the attackers send malicious URLs or emails usually from banks and ask the user to click on the link and verify their account.

2.6 SPEAR PHISHING

Spear phishing is mainly targeted to an individual or a particular organization or business firms where they send personalized emails in a more sophisticated way. In this case the attackers usually know considerable details of the victims such as name of the firm, location, type of the firm, jobs offered and also their personal email id's. Spear phishing is mainly concentrated to access the sensible information like account details and other credentials. The different firms of spear phishing statistics is depicted in Figure 7.

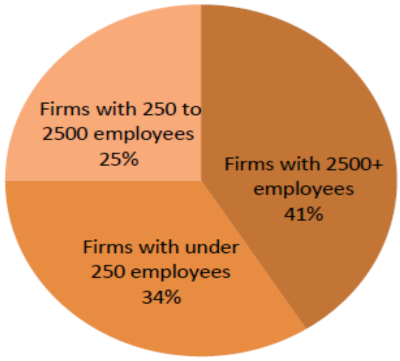

Fig 7: Percentage of spear phishing in different firms

2.7 WHALING

Whale being the largest sea animal gives a similar meaning to this type of phishing attack where the victims are usually high profile employees or seniors of the company. They are attacked in order to gain access and information about the companies as these people have access to almost all the sensitive data and information of the company. *Whaling email with a phone call:* In this case, the victim will be receiving a whaling email which is then followed with a phone call that confirms the requested email. This is also called cyber - enabled fraud .The phone call has a dual purpose of collaborating the email request and to make the victim think that he is in interaction with the real world.

Fig 8: Whaling email with a phone call

Whaling emails which appear to be from colleagues: This can happen when an employee's email address or any other spoofed email address is used to convince the victim in a way that the mail has come from a legitimate or from a trusted source. This method is very much effective when the email ID or address of the organization's senior most executive is spoofed and is sent to the organization's junior executives. The working of whaling is shown in Figure 8.

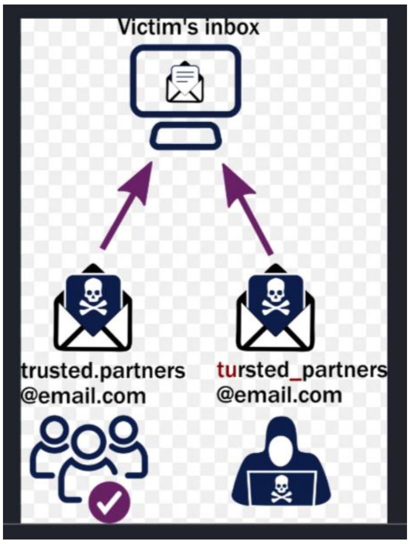

Fig 9: Whaling emails which appear to be from colleagues

2.8 ANGLER PHISHING

This is a newly transpired type of phishing where the attacker impersonates himself as a customer service agent on social media platforms and builds a healthy conversation with the unhappy customer and tries to obtain their personal information or account credentials. This type of attack is mainly concentrated on financial institutions as per the survey of 2017.

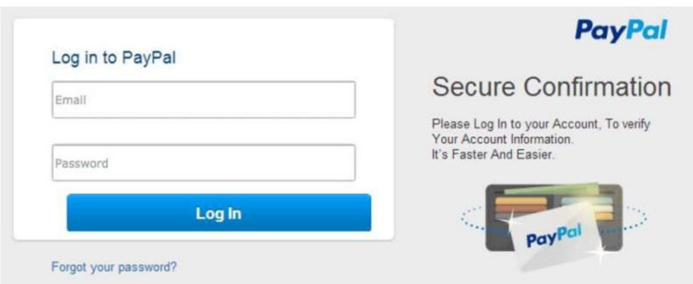

Fig 10: Fake Site with Stolen Branding, Which is Directed from the Angler Phishing Attack on the AskPayPal_Tech Account

2.9 CATPHISHING / CATFISHING

This is a type of romantic scam where the fraud falsify his identity most of the times on social media platforms or on online dating websites in order to have an emotional relationship which might lead to phony conversation, romantic relationships with at most trust on the victim side which inadvertently acts as a vulnerability to the victims personal information. Also, sometimes this attack may lead to financial loss.

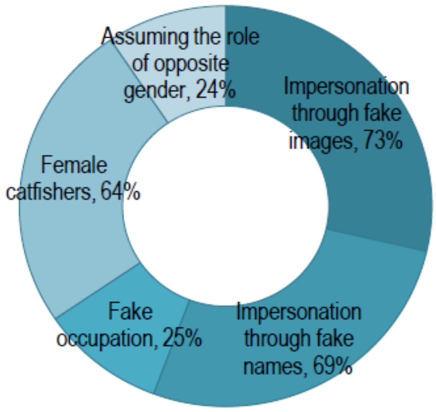

Fig 11: Percentage of catphishing by different means

2.10 CLONE PHISHING

Clone phishing is a type of spear phishing where the already sent and authorized emails containing an attachment or a link are cloned with almost the same content but a replaced or added malicious link or a fake website to it. When this type of email is sent, the users will usually not pay attention to the minute changes in the cloned email but trust it blindly and click on the link or the website and thus get trapped.

