**Phishing Detection: Analysis of Visual Similarity Based Approaches**

**Abstract:**

Phishing is one of the major problems faced by cyber-world and leads to financial losses for both industries and individuals. Detection of phishing attack with high accuracy has always been a challenging issue. At present, visual Similarities based techniques are very useful for detecting phishing websites efficiently. Phishing website looks very similar in appearance to its corresponding legitimate website to deceive users into believing that they are browsing the correct website. Visual Similarity based phishing detection techniques utilise the feature set like text content, text format, HTML tags, Cascading Style Sheet (CSS), image, and so forth, to make the decision. These approaches compare the suspicious website with the corresponding legitimate website by using various features and if the similarity is greater than the predefined threshold value then it is declared phishing. This paper presents a comprehensive analysis of phishing attacks, their exploitation, some of the recent visual Similarity based approaches for phishing detection, and its comparative study. Our survey provides a better understanding of the problem, current solution space, and scope of future research to deal with phishing attacks efficiently using visual Similarity based approaches.

**1.Introduction**

Phishing is a crime in which a perpetrator sends the fake e-mail, which appears to come from popular and trusted brand or organization, asking to input personal credential like bank password, username, phone number, address, credit card details, and so forth. The fake e-mails often look amazingly legitimate, and even the website where the Internet user is asked to input personal information also looks similar to legitimate one. Phishing messages propagate over e-mail, SMS, instant messengers, social networking sites, VoIP, and so forth, but e-mail is the popular way to perform this attack and 65% of the total phishing attack is achieved by visiting the hyperlink attached to the e-mail. Moreover, spear phishing attack is becoming popular nowadays. Business e-mail compromise (BEC) is observed as a major Internet threat in 2015. In BEC, the intruder uses spear phishing methods to fool organizations and Internet persons. More sophisticated spear phishing attacks targeted particular individual or groups within the organization. Phishing is metaphorically similar to fishing in the water, but instead of trying to catch a fish, attackers try to steal consumer’s personal information. When a user opens a fake webpage and enters the username and protected password, the credentials of the user are acquired by the attacker which can be used for malicious purposes. Phishing websites look very similar in appearance to their corresponding legitimate websites to attract large number of Internet users. Recent developments in phishing detection have led to the growth of numerous new visual Similarity based approaches. Visual Similarity based approaches compare the visual appearance of the suspicious website to its corresponding legitimate website by using various parameters. Due to different phases of phishing detection, this paper contains the following

**2.Background, History, and Statistics:**

A phishing scam has attracted the attention of both academicians and corporate researchers as it is a serious privacy and web security threat. Phishing cannot be controlled by firewalls or any encryption software.

**2.1. Brief History:**

First phishing attack was observed on America online network systems (AOL) in the early 1990s where many fraudulent users registered on AOL website with fake credit card details. AOL passed these fake accounts with a simple validity test without verifying the legitimacy of the credit card. After activation of the fake account, attackers accessed the resources of America online system. At the time of billing, AOL determined that the accounts were fraudulent, and associated credit cards were also not valid; Therefore AOL ceased these accounts immediately. After this incident, AOL took measures to prevent this type of attack by verifying the authenticity of credit card and associated billing identity, which also enabled the attackers to change their way of obtaining AOL accounts. Instead of creating a fake account, attackers would steal the personal information of registered AOL user. Attackers contacted registered AOL users through instant messenger or e-mail and asked them to verify the password for security purposes. E-mail and instant messages appeared to come from an AOL employee. Many users provided their passwords and other personal information to the attackers. The attackers then used the variously billed portions of America online website on behalf of a legitimate user. Moreover, an attacker no longer restricts themselves to masquerading America online website but actively masquerade a large number of financial and electronic commerce websites.

