International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
http://ijcjournal.org/

A Survey on Phishing Attacks in Cyberspace

Marran Zabin Aldossari*

The University of North Carolina at Charlotte, Charlotte, North Carolina, USA
Shaqra University, Riyadh, Saudi Arabia
Email: maldossari@su.edu.sa

Abstract

Phishing is a type of cyber attack in which cybercriminals use various advanced techniques to deceive people, such as creating fake webpages or malicious e-mails. The objective of phishing attacks is to gather personal data, money, or personal information from victims illegally. The primary aim of this review is to survey the literature on phishing attacks in cyberspace. It discusses different types of phishing attacks, such as spear phishing, e-mail spoofing, phone phishing, web spoofing, and angler phishing, as well as negative consequences they may cause for people. Phishing is typically carried out through different delivery methods such as e-mail, phone calls, or messaging. Victims of phishing are usually either not sensitive to privacy protection or do not have enough knowledge about social engineering attacks to know they are at risk. In addition, this paper introduces different methods for detecting phishing attacks. The last section discusses certain limitations of existing studies on phishing detection and potential future research.

Keywords: social network attacks; spear phishing; angler phishing; phishing detection.

1. Introduction

Social networking sites are online platforms that allow people to engage in social relationships with others by using various means such as e-mails, messaging, or phone calls. Social networking sites have become an important part of people's daily lives and play significant roles in social and business interactions. At the same time, they pose many privacy and security risks to users, because social networking exposes various kinds of personal information to the public [1]. As the popularity of social networking grows, so does its attractiveness to criminals who seek to make illegal financial earnings or sometimes merely to have fun. These activities are known as phishing attacks. The term 'phishing' refers to technological methods of deceiving people by using e-mails, messaging, or phone calls. Phishing practices are defined as acts that attempt to obtain critical and sensitive information such as personal identification information, usernames, bank accounts, credit card details, and passwords [2]. Phishing is a kind of online identity crime that is correlated with both social engineering and technical tricks [3].

---

* Corresponding author.

Spoofing is one of the oldest types of cyber-crimes and one of the most common ways of stealing information from people. The result of a recent study at Queens University suggests that there has been a 500% increase in phishing attacks since the fourth quarter of 2016 [4]. Although some phishing attacks are complex and beyond the capability of general users to prevent or detect, most attacks typically occur in simple user interactions, such as downloading software from unknown sources or clicking on a hyperlink. Attackers apply phishing techniques to lure victims into engaging in behavior that leaves them compromised. The user is often the weakest link in the security chain [5]. Furthermore, it is difficult for people to take actions against phishing because phishing may not present itself as a malicious activity to the victim.

Table 1: The amounts of financial loss in recent years.

Year	Amount of Financial Loss	Number of Reported Phishing Incidents
2016	373,860.00	24,925
2017	810,224.00	26,386
2018	933,470.00	24,291

As presented in Table 1, the Australian Competition and Consumer Commission (ACCC) reported increasing amounts in annual financial loss due to phishing. The Federal Bureau of Investigation (FBI) reported a $12.5 billion loss incurred by companies in the U.S. between October 2013 and May 2018 due to phishing e-mails, which demonstrates that phishing attacks are a serious problem [6,7].

The primary objective of this research is to examine different types of phishing, such as spear phishing, e-mail spoofing, phone call phishing, web spoofing, and angler phishing, phishing strategies, current anti-phishing solutions, and potential issues for future research.

A. Data collection methods

This survey was developed based on a literature search using the following international databases: ACM digital library, Google Scholar, IEEE digital libraries, and Science Direct. The researcher used different combinations of search keywords, such as phishing attacks, social network attacks, deceptive phishing, cybercrime, social media threats, and phishing detection. Other resources include journals such as Usable Security and Privacy, Security and Privacy, Human-Computer Interaction, and Computers in Human Behavior as well as several other conference proceedings. In order to reflect the state-of-the-art, this paper focuses on relevant studies that were published in the past five years. A total of 24 academic papers were identified as relevant to the survey topic.

2. Different types of phishing

Phishing attacks can be carried out by different techniques that deceive a victim into disclosing his or her private information. Phishing can be categorized into five types based on delivery method. These methods include 1) spear phishing, 2) e-mail spoofing, 3) phone call phishing, 4) web spoofing, and 5) angler phishing.

