**International Journal of Innovative Research in Engineering**
Volume 5, Issue 1 (January-February 2024), PP: 55-59
https://www.doi.org/10.59256/ijire.20240501001
www.theijire.com
***ISSN No: 2582-8746***

# An Investigation of AI-Enabled Comprehensive Survey of Phishing Attacks detection techniques

**Sivakumar Nagarajan**
*Technical Architect, I & I Software Inc, 2571 Baglyos Circle, Suite B-32, Bethlehem, PA-18020, USA.*

**How to cite this paper:**
Sivakumar Nagarajan, "An Investigation of AI-Enabled Comprehensive Survey of Phishing Attacks detection techniques", IJIRE-V5I01-55-59.



***Abstract:*** *Phishing is an online criminal activity which traps regular online customers to reveal their sensitive information into fake destinations by disguising themselves as original website. Because of the short life expectancy of phishing sites and the fast progression of phishing systems the current anti- phishing solutions are either unfit to manage the rising changes or in fit for assuming a successful part against this attack.Natural language handling and machine learning – these are the centre usage of the multi-stage approach proposed to identify phishing attacks and to perceive the substance/association that has been misused by the attackers to execute the phishing attacks. In this technique the primary stage is the revelation of named elements (names of areas, individuals and associations) and afterward the disclosure of concealed topics and for this the strategies that backings both phishing and non-phishing information therefore, Conditional Random Field (CRF) and Latent Dirichlet Allocation (LDA) is utilized. Next stage is the AdaBoost arrange where the named elements and the concealed subjects are dealt as features and the messages are ordered into phishing or non-phishing. proposed techniques are planned to alleviate the effect of phishing attack.*

*The principal strategy proposes is to identify Wi-Fi phishing utilizing Association Rule mining. A Wi-Fi hotspot which associates such hand held gadgets has turned into a transitory archive of delicate data, in this way giving an open door for programmers to gather money related gain .Consequently data security arrangements tending to Wi-Fi hotspots (Wi-Fi phishing attack) has turned into the need of great importance. The conceivable approaches to attack the security of Wi-Fi hotspots and counter-attack methodologies have been tended to in this strategy.*

***Key works:*** *Phishing, LDA,AI*

## I.INTRODUCTION

The invention of Web 2.0 presented web based social networking organizing sites. The online networking organizing sites are used by people to share information about them with the rest of the world. Entrepreneurs and business people often use social media to market their products which resulted in sharing of their services and offering to the Internet. Entrepreneurs started sharing potential information into social media networking sites which created the need for information security. Because of the accessibility of information in social media, networking websites resulted in security threats. The security threats created the need for web security policy that will help the social media sites to protect user data from intruders. Social media sites started introducing web application to make their sites productive to users. The web applications process the information given by the user and perform transactions. It leads to the need for Web application security like Information Security. The web application security manages to secure the information that is exchanged online to remote servers. The information is prepared by web applications that utilize the internet and web based system.

**Vulnerability:** The web applications are developed by developers who may not aware of web application security. This resulted in flaw at a particular portion of the application. The attacker uses this weakness to enterinto the web application and tries to access the potential data. The scenario mentioned above is called as vulnerability.

**Threat:** The Web applications are hosted on remote servers which may or may not provide needed security to the hosted application. The above-mentioned scenario is a kind of threat to a web application which triggers vulnerability to takes place in the system. The threat comes in multiple forms. The forms changes according to the scenario. The single definition for threat is not possible because of dynamic nature of the threat.

The major difference between threat and vulnerability is the place of flaw that occurs in a web application. For example, if flaws occur in part of web application then it is called as vulnerability. If flaw occurs external to the application then it is called as a threat. In the above-mentioned example, managing the web application is not in direct control to the developer which possibly causes threat. If the flaws are present in a web application due to lack of knowledge of programmer then it is called as vulnerability.

These online attacks represent a wide scope of risks including money-related harms, identity theft, loss of secret business information theft of network resources, Damage of the brand or individual reputation, and reducing customer trust in internet business. These high stakes, the inescapable utilization of the web, and the trouble of ensuring security against online attack consolidate to the frame. It might be the best challenge to securing individual and business information.

