A Brief Review of Phishing Detection and Prevention Methods

Prof. R.A. Khan[1], Prasad Mahabare[2], Kanak Likhite[3], Makarand Raut[4], Swapnil Baviskar[5]

Computer Science & Pune University, India

***Abstract*: Cyber-attacks have become an international threat worldwide - confidential and secret data is being compromised which can harm national security. Two domains of the IT industry are majorly compromised which primarily consists of information processing and physical infrastructure supporting the first domain. Phishing is one of the most popular attacks that malicious groups carry out towards the general users. Phishing is the vindictive attempts to gain sensitive information like username, passwords, credit card information etc. which is often disguised as trustworthy source to the innocent users. When combined with Social engineering which often differs for different users, they may find very tempting to log in their credentials. This makes phishing one of the most dangerous and malignant attack. Although Phishing websites are very common, there are numerous methods to detect are prevent these attacks. These range from URL detection where a phishing website can be detected using some of the key features based on their Uniform Resource Locator to the use of Machine Learning Algorithms like Random Forest, Artificial Neural Network or Select Vector Method so that to stop these websites dynamically. There are also some methods that use Blacklist approach, where the system refers to anti-phishing repositories like Phishtank or Yahoo Phishing database to check whether the site is a phishing website or a legitimate one. This review paper explains many different methods used for the detection and prevention of phishing websites explaining the above-mentioned techniques in much more detail and also many other methods that help the users stay safe and secure from this type vicious attack.**

***Keywords:* Phishing attack, URL, Machine learning, Anti-phishing repositories, Social Engineering.**

I. INTRODUCTION

Phishing attack happens when a malicious website mimics a legitimate and trustworthy website to trick the users into submission of their sensitive credentials. The main motive of these malignant websites is to harvest the credentials of different users and to use this for various fraudulent activities. Nowadays users can perform various online activities like sending/receiving emails, banking transactions, buy/sell goods and others. Such activities are susceptible to phishing attacks and many victims suffer due to it. The victims may lose information in this process. Hence, due to the ignorance of internet users, the phishers exploits the security. Two types of issues occur with phishing -technical and non-technical (human). To obtain a powerful solution, both issues should be handled effectively. Over a time, multiple software has been designed to tackle the overlooked situation of phishing. Techniques for phishing can be classified as web content, industrial toolbar and user interface based anti-phishing. These methods cover filtering, authentication, analyzing and attack tracking. These services, however, all phishing attacks are not blocked/stopped by them. Latest studies show that the use of Machine Learning can help tackle this type of attack. Machine Learning is a branch in Artificial Intelligence that that gives the system the functionality of learn things automatically without someone explicitly programming it. The use of algorithms like Artificial Neural Network, Naive Bayes can be used for the detection and prevention of Phishing websites. Artificial Neural Network is a archetype of Machine Learning algorithm where information communication is inspired by the actual working of neurons. It helps the system to have adaptive learning and self-organization. Its applications range from self-driving automatic vehicles to fraud detection. Naive Bayes is a type of Machine Learning algorithm where classification is done with the help of our understanding of probability. The real-world applications of Naive Bayes range from email spam detection to facial recognition and much more. These and many other algorithms can be used for detection and prevention of phishing websites. In this survey paper, many machine learning algorithms are compared with one another to analyse their accuracy over different standard metrics on a common data-set. According to APWG survey report the absolute of phish identified in 1Q2018 was 263,538. This was raised up 46 percent from the 180,577 examined in 4Q 2017 as shown in Fig. 1. It was also compellingly more than the 190,942 seen in 3Q 2017.

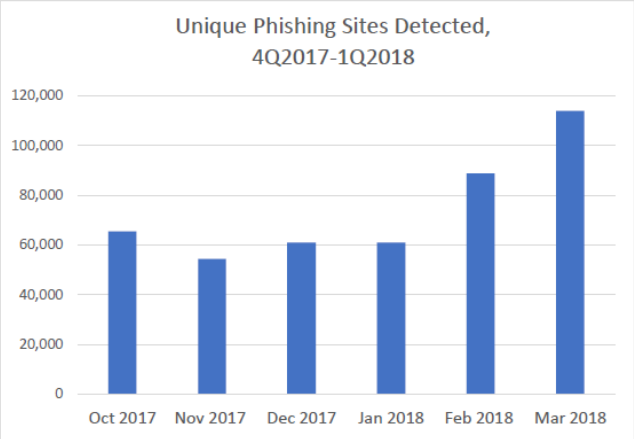

Fig. 1. Total number of submitted unique phishing reports in the 1Q of 2018 to APWG. Source: [10]