**2.2. Statistics:**

According to Internet world stats, total numbers of Internet users worldwide are 2.97 billion in 2014; that is, more than 38% of the world population uses Internet. Hackers take advantage of the insecure Internet system and can fool unaware users to fall for phishing scams. Phishing e-mail is used to defraud both individuals and financial organizations on the Internet. The Anti-Phishing Working Group (APWG) is an international consortium which is dedicated to promoting research, education, and law enforcement to eliminate online fraud and cyber-crime. In 2012, total phishing attack increased by 160% over 2011, signifying a record year in phishing volumes. The total phishing attacks detected in 2013 were approximately 450000 and led to financial losses more than 5.9 billion dollars. Total attack increases by 1% in 2013 as compared to 2012. The total number of phishing attacks noticed in Q1 (first quarter) of 2014 was 125,215, a 10.7 percent increase over Q4 (fourth quarter) of 2013. More than 55% of phishing websites contain the name of the target site in some form to fool users and 99.4% of phishing websites use port 80. According to the APWG report in the first quarter of 2014, second highest number of phishing attacks ever recorded was between January and March 2014 and payment services are the most targeted industry. During the second half of 2014, 123,972 unique phishing attacks were observed. In the year 2011, total financial losses were 1.2 billion, and they rose to 5.9 billion dollars in 2013. The financial losses due to phishing attack in 2014 and 2015 were 4.5 and 4.6, respectively. The growth of phishing attacks from 2005 to 2015

**2.3. Phishing Mechanism.**

The fake website is the clone of targeted genuine website, and it always contains some input fields (e.g., text box). When the user submits his/her personal details, the information is transferred to the attacker. An attacker steals the credential of the innocent user by performing following steps: Construction of Phishing Site. In the first step attacker identifies the target as a well-known organization. Afterward, attacker collects the detailed information about the organization by visiting their website. The attacker then uses this information to construct the fake website. URL Sending. In this step, attacker composes a bogus e-mail and sends it to the thousands of users. Attacker attached the URL of the fake website in the bogus e-mail. In the case of spear phishing attack, an attacker sends the e-mail to selected users. An attacker can also spread the link of phishing website with the help of blogs, forum, and so forth. Stealing of the Credentials. When user clicks on attached URL, consequently, fake site is opened in the web browser. The fake website contains a fake login form which is used to take the credential of an innocent user. Furthermore, attacker can access the information filled by the user. Identity Theft. Attacker uses this credential of malicious purposes. For example, attacker purchases something by using credit card details of the user.

**2.4. Taxonomy of Phishing Attack:**

Attacker performed the phishing attack by utilising the technical subterfuge and social engineering techniques. In social engineering techniques, attackers carry out this attack by sending bogus e-mail. Attackers often convince recipients to respond using names of banks, credit card companies, e-retailers, and so forth. Technical subterfuge strategies install malware into user’s system to steal credentials directly using Trojan and keylogger spyware. The malware also misaddresses users to fake websites or proxy servers. Attackers attached malware or embedded malicious links in the fraudulent emails and when the user opens the fraud hyperlink, malicious software is installed on the user’s system, which collected the confidential information from the system and sent it to the attacker (e.g., keylogger software sends the details of every key hit by the user). Attackers may also get remote access to victim’s computer and collect data whenever attackers want. In this paper, we focus on social engineering schemes, as it is the most popular way to steal victim’s information by phishing.

**Antiphishing Technique:**

Modus Operandi. A phishing scam starts with spreading bogus e-mail. After receiving an e-mail, Antiphishing techniques start working, either by redirecting the phishing mail in the spam folder or by showing a warning when an online user clicks on the link of phishing URL

The following steps are involved in phishing lifecycle:

Step 1. Attacker creates the fake copy of a popular organization and sends the URL of fake website to the large number of Internet users using e-mail, blog, social networking sites, and so forth.

Step 2. In the case of fake e-mail, every e-mail is first to pass through the DNS-based blacklist filters. If the domain is found in the blacklist, then e-mail is blocked before it reached to SMTP mail server. There are also various solutions available which block the fake e-mail based on structural features of mail.