In Recent days, one can notice that there is a sharp rise in the number of web threats, most of which are designed by the help of crime ware (Application Security Project 2013). The usage of these kinds of toolkits makes the job easier for the attackers when compared to other methods. Some of the well-known toolkits are as mentioned - Zeus, MPack, Neosploit, BlackHole, NukesploitP4ck, and Phoenix.

In current scenario the development of security threats is huge. Web application attacks are excessively remarkable among all the threats. According to the measurements, The Web application attacks that occupy nearly 92% as it comprises of SQL Injection, cross-site scripting, and Phishing. Figure 1.1 shows different security threats (Symantec, Internet Security Threat Report 2016).

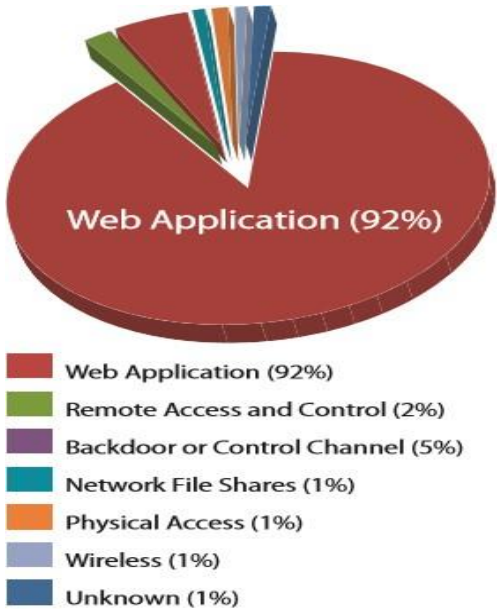


*Figure 1 Report Indicating Different Security Threats*

**1.2 Phishing**

Phishing is another kind of web security vulnerability which uses mimic websites that appear legitimate to end user (Anjum & Shaikh 2016). The intruders create an appearance like the website is a trusted source and tries to capture the confidential information like credit card numbers and other personal information. For example, the mimic website of the bank is created and hosted in web server with minimal difference in the domain name of the site. The intruders send email to users of original bank website with the fraudulent link. The end user opens the website page and it seems like a unique page and login the site, as usual, to carry out the transaction. The intruders use this information in original bank websites to attack the user bank account. Figure 1.2 shows phishing workflow.

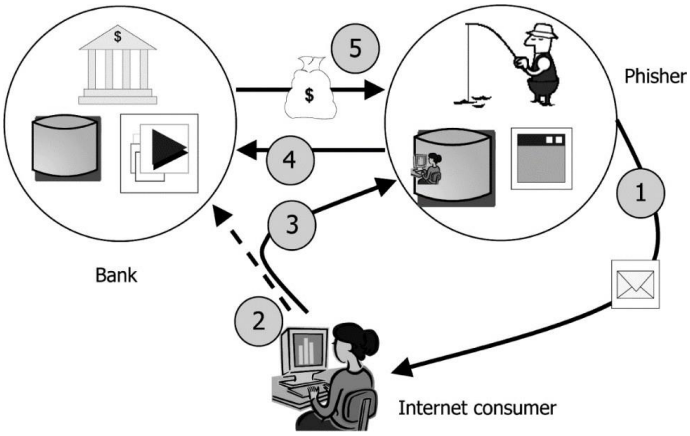


*Figure 2.Phishing Workflow*

The financial crisis and stealing the identity will be the result when the client faces a bribe of his/her personal information. 'America Online'- this is the very first website which has been trapped by a Californian teenager in the year 2004 and was impersonated. This case was brought up legally. The attacker happened to abuse all the user information and credit card details and made the profit out of the same through money transactions.

**Different Ways to Perform Phishing**

Email-to-email: In this technique, the intruder‘s sends an email like an e-mail sent from the legitimate company to

target user and ask for confidential information. The user will provide confidential information. The intruder uses this data for hacking.

Email-to-website: In this technique, an email is sent to the users to click the link. If the user clicks the link then the mimic website is opened that looks like a legitimate website and prompt the user to enter the confidential data. Once if the user enters the data then it will store in intruder database which will be used for hacking the user accounts.

Website-to-website: In this technique, an advertisement is displayed on the legitimate website. When the user clicks the advertisement then it will execute few lines of the script which will fetch data from the local system and sends to the remote server. The intruder uses this information to hack the user account (Barraclough *et al.* 2013).