I. LITERATURE SURVEY

The ranks and number of results generated by famous web search engine were used for classification [1]. Legitimate websites get back huge number of results and are ranked first, whereas phishing websites gets no response and are not ranked at all. Common characteristics of phishing websites are analyzed by Heuristic-based techniques as shown in Fig. 2. Maintenance of central database is not required. The regularly used technique is white-listing and blacklisting, one of the main drawbacks of using blacklists and white-lists is that they can only identify/detect previously-known phishing or legitimate websites.

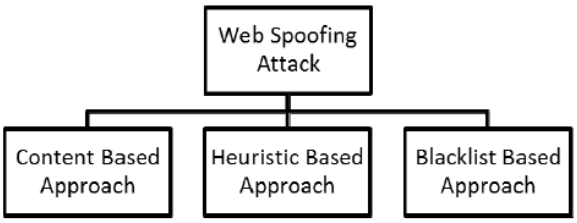

Fig. 2: Web Spoofing Attack Detection Approaches

Reputation of a website is used for classification in this paper. This approach has two advantages (1) it is easy to develop and deploy (2) web search engines crawl and cache of old and new web pages so its effectiveness increases against new websites. When it comes to classifying new websites, existing phishing detection methods based on white-list and blacklists gives a low performance. The phishing websites spoof only the web pages that have their primary language as English. Famous brand names are placed in many distinct parts of URL [2]. Such method of phishing is exploited by giving weights to words obtained from the HTML contents. Brand in URL is efferent way to distinguish between legitimate website and phishing website. To find owner of selected domain WHOIS look-up is used. Payment services and financial sector are the most phished industry. URL and domain of websites checking is the most common method for anti-phishing. Brand name is a unique identity as it is given to a legally registered service, product or business. Sub-domain of hacked website-domain and maliciously registered domain are used by attacker. When domain name owner is different from domain name owner from legitimate website then the query website is considered as phishing.

This paper focuses on tackling phishing attacks by building a fuzzy model [3] using fuzzy rules in combination with neural networks with six inherent data sources to discover phishing websites and prevent attacks. Goals The goal is to use optimization technique like hybrid learning method to evaluate and clarify the framework of fuzzy systems. The proposed system employs six data sources built on fuzzy system along with neural network to tackle the issue strongly. The six data sources include: 1. Legitimate site rules 2. User behavioral profile 3. Phish Tank 4. User-specific sites 5. Pop up windows 6. User credential profile This feature is the centre of the system from 300 features are devised. These features are passed through ML algorithms, fuzzy systems and neural network to group them into legitimate, suspicious or fake(phishing) websites. Fuzzy IF-Then rules used are devised to extract results. * If features are low then legitimate website. *If features are medium then the suspicious website. *If features are high then phishing website. The devised fuzzy model is somewhat alike to Sgueno type. Input layer, fuzzification, rule base, normalization, and defuzzification are the 5 major constituents of the system.300 features are arbitrarily tested or trained. 2-fold cross-validation is used to calculate its precision. Average accuracy was found to be around 98.7%. After tuning the model, the best-case accuracy was found to `be 99.6%. This method is based on Fuzzy system with proper functional tuning along with varied data proves to be among one of the top successful system to detect phishing precisely. Fuzzy rules in order to classify data into safe, suspicious and phishing website were contributed. New parameters based on the system were found to provide best and optimized results.

On account of Communication architectures [4]: if fact being more specific with client-server architecture server administers the utilities to his clients and that includes forestall from numerous cyber-attacks which further includes phishing attacks too which has its own stumbling blocks such as the mugger gains the IP of servers which leads to falsification of data and can cause impairment of organization or individual. To vanquish this flaw the author has brought into a new phishing inhibitor execution. To illustrate