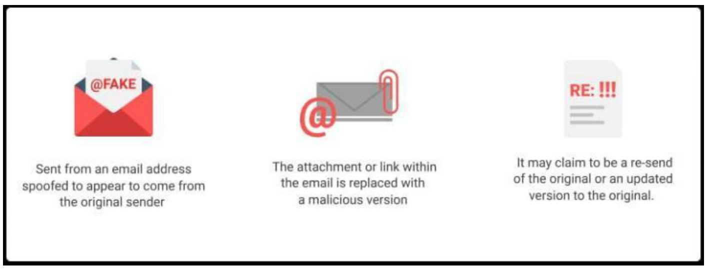

Fig 12: Steps of clone phishing

3. DETECTION TECHNIQUES

3.1 HEURISTIC BASED APPROACH

Heuristic approach is a classical method to detect phishing. Heuristics stand for the different features that are considered to check the originality of a website or URL. In this approach we extract different features such as IP address in the domain part, pop-up windows for passwords, '@' symbols in the URL from the URL & HTML Document Object Model of the webpage. On the later phase we compare the features that are already extracted with either that of the legitimate pages or the already recognized phishing features and later decide its authenticity. The technique that is used in this approach is the Decision Tree Algorithm with an accuracy of 96.76%.

3.2 BLACKLIST APPROACH

Blacklist contains a list of non-trusted URLs, spam websites and phishing sites that are already found and most of which are banned. This is usually maintained by large firms like Google. Blacklist is usually updated with multiple data sources like spam filters, user posts and financial institutions. To carry out this approach Simhash algorithm is used with an accuracy of 84.36%. However, coming to the disadvantage, it is often possible that the newly emerged phishing URL or website will not be available in the blacklist which is a hindrance to this approach. This becomes a benefit to the attacker as the unregistered URL will allow the user to access it whereas the registered URLs in the blacklist is completely blocked and inaccessible.

3.3 FUSSY RULE-BASED APPROACH

In fuzzy rule based approach uses the factors and characteristics that have been identified by different case studies and surveys. These factors helps in identifying the phishing website. This approach uses fuzzing data mining algorithm which has an accuracy rate of 100%.

3.4 MACHINE LEARNING APPROACH

Machine learning approach is a type of phishing detection technique which uses different types of algorithms to detect the malicious website. These algorithms basically take into consideration a feature or a set of features extracted from the website by comparing it with the existing phishing URLs. Some machine learning algorithms used is listed as below: Random forest algorithm Support vector machine (SVM) Swarm intelligence Genetic algorithm Accuracy in machine learning approach is more than 98.4%

3.5 CANTINA BASED APPROACH

Cantina based approach is a better detection technique where it concentrates on the content rather than the surface level characteristics of the given website. It has greater effects when combined with a heuristic approach in detecting phishing websites. This uses both Term Frequency and Inverse Document Frequency (TF-IDF) which is often known as a retrieval algorithm with an accuracy of 97%.

3.6 IMAGE BASED APPROACH

In an image based approach the normal and the phishing website can be clearly compared based on the visual blocks that are divided which are dependent on the visual cues. Each and every block in the phishing website is compared with that of the authorized website and based on their visual similarity the difference between malicious and normal websites is found. The technique used in this type of detection is web logo technique with an accuracy rate of 98%.

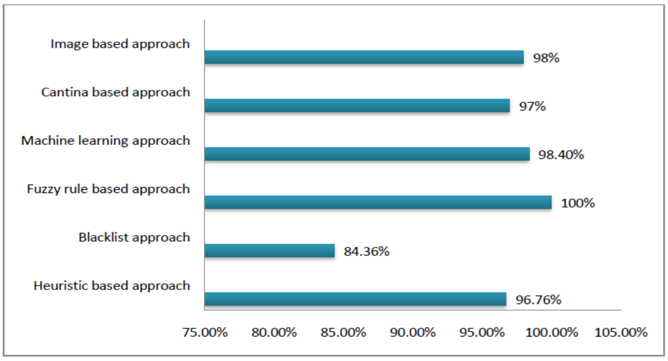

Figure 13: Detection Techniques with Accuracy in Percentage

4. PREVENTION MEASURES

As said: 'KNOWLEDGE IS POWER!!!' So it's a very high time that all the users have awareness towards the phishing attacks and their prevention measures.' AS PREVENTION IS BETTER THAN CURE!!!' it is the duty of an individual to take care and maintain their personal and financial information from the hackers/attackers in this modern era. To support to this awareness a list of preventive measures has been listed below for the benefit of the user.