Browser-to-website: In this technique, a phishing website is created and hosted on the internet with minimal difference in the domain name. If the user misspells the address of the website in a web browser then it will automatically open phishing website according to the misspelled site provided by the user. The phishing site will try to capture few confidential data from the user. The intruders use this data to attack the user account.

Phone Phishing: In this technique, the intruder makes a phone call to the target users and introduces him or her as calling from a legitimate company and creates a trust in target user mind by providing few data that he or she gathered from the web. At that point, the intruder attempt to gather secret information which he or she uses for hacking the target user account.

## II.ANTI-PHISHING MODELS

**Server-Based Anti-Phishing Techniques**

Server-based Techniques are implemented by website providers.

**Brand Monitoring:** A web-crawler is used to search websites to identify clones (which looks like a legitimate website). Suspicious websitesare then added to the given list repository.

**Conduct Detection**: For every client, a profile is recognized, whichis utilized at that point to identify irregularities in the conduct of clients.

**Client-Based Anti-Phishing Techniques**

Customer based methods are actualized with the given client's endpoint through program modules or email. New techniques of authenticationare under research, such as using an image during the registration phase whichis shown during every login process.

E-Mail Analysis: Email-based methodologies usually utilize channels and substance examination. In case of utilizing those features consistently, Bayesian channels are quite successful in blocking bothspamming and phishing messages.

Black-Lists: Blacklists are collections of URLs recognized asharmful. The blacklist is questioned by the program run-time at whatever pointa page is loaded. If the recently visited URL is incorporated into the blacklist, the user is informed with respect to the threat, otherwise, the page is viewed asgenuine.

## III.ANTI-PHISHING STRATEGIES

**List based anti-phishing approaches**

In this approach, a website is classified as phishing or trusted by asimple database look up. These list-based approaches are further breaking down into blacklist and whitelist. White and black list matching is one of the best effective methods to detect the phishing .

**a) Blacklists**

Blacklist is a database that contains the list of websites that have been proven to be fraudulent. Before navigating to a website, the browser checks the database to see, if the requested URL is a genuine or a phishing website. Some online databases such as Phishtank (http://www.phishtank.com)gives a list of phishing websites, however, it takes time to a phishing websiteto be analysed and added to the blacklist. Within this time frame, the phishing website would have done most of the damage to the targeted user and the organization that is being impersonated. Another issue is that blacklist approach cannot aid in detecting targeted phishing attacks such as spear phishing (Kesler *et al.* 2006) since they target small groups or even sometimes an individual web user.

**b) Whitelists**

This approach is not as preferred as blacklists. The idea is that a site must be explicitly trusted before granting access to the website. Here the user manually builds a white list by adding the trusted website to the white list.In this case, either a) client is denied to get the websites other than the one included in the white list – static implementation or b) the user is prompted to add the site to the white list before granting access to the website. The problemwith this approach is that every time the user visits a new website, he has to add that to the white list and eventually the user will be annoyed and disable this feature. Also, the vast majority of the site that the client explores will be new and the web client needs to frequently and manually analyse the trustworthiness of the site which the user has not already included in the white list. White list method is also used in some of the phishing detection methods based on the visual similarity techniques .

Both these type of the list-based approach fails to detect zero-day attack (newly created phishing site) as there will not be any information recorded in any blacklist databases. This is because a considerable amount of time and analysis is required before confirming the trustworthiness of the website and adding it to the phishing list.

## IV. CONTENT-BASED PHISHING ANALYSIS

content-based image analysis technique to battle zero-day phishing attacks. The heuristic-based approach is essentially used to recognize content based zero-day phishing attacks and it cannot detect the phishing email which contains images. However, the suggested method is capable of detecting image based on phishing attacks with high accuracy. It captures the image of a page, then it uses Optical Character Recognition (OCR) to change the picture to text, then the content of the text is analysed and finally, it uses the Google Page Rank algorithm to make a decision on the validity of the site. A tool called GoldPhish is developed which is a browser plug-in that is used to detect and report phishing sites.