further it is deployed as Master-Slave utilization and a browser flavour enhancer. This new execution also brings to light the target and bid user to side-track there. The system proposed here unruffled by two fundamental regulations: A phishing web page espial mechanism that will categorize the phishing as well as lawful web page whereas an intent recognition arrangement will derive probable target of phishing page. Heretofore, the prevention paradigm utilizes blacklists of websites as a sturdy handler which might be time leech in some cases. In authors direction to diminish the call of duty a white-list of hashes is developed upon URL initiating and landing along with HTML wellspring that pinpoint trustworthy web pages and sidestep scrutiny. The application tranquil of five segments: (a) Backdrop script that gathers the logged links and redirection chain and (b) Foreground script has one object instill in each open tab of the browser executes for every loaded web page. It also blends data wellspring gathered by Backdrop script then this prepared information is traded for analysis after this (c) Bearer obtains data wellspring saved by Foreground Script which will evaluate the hash of web page on the subject of white-list. The Bearer's objectives are: (I) If it constructs no fit the data will get post to (d) phishing determiner which will apply phishing determination emphasized on data wellspring and the opinion is given to reciprocal of object of Foreground script. (ii)If it constructs no fir the piece of information is sent to one object of (e) Target Identifier presumes the often targets of the phishing web page from the data wellspring. Operations of Target Identifier are: (I) if the target matches with the Top-level domain of ongoing website then treated safe without opinion of phishing determiner and warning message will die out or else the notice is upgraded with probable targets. To eliminate the time leech two target identifiers are involved to distribute workload. According to author, Accuracy appraised is 99.9%.

An algorithm was proposed primarily based on heuristic anti-phishing [8] approach to know whether a web address is legitimate or not, as shown in Fig. 3. The algorithm provides alert on whether the URL of a particular website is legit or not by straight providing URL as a standard input. The algorithm progresses in four major test or steps Usually each honest URL has a specified predefined syntax: <protocol>://<host-name><path>. URL or hyperlink is taken as the input, Alert message on whether the URL is safe or not is provided as output. Step 1; Safe Browsing API is used to know whether the URL is present in the Google's latest blacklist of malicious phishing and fake web pages if found user is alerted otherwise. Step 2; URL is checked whether if it exists in the Google Search Index. If the specific URL is absent from the top 10 results the Domain of the URL is tested separately if present, then the URL is flagged as legitimate if absent it is flagged as malicious phishing URL. Step 3; If URL is absent from the blacklist but found by the search engine the ranking of the URL in Alexa page ranking Database is checked (page rank is calculated by no of visitors of the URL and popularity) Legit URL have higher rank, whereas malicious URL have low rank close to zero. If rank is high it is denoted as safe, if close to zero then it is marked as phishing URL. Step 4; For apparently new URL a. Top level domain is tested. b. Spelling of the domain is checked. c. Check if IP address is masked in the domain name. d. Special characters or dots present in URL are checked. f. Irrelevant Slashes (//) present in domain are checked. g. Time to live value of the URL is checked. This algorithm provides quick results on new as well as old URLs. The only drawback is that it works only on HTTP URLs.

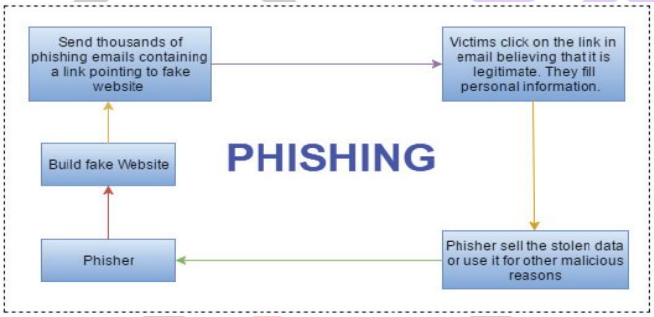

Fig. 3: Flow of general phishing attacks

Based on the analysis of web server log [7] pages, a new method for the detection of phishing website has been introduced in this paper. When the user clicks on a phishing website, the spoofed site always asks for some resources to the regular website. This request always gets stored in the form of log files of the website server. By analyzing these log files, one can accurately detect phishing websites. The process of obtaining information by the phishing website can be categorized into four steps: 1. When the user first clicks on a malicious website, an HTTP request is sent to that website to gain access to the elements of the website 2. There are some features that are not present in the phishing website which are shown in the legitimate website, hence the phishing website requests these resources to the legal site. 3. The legitimate website acknowledges this request and responds to the phishing website with the additional required resources. By doing this, it also stores the information of this transaction into its official log file. 4. This is the reason the general users who are deceived by the spoofed websites cannot differentiate between the legitimate website and phishing websites. Phishing Detection: The study proposes a two-stage process for Phishing detection: Stage 1: Refine Stage 2: Affirmation. The first stage of the process is called refinement where web server log files are taken as input. The first stage involves the collection of all the legal information about the legitimate website this includes features like domain, IP address, ICP numbers etc. After this stage, we can easily extract all the different URLs that have interacted with this website. Once we get these URLs, we can filter out the legitimate URLs to the "suspicious URLs". Stage two is called Affirmation Stage where each suspicious websites are given a Phishing scale with the help of automated verification. These scores will differ from each website. After this stage there comes the step of Human Validation where a high phishing score is analyzed closely by human scrutiny. After the above stages, one can determine whether the site is spoofed or not.