A. Spear phishing

A spear phishing attack targets at specific individuals or departments within an organization rather than attacking a broad group of people [6]. Symantec has reported that 91% of cyberattacks start with a spear phishing e-mail [7]. An example of spear phishing is the use of an organization's information and spoofed addresses to send e-mails to specific individuals so that those e-mails appeared to come from a known source, such as co-workers. A recent study at New York University [8] used a real-world spear-phishing e-mail attack on a group of company employees in order to examine how users' personalities and attitudes affected their tendency to expose themselves to such an attack. Of the 40 participants, 32.5% clicked on the phishing link, while 30% clicked on the 'download plug-in' button that was attached to the e-mail [8].

B. E-mail spoofing

It is a phishing attack in which an attacker impersonates someone that the victim knows or trusts [9]. In general, e-mail spoofing refers to sending an e-mail with fake content by using someone else's identity. Fig. 1 presents an example of a spoofing e-mail sent to a Gmail account requesting that the user reset a PayPal password. This example looks like an authentic e-mail [10]. Each day, increasing numbers of e-mails are sent with an aim of making online users believe that they are legitimate and from trusted institutions or sources [11]. The main strategy of e-mail spoofing is to create a sense of urgency, for example, by telling victims that they have failed to log into their account too many times, and must verify their account details [11,12]. E-mail phishing engages victims via e-mails and leads them to a phishing website.

C. Phone phishing

Phone phishing uses social engineering through phone calls to gather sensitive and private information from individuals for financial gain. The use of phone phishing has been increasing in the past two years [14, 15]. One example of a phone phishing scam carried out via social networks is when phishers call potential victims, offering them a very low-cost travel package for an upcoming vacation and asking them for their credit card number in order to hold the offer [14]. Another example is when phishers call potential victims and tell them that they have been randomly selected to win a monetary prize due to their participation in an online survey via Twitter. If the victims are interested in claiming the prize, they must first provide personal information such as name, mobile number, address, and bank account number.

D. Web spoofing

It is another type of phishing attack, which involves tricking people into connecting to a web server to which they did not intend to connect. The attacker can trick a victim by creating a fake website that looks like a legitimate site by copying the front-end code. Only a small amount of web programming is required to redirect users' inputs into phisher files or databases [10]. Moreover, many of the attackers use free hosting sites. A report from PhishLabs has reported that the number of free hosting domain providers has increased over the past four years; from just 3% in 2015 to 13.8% in 2018 of the total phishing volume [15]. Furthermore, malicious links to fake websites are usually embedded in phishing e-mails or advertisements [13].

E. *Angler phishing*

It is the practice of masquerading as a customer service account of social network sites [16]. An angler phisher tries to reach and deceive consumers by creating a fake brand support page on social network sites in order to redirect victims to phishing websites that look like legitimate webpages. According to recent reports, approximately 55% of such attacks in 2017 targeted clients of financial services companies [15,17]. The primary purpose of the attackers was to lure victims into providing sensitive information or account credentials [17]. A previous study from Phsihmelab reported that 66% of the users of social network sites did not know how to deal with privacy control, making it easy for them to be victimized by such attacks [4]. A recent report from Fraud Watch indicated that the amount of angler phishing on social media was on the rise, having demonstrated a 1,100% increase from 2014 to 2016. Many victims of those Angler phishing incidents involved well-known brand names such as Amazon, Nike, and Samsung [18].