**URL based phishing detectors**

URL based phishing detectors particularly used to reduce the false positive ratio of the phishing detectors. The main idea of this approach is to extract the possible domain name from the victim URL and then compare the page rank of the started domain names with the first domain. On the off chance that there is a considerable difference in the ranks then the extracted domain name will be reported as phishing. This approach based on the domain rank can effectively detect phishing because the phishing campaigns live only for a short period of time.

**Behavior model approach for testing phishing sites**

Hossain Shahriar *et al.* (2010) suggested a behaviour model-based approach for testing phishing sites. This method addresses the problem faced by the conventional phishing detector which is based on testing against aknown set of inputs and matching the actual output with the expected ones. This approach checks the behaviour of the website using a number of heuristics and then the behaviour model is characterized using a notion of the finite machine. There are totally eight different heuristics those falls into three main categories which are used to test the behaviour model. They are

**a) State-based heuristics**

**No loop (H1):** If a site navigates more than one state, it will be considered as a heuristic to demonstrate whether the site is phishing or genuine site.

**Single loop (H2):** If asks for and the comparing reactions result ina site to continue as before state more than once, a loop is framed. An experiment having a loop as for a state can speak to either a phishing or a genuine site.

**Multiple Loops (H3):** If requests and the corresponding responses results in the formation of more than one loop, then multiple loops are formed which is again used as heuristics to detect advanced attacks

**b) Response and form-based heuristics**

**Maximum form submission (H4):** A legitimate website uses a limited number of forms, whereas a phishing website is designed to accept numerous form submissions and hence maximum form submissions are used as a heuristic.

**Maximum error message (H5):** Phishing websites rarely verify the provided information for login functionality, whereas a legitimate website rejects random inputs and generates error messages in response pages. Thus some of the error messages are considered as a heuristic.

**Presence of provided input (H6):** A legitimate site regularly welcomes a client after an effective login or enrolment with the provided name, client id, or an email, while a phishing site does not create a reaction page.

**No form (H7):** This heuristic premise checks whether a casing convenience achieves a page that has no data frame.

**Common form (H8):** This premise is satisfied if a current frame being submitted with unpredictable data sources matches with any of the structures that have been submitted at some point as of late.A tool called Phish Tester is implemented and tested against 33 phishing and 19 legitimate websites and it has been found that the approach is capable of exactly detecting all phishing (zero false positives) and legitimate website (zero false negatives). However, this method is not efficient in testing phishing sites that contain embedded objects such as images and flash content

## V.CONCLUSION

The credibility of a phishing detector lies in protecting the individuals from falling prey to phishing. Obviously we cannot claim that every web users are security experts and hence a sophisticating phishing toolis required to protect the web users. The list based and heuristic based approaches, though can detect the phishing website the observed false alarm rate with this approach is quite unacceptable. On the other hand the machine learning and multi-tier classification approaches improves the detection accuracy, but it is inefficient in detecting image based phishing content. Also, when on one side ,the web users suffers privacy and economic loss ,due to the unintended disclosure of sensitive information, on the other side the phishing sites jeopardize the impersonated site which is usually a reputed organization and hence they tend to lose valuable customer and money. However, only a few researches have taken effort to discover the targeted phishing site. Recently, a more sophisticated form of phishing based on flash content is prevalent, which bye passes the strategy of most phishing. So, we propose a phishing detector, which can detect phishing content containing embedded objects and aids in target discovery. The proposed phishing tool will be designed in such a way that it will have a perfect trade-off between time complexity and detection accuracy.

## References


1. *Alaa M Riad, Hamdy K Elminir & Sameh Abd Elghany 2012, _ALiterature Review of Image Retrieval based on Semantic Concept',International Journal of Computer Applications ( 0975 – 8887), vol. 40,no. 11.*
2. *Algorithms for WebCrawlingin the proceedings of WebMedia andLAWeb, 2004.*
3. *Almpanidis, G, Kotropoulos, G & Pitas, I 2005, _Focused crawlingusing latent semantic indexing–An application for vertical searchengines', Research and Advanced Technologyfor Digital Libraries, pp.402-413.*
4. *APWG. Anti phishing working group [accessed 30.09.12],http://www.antiphishing.org; 2012.*
5. *Ardö 2005, _Focused crawling in the ALVIS semantic search engine', in2nd European Semantic Web Conference (ESWC 2005), Heraklion.*