Authors in [6] proposed a system was proposed to identify phishing web page using Machine learning algorithms. 5 popular classification algorithms are compared on the basis of data-sets generated by extracting features from URL and web page. A web crawler was implemented to scan the URL and derive the distinct features from the content of the web page. 1. Feature Extraction:

The web crawler was used to extract distinct attributes and classify them into three major classes a. Lexical Features; IP address Malicious URLs have IP address in place of domain name. Whether the IP address contains the domain name is checked by this attribute. Suspicious URL Presence of special character such as "@", dash etc. in an unusual place which identifies malicious URLs are checked. Host-name Spell Spelling and length of the host-name is checked and verified to get more clarity by this feature. b. Page Content Features TF-IDF: Term Frequency-Inverse document frequency. It is used to calculate the occurrence of a specific term in a given document. This feature derives top 5. TF-IDF terms of the web page, Google searches them and verifies if the URL associated is present in the top 5 search results. Suspicious link: This feature checks whether the links and hyperlinks present in the web page are legitimate or not. Forms: This HTML features identifies if the host is demanding to know any kind of personal or private information. c. Domain Features Site Popularity: This feature determines the popularity and activity of the address from Alexa Ranking. Age of Domain: By the help of WHOIS this feature checks the registry age of Domain. Relatively new domain has a high rate to be Phishing website. 2. Data-sets: 4420 legitimate websites collected by crawler as well as 5389 phishing address from Phish Tank were collected for training and testing. 3. Training and testing was implemented using fivefold method. WEKA was used to portray the following classification algorithms: a. Support Vector Machine b. Naive Bayes c. J48 decision tree. d. Random forest e. Neural networks. The tests and evaluations proved that domain feature group (97.9%) and page content feature group (94.9%) made higher contribution in identifying Phishing while lexical feature group (72%) provided least. Among the Classification Algorithms, Random Forest (98.8%) provided the most accurate results. This search material emphasis on, it is proposed the discernment of web spoofing websites with the focus on Uniform Resources Locators. By auditing URLs one can easily distinguish various URL features of a legitimate website and a phishing website. By careful examination of different URLs, when a phishing website is distinguished, it is reported to anti-phishing data-sets like Phish Tank or Yahoo directory [5]. The following study involves the use of approach involving blacklists. Approach involving Blacklists: This is the most common approach when dealing with Phishing websites. In this approach, a known anti-phishing data set called blacklist keeps on revising the names of all the acknowledged phishing websites. Thus, if a web page is mentioned in the blacklist, the user cannot access that website on the Internet. Example of an entity that uses Blacklist approach is Net Craft Toolbar. This is one of the many available anti-phishing tools available over the internet that investigates security leaks via web crawling techniques. Phishing Features based on Address bar: 1. If the URL of the website contains an IP address, then that website is a spoofed one. For example, if a website has a URL of "<<http://192.168.2.1//login.html>>" that web page will probably steal your credentials and use it for nefarious activities. 2. In general, the length of any legitimate URL does not surpass 54 characters. If the extent of the URL is between 54 to 75 characters, then the web page is a suspicious one. If the extent of the URL exceeds 75 characters, then the web page is a phishing site. 3. It is observed that to deceive the general users to think that the spoofed website is a legitimate one, a hyphen (-) is added at the beginning or at the suffix of the URL. Hence if the URL contains this hyphen at the start or at the suffix, the website is categorized as a Phishing website. 4. Some URLs contain real legitimate websites as a prefix and then implement the phishing part at the end. For example: "<https://genuinewebsite.com//https://spoof.com>" This can be identified by the position of "//" symbol. Generally, if the website contains HTTP then the position of the double slash would be sixth, or if the site contains HTTPS symbol, then the position of the double slash would be in the seventh position. If the is an occurrence of the double slash at any point greater than the seventh character the site will be a phishing website. 5. If the URL contains '@' symbol, the browser tends to ignore anything before that. Hence the spoofed site gets away with this. Hence if the URL contains '@' symbol, it is automatically classified as phishing web page. The paper focuses on the drawbacks of phishing websites by implementing an application called PhishChecker. This application takes any website name as an input and then checks whether the URLs of that website match the above conditions regarding spoofed versus legitimate websites. For experimental purposes, a series of 100 URLs were taken where 41 sites were elected from anti-phishing data sets with 59 were legitimate websites. Result of the experiment was that the application listed 68 websites as legal while 32 websites as phishing. Hence achieving a reputable accuracy percentage of 96%.