4.1 GUARD AGAINST SPAMS:

Being extra cautious of the e-mails from unrecognized senders which might ask for the personal and financial information over the internet or those which frighten the user into acting quickly by threatening the user

4.2 USING TRUSTED WEBSITES:

It's always recommended to use the trusted website as one will have no vulnerabilities in those websites. Better to look into the URL and make sure it has a secured connection and information before accessing any website.

4.3 BEWARE OF ADS AND POP UPS:

Nowadays it has become a practice where we encounter a lot of ads and pop ups mostly related to your previous search history. One has to be extra careful while dealing with such ads. Better not to click on any pop-ups as it might lead you to some malicious website or link which later on might become a threat to your system.

4.4 FIREWALL AND SPAM FILTERS:

As the number of spams are increasing so do the efficiency of the spam filters and firewall. It is always recommended that we have firewalls and spam filters in our systems as it is of very high priority to secure the data and other important credentials from the hackers.

4.5 BLOCK UNWANTED CONTACTS:

If the user feels and experiences a non-trusted relationship with any contacts before it's better to get rid of it by blocking those contacts as it might become a problem somewhere in future also.

4.6 PROFILE PRIVACY:

Profile privacy can be accomplished by having multi factor authentication. Privacy can be effectively maintained when the user doesn't share his/her personal or financial sensitive information.

4.7 AVOID STRANGERS:

Ignoring the suspicious emails, phone calls or text messages which asks for personal data information is the best way to avoid attackers.

4.8 IDENTIFY SPAM EMAILS:

Whenever the user gets an email from a stranger it is better not to open it or click on any link present in it or download any embedded attachments since it is not from a trusted source. Most importantly when the victim gets to know it as a phishing trap he/she has to report it as spam without forgetting it.

4.9 USING SPAM AND PHISHING DETECTION TOOLS:

With an increase in the number of phishing attacks there is also increase in the development of phishing detection tools. They are user friendly, efficient and easily available (most of them are open source) so that any user can easily make use of these resources by adopting them to their systems to make sure their data is safe and secured from hackers. Below is list of few spam and phishing detection tools and platforms:

- SecurityIQ PhishSim

- LUCY

- MSI Simple Phish

- King Phisher

- Gophish

- Duo Insight

- Metasploit

4.10 MAINTAIN CONFIDENTIALITY:

Best way to maintain confidentiality is to encrypt the sensitive emails and data in order to prevent it from being vulnerable.

This can be carried out by installing an antivirus solution, schedule signature updates, monitor the anti-virus status on all installed equipment, and keep all systems with latest security patches.

TYPES OF PHISHING	PREVENTION METHODS
SPOOFING EMAIL	• Guard against spams • Identify spam emails • Using spam and phishing detection tools • Firewall and spam filters
FAKE SOCIAL NETWORK ACCOUNTS	• Block unwanted contacts • Profile privacy • Avoid strangers • Maintain confidentiality
HACKING	• Using trusted websites • Beware of ads and pop ups

	• Firewall and spam filters • Profile privacy • Using spam and phishing detection tools
DECEPTIVE PHISHING	• Guard against spams • Block unwanted contacts • Avoid strangers • Identify spam emails • Using spam and phishing detection tools • Maintain confidentiality (especially financial and bank details)
SPEAR PHISHING	• Guard against spams • Block unwanted contacts • Profile privacy • Maintain confidentiality • Avoid strangers • Using spam and phishing detection tools
WHALING	• Block unwanted contacts • Profile privacy • Maintain confidentiality • Avoid strangers • Using spam and phishing detection tools
ANGLER PHISHING	• Profile privacy • Avoid strangers • Maintain confidentiality • Block unwanted contacts • Using trusted websites and apps
CATPHISHING / CATFISHINGS	• Profile privacy • Avoid strangers • Maintain confidentiality • Block unwanted contacts • Using trusted websites and apps
CLONE PHISHING	• Guard against spams • Block unwanted contacts • Profile privacy • Maintain confidentiality • Avoid strangers • Using spam and phishing detection tools • Using trusted websites

Table - 1: Preventative Measures according to the type of Phishing

4. CONCLUSIONS

Social media and all social networking sites have become a part and parcel of life. Nowadays it has become a gateway where people tend to share their personal information and pictures with their friends and family to stay connected. Hence it has led for the social media servers to have a huge amount of data under different layers of security. As it is always said anything and everything has both good and bad in it, so does the technologies. We are able to experience a lot of malwares, worms and malicious contents in our mails and phones that spread through different means of social networks. Social media now acting as a new vector of attacks and causing multiple cases where the privacy of user is breach. Hence, it is necessary to understand, implement and engage in more productive discussion of sharing best practices to mitigate social media security risks.