Step 3. If a fake e-mail bypasses the blacklist and features based solutions and if the user opens attached link in the Email then some browser based blacklist techniques block the site at client side.

Step 4. Some other solutions like the heuristic and visual Similarities based approaches also blocked the webpage only when the browser requests for any suspicious webpage.

Step 5. If the phishing attack bypasses all the Solutions then it steals the credential of innocent users and sends it to the attacker. The attacker uses this information for financial or some other benefits.

**3. Visual Similarity Based Phishing Detection and Filtering Approaches :**

A user could become the victim of the phishing attack by looking the high visual resemblance of phishing website with the targeted legitimate site, such as page layouts, images, text content, font size, and font colour. The fake and genuine webpages of PayPal are shown in Figure 6, and both pages have same visual appearance but different URLs. It is not always necessary that the people carefully notice on URL and SSL (Secure Socket Layer) certificate of websites. If an attacker does not copy the visual appearance of targeted website well, then chances of inputting credentials by Internet users are very less.

An attacker fools the user by the following ways:

**(1)** Visual Appearance. The phishing website looks similar to its legitimate website. Attackers used to copy the HTML source code of genuine website to build the fake website.

**(2)** Address Bar. Attackers also cover the address or URL bar of website by script or image. The user would believe that they are inputting information on the right website.

**(3)** Embedded Objects. Attackers use embedded objects (images, scripts, etc.) to hide the textual content and HTML coding from the phishing detection approaches.

**(4)** Favicon Similarity. Favicon is an image icon associated with the particular website. An attacker may copy the favicon of targeted website. If the favicon shown in the address bar is other than the current website, then it is considered as a phishing attempt.

Dhamija et al. conducted a survey on various participants to identify whether a website is phishing or genuine. Participants were unable to identify 90% of phishing sites. Many participants wrongly judged the site on the basis of their text content and visual appearance. They also found that even an experienced user could also be fooled by the visual appearance of a fake website, and 23% of the users do not look at the address bar of a website. Therefore , we can say that if the appearance of a phishing site is similar to its legitimate one and domain is different then also users can easily be trapped by the attackers.

**6. Open Issues and Challenges:**

Various types of Anti-phishing techniques based on visual similarity approach have been given in the literature. However, still there is no single technique that can detect all types of phishing attacks (i.e., zero-hour phishing attack, embedded objects, DNS poisoning, etc.). Day by day phishing attack is increasing continuously and becomes the most popular e-crime. Consistently, when researchers design a new technique to control phishing attack, attackers change their way to perform attack or exploit the vulnerability in the solution. Hence, there is the tight race between attackers and Anti-phishing developers. There are various issues which have to take care while designing a new antiphishing technique. The first problem is the zero-hour phishing attack. Most of the antiphishing techniques compare the suspicious website from the pool of legitimate sites using feature set including URL, keyword, and visual appearances. These techniques required a large dataset and still fail to detect zero-hour phishing attack. If attacker designs a new webpage and its target (corresponding legitimate page) is not available in the dataset, then technique fails to detect new fake webpages (zero- hour attack). Liu et al. Presented a technique which can detect zero-hour phishing attack; However this technique depends on the TF-IDF algorithm and hyperlinks. Therefore, detection of zero-hour phishing attack with high accuracy is still an open challenge. The second issue is the language independence. Various text languages are worldwide used in the websites, and the ecommerce and banking websites also have different text languages in various countries for example, Amazon, eBay, and Citibank. The layout of e-commerce and banking sites is almost similar in different languages. Heuristics based phishing detection Techniques use the keywords, and they are language dependent. As we discussed, some of the visual Feature based techniques can detect this attack because they utilise the webpage features like the logo of the company, CSS Structure, DOM tree, and so forth. Such techniques only detect the attack if the layout of phishing website is similar to the real one. However, these techniques are unable to detect a new phishing attack (zero-hour) because they compare the current website with the stored database. The third issue is the embedded objects present in the webpage as attackers use images, JavaScript, and so forth, to bypass the antiphishing system. As we discussed, image Processing based techniques can detect the embedded objects present in suspicious webpage because these techniques take the snapshot of the webpage and compare it with the corresponding legitimate webpage. But identifying the correct corresponding legitimate webpage is the major problem in image Processing based solutions. Image Processing based approaches also consumed a lot of time to compare a suspicious website with the pool of websites. Therefore detection of phishing site which uses embedded objects is still an open challenge. The fourth issue is determining an appropriate threshold to take appropriate decision. The threshold is the matching score between two websites. As we discussed, attacker constructs a phishing website which looks similar to legitimate one. If the phishing website is partially copied (less than 50%) from the legitimate website, then none of the visual similarity based approach can detect it. Therefore, adjusting the appropriate threshold to detect a maximum number of phishing websites is a challenging task. If antiphishing system increases the threshold then the false negative rate increases and if it decreases the threshold then false positive rate increases. A good antiphishing system requires that both false negative and false positive rate should be as minimal as possible.