David G. Dobolyi [9] created an application named PhishMonger which has both open source analysis of live phishing websites and public database. They tackle many challenges like (1) There's a time limit to every phishing website means they are online for only a few hours. (2) Phishing websites contain Malware in different forms like images, multimedia, and scripts. It provides help to researchers in two ways: (1) To analyse the properties of live phishing websites. (2) A public repository of phishing websites that help to figure out users' susceptibility. This application runs on Amazon Web Services, EC2 (Elastic Compute) in which they have used Ubuntu Virtual Machine. So, while the application is viewing these phishing websites it not affected by malware present in the website. Once data is collected, the folder having new sites is compressed into the tar.gz format to avoid continues anti-virus warning. While an organized, searchable achieve of every report and more than hundred pre-defined categories are provided by PhishTank. Its API is also available.

Both business and general people are constantly affected by the serious threat of phishing on the Social network [11]. Social engineering (SE)is easy on those people who are very active on Social Media. Social Network is used by many people with distinct background and are influenced to share their information, phishers use this chance to steal confidential information. Spear phishing which means more targeted phishing attacks are done on the basis of such information both on or off the social network. Users poor privacy habits are used to exploit their online behaviour by provoking them to click on links that are related to them. To induce users, Social Engineering methods are commonly used by phishers that focus on encouragement of human emotions such as greed, fear, heroism and desire to be liked. ELM framework is suitable for analyzing SE attack traits. In this recommended research paper states trait extraction from website's URL and scrutiny subgroup emphasized on feature excerpt techniques and distribution algorithms for determining phishing websites.

In the mentioned paper author [12] proposed fortunate determination of diversity of phishing Web-pages by developing new trait set entrust on their scrutiny and numerous present researches on phishing websites. The main focus behind this approach was to generalize the formal phishing attacks disclosure routines and make the scheme more malleable with simple to enhance trait set by blending new and upcoming scenario as they emerge. Here the testimony set emphasize on phishing sites which are mostly aimed

on the well-known brand label. The recommended system regulates most aimed brand signs with their real time phishing URLs from PhishTank website. After determining the phishing author used Google to gain Legitimate URLs relevant to those brand signs and scrutinized 8538 URLs involving 3622 original and 4919 proved phishing website. In the Traits extraction phase, a trait matrix is developed on the eradication of URL features and categorized in five major tests. Most of the traits of URL are in textual characteristics and remaining depends on the third parties' services. For the Textual properties codes are built on C# programming while some online transformations are gathered for some of the traits extraction and to get the "Whoisrecord" R programming scripts are written along with some manual work on collected information. According to author, 133 distinct traits are found in URLs from their data-sets, as shown in Fig. 4. So, after matrix creation for traits author applied subgroup-oriented trait picking method to find notable traits and also to optimize information dimensions by dropping redundant and not so related traits in consideration of analysis. The evaluation of traits picking with performance impact to categorization algorithm is done on CFS subgroup and Consistency subgroup and for the scrutiny WEKA apparatus is used where Naive Bayes along with Sequential Minimal Optimization algorithms are used for categorization. The accuracy of Naive Bayes and SMO distribution algorithms are 88.17% and 95.39% respectively. The above statistics shows that SMO displayed better performance in Consistency as well as CFS subgroups if compared with Naive Bayes approach.