REFERENCES

[1] S. Latha, Dr. Sinthu Janita Prakash, "A Survey on Network Attacks and IntrusionDetection Systems", 4th International Conference on Advanced Computing and Communication Systems, 6-7 Jan. 2017.

[2] Amber Umair, Priyadarsi Nanda, Xiangjian He, "Online Social Network Information Forensics -A survey on use of various tools and determining how cautious facebook users are?",

[3] Prajakta Tambe, Deepali Vora, "Privacy Preservation on Social Network using Data Sanitization", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.

[4] Khizar Hameed, Nafeesa Rehman, "Today's Social Network Sites: An Analysis of Emerging Security Risks and their Counter Measures", 2017 International Conference on Communication Technologies (ComTech), 19-21 April 2017.

[5] M V Suraj, Nikhil Kumar Singh, Deepak Singh Tomar, “Big data Analytics of cyber attacks: a review”, 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA), 6-7 July 2018.

[6] Jemal Abawajy, Mohd Izuan Hafez Ninggal and Tutut Herawan, “Privacy Preserving Social Network Data Publication”, IEEE Communications Surveys & Tutorials, 08 March 2016 .

[7] Soumya.T.R and S. Revathy, “Survey on Threats in Online Social Media”, 2018 International Conference on Communication and Signal Processing (ICCSP), 3-5 April 2018.

[8] Rakesh Singh Kunwar, Dr. Priyanka Sharma, “Social Media: A New Vector for Cyber Attack”, 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), 8-9 April 2016.

[9] Poonam Patel, Krishnan Kannoorpatti, Bharanidharan Shanmugam, Sami Azam, “A theoretical review of Social Media usage by Cybercriminals”, 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), Jan. 05 – 07, 2017, Coimbatore, INDIA.

[10] Edwin D. Frauenstein1 and Stephen V. Flowerday2, “Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats?”, Information Security for South Africa (ISSA), 17-18 Aug. 2016.

[11] Ana Ferreira, “Why Ransomware needs a human touch”, International Carnahan Conference on Security Technology (ICCST), 22-25 Oct. 2018.

[12] S.Nisha, Dr.A.Neela Madheswari, IEEE Member, “Prevention of Phishing Attacks in Voting System using Visual Cryptography”, International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 24-26 Feb. 2016.

[13] Purushotham Parthiban Parthy Gowthamaraj Rajendran,“Identification and prevention of social engineering attacks on an enterprise”, 2019 International Carnahan Conference on Security Technology (ICCST), 1-3 Oct. 2019.

[14] Thierry Mbah Mbelli, Barry Dwolatzky, “Cyber Security, a Threat to Cyber Banking in South Africa - An approach to Network and application security”, IEEE 3rd International Conference on Cyber Security and Cloud Computing, 2016.

[15] Suman Bhattacharyya , Chetan kumar Pal, Praveen kumar Pandey, “ Detecting Phishing Websites, a Heuristic Approach**”,** International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137, Volume – 02, Issue – 03, March – 2017, PP – 120-129

[16] Nathezhtha, Sangeetha, Vaidehi, “WC-PAD: Web Crawling based Phishing Attack Detection”, 2019 International Carnahan Conference on Security Technology (ICCST), 1-3 Oct. 2019.

[17] Hong Bo, Wang Wei, Wang Liming, Geng Guanggang, Xiao Yali, Li Xiaodong, Mao Wei, “A Hybrid System to Find&Fight Phishing Attacks Actively”, 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology.

[18] Muhammet Baykara, Zahit Ziya Gürel, “Detection of phishing attacks”, 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 07 May 2018.

[19] G. Jaspher Willsie Kathrine, Paradise Mercy Praise, A. Amrutha Rose, Eligious Kalaivani. C, “2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)”, 23-25 April 2019.

[20] Lakhita1 Surendra Yadav, Brahmdutt Bohra, Pooja, “A Review on Recent Phishing Attacks in Internet”, 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

[21] Juan Chen, Chuanxiong Guo, “Online Detection and Prevention of Phishing Attacks”, 2006 First International Conference on Communications and Networking in China, 25-27Oct. 2006.

[22] Prasanta Kumar Sahoo, “Data mining a way to solve Phishing Attacks*”,* 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), 1-3 March 2018.

[23] Surbhi Gupta, Abhishek Singhal, Akanksha Kapoor, “A Literature Survey on Social Engineering Attacks: Phishing Attack”, 2016 International Conference on Computing, Communication and Automation (ICCCA), 29-30 April 2016.

[24] Rakesh Singh Kunwar, Dr. Priyanka Sharma, “Social Media: A New Vector for Cyber Attack”,2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), 8-9 April 2016.