**7. Conclusion:**

Phishing is an appalling threat in the web security domain. In this attack, the user inputs his/her personal information to a fake website which looks like a legitimate one. We have presented a survey on phishing detection approaches based on visual similarity. This survey provides a better understanding of phishing website, various solution, and future scope in phishing detection. Many approaches are discussed in this paper for phishing detection; however most of the approaches still have limitations like accuracy, the countermeasure against new phishing websites, failing to detect embedded objects, and so forth. These approaches use various features of a webpage to detect phishing attacks, such as text similarity, font colour, font size, and images present in the webpage. Text based similarity approaches are relatively fast, but they are unable to detect phishing attack if the text is replaced with some image. Image processing based approaches have high accuracy rate while they are complex in nature and are time-consuming. Furthermore, most of the work is done offline. These involve data collection and profile-creation phases to be completed first. A comparative table is prepared for easy glancing at the advantages and drawbacks of the available approaches. No single technique is enough for adopting it for phishing detection purposes. Detection of phishing websites with high accuracy is still an open challenge for further research and development.

**References**

[1] M. Khonji, Y. Iraqi, and A. Jones, “Phishing detection: a literature survey,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091–2121, 2013.

[2] R. Islam and J. Abawajy, “A multi-tier phishing detection and filtering approach,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 324–335, 2013.

[3] A. K. Jain and B. B. Gupta, “Comparative analysis of features based machine learning approaches for phishing detection,” in Proceedings of the 10th INDIA-COM, New Delhi, India, 2016.

[4] G. Weaver, A. Furr, and R. Norton, Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-Day Phishing Attacks on Universities, 2016.

[5] Kaspersky Lab, “Spam in January 2012 love, politics and sport,” 2013, http://www.kaspersky.com/about/news/spam/ 2012/Spam in January 2012 Love Politics and Sport.

[6] APWG Q1-Q3 Report, 2015, http://docs.apwg.org/reports/ apwg trends report q1-q3 2015.pdf.

[7] B. Parmar, “Protecting against spear-phishing,” Computer Fraud & Security, vol. 2012, no. 1, pp. 8–11, 2012.

[8] W. Jingguo, T. Herath, C. Rui, A. Vishwanath, and H. R. Rao, “Phishing susceptibility: an investigation into the processing of a targeted spear phishing e-mail,” IEEE Transactions on Professional Communication, vol. 55, no. 4, pp. 345–362, 2012.

[9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” Communications of the ACM, vol. 50, no. 10, pp. 94–100, 2007.

[10] C. H. Hsu, P. Wang, and S. Pu, “Identify fixed-path phishing attack by STC,” in Proceedings of the 8th Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS ’11), pp. 172–175, ACM, Perth, Australia, September 2011.

[11] N. A. G. Arachchilage and M. Cole, “Designing a mobile game for home computer users to protect against phishing attacks,” https://arxiv.org/abs/1602.03929.