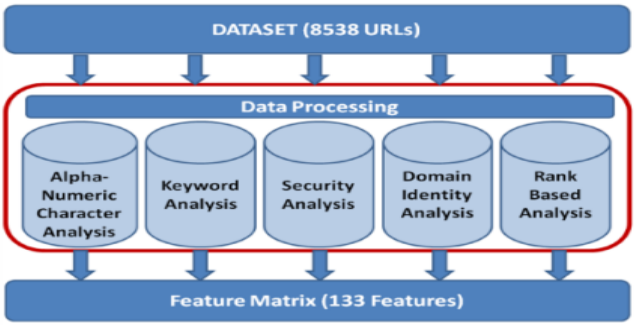

Fig. 4. Feature matrix

The evaluation of traits picking with performance impact to categorization algorithm is done on CFS subgroup and Consistency subgroup and for the scrutiny WEKA apparatus is used where Naive Bayes along with Sequential Minimal Optimization algorithms are used for categorization. The accuracy of Naive Bayes and SMO distribution algorithms are 88.17% and 95.39% respectively. The above statistics shows that SMO displayed better performance in Consistency as well as CFS subgroups if compared with Naive Bayes approach.

II. CONCLUSION

From this paper, it can be inferred that there are many possible ways to detect and prevent phishing attacks. Some methods involve Machine learning concepts while the others do not. Some of these methods analyse URLs to identify their potential peculiar characteristics. While the other method checks the web server log files to identify whether the phishing website did some transaction of resources with the legitimate website. Hence tracking it down and blocking it. Machine Learning plays a very vital role in this field. It enables a dynamic approach for detecting and preventing phishing websites. Machine learning algorithms like Artificial Neural Network, Naive Bayes, Random Forest help to classify these phishing websites into different categories. Hence, this approach dynamically declares a website as legitimate or phishing website. There are three methods of the prevention viz. Content Based Approach, Heuristic Based Approach and Blacklist Based Approach. The methods that do not use Machine learning techniques often use Blacklist based approach, which leads to a static method of detection and prevention. Machine Learning techniques prevents these attacks dynamically and works at run-time. Studies praising fuzzy system along with neural network based on fuzzy rules also provided beneficial results. After reviewing the above-mentioned studies and researches it can be concluded that among various Machine Learning algorithms Random Forest algorithm emerges as most optimal classifier for feature extraction.

REFERENCES

[1] Jun Ho Hun and Hyoungshick Kim, "Phishing Detection with Popular Search Engines: Simple and Effective ," in, Springer-Verlag Berlin Heidelberg, 2012.

[2] Choon Lin Tan, Kang Leng Chiew, San Nah Sze, "Phishing Website Detection Using URL-Assisted Brand Name Weighting System ," in, IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS) December 1-4 , 2014.

[3] Phoebe Barraclough, Graham Sexton, "Phishing Website Detection Fuzzy System Modeling ," in, Science and Information Conference 2015 July 28-30, 2015.

[4] Giovanni Armano, Samuel Marchal, N. Asokan, "Real-Time Client-Side Phishing Prevention Add-on," in, IEEE 36th International Conference on Distributed Computing Systems, 2016.

[5] Abdulghani Ali Ahmed,Nurul Amirah Abdullah, "Real Time Detection of Phishing Websites," in, IEEE 2016.

[6] Huu Hieu Nguyen and Duc Thai Nguyen, "Machine learning Based Phishing Websites Detection," in, Springer International Publishing Switzerland 2016.

[7] Jun Hun, Xiangzhu Zhang, Yuchun Ji, Hanbing Yan, Li Ding, Jia Li and Huiming Meng, "Detecting Phishing Websites Based on Study of the Financial Industry Webserver Logs ," in, 3rd International Conference on Information Science and Control 2016.

[8] Varsharani Ramdas Hawanna, V. Y. Kulkarni, "A Novel Algorithm to Detect Phishing URLs," in, International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology(I^2IT), Pune, 2016.

[9] David G. Dobolyi, Ahmed Abbasi, "PhishMonger: A Free and Open Source Public Archive of Real-World Phishing Websites," in, IEEE, 2016.

[10] Anti-Phishing Working Group (APWG), "Phishing activity report 1Q 2018," http://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf , 2018, accessed May 2018.

[11] Edwin D. Frauenstein and Stephen V. Flowerday, "Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats," in, IEEE, 2016.

[12] Mustafa AYDIN, Nazife BAYKAL, "Feature Extraction and Classification Phishing Websites Based on URL," in IEEE CNS Poster Session, 2015.