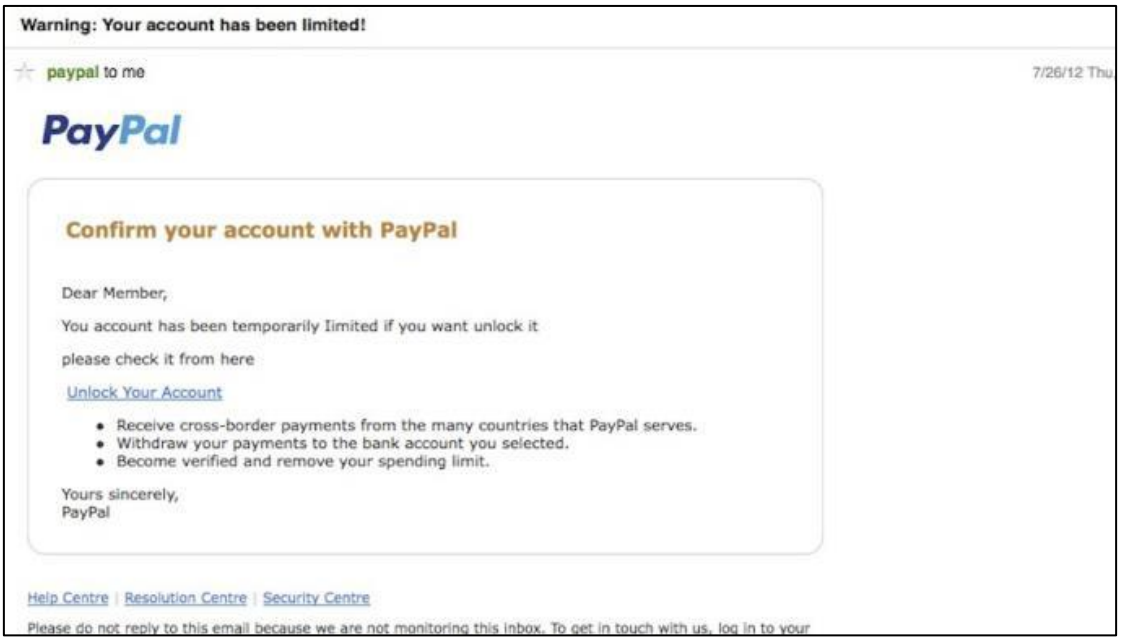

Figure 1: A fake e-mail that appears to be from PayPal, but is generated by command lines of UNIX system.

An example of how this kind of angler phishing is carried out is when a criminal creates a fake customer service account across different social media platforms and makes that account look very similar to that of a real business [19]. Later, when someone tweets to his or her bank asking questions, the imposter account replies to that message with what seems like an authentic answer. The imposter then asks the client to follow the fake link provided in that message, saying it is to ensure that the client is one of the bank's actual customers and to ensure the client was satisfied. In reality, this link redirects the victim to the criminal's website, so the criminal can steal the victim's credentials. Fig. 2 below illustrates how angler phishing works.

Figure 2: A fake bank customer service account that appears to be from Twitter, but redirects customers to a fake webpage [19].

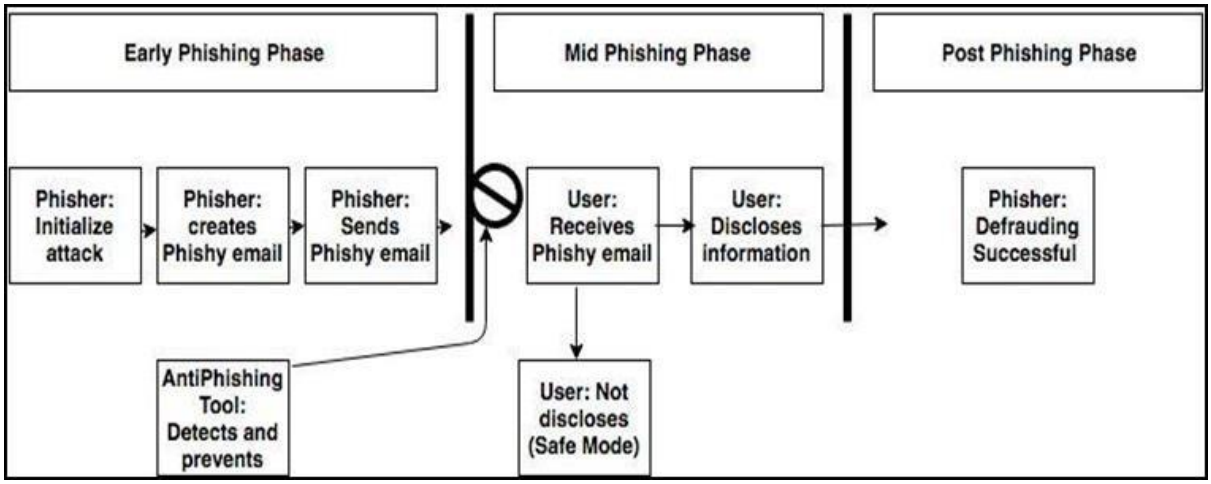

Figure 3: Phishing life cycle process [20].

Figure. 3 presents an overview of the phishing cycle process. A phishing attack starts with criminals sending a phishing e-mail or a fake reply to a client tweet with a malicious link that appears to the users as authentic content. If phishing passes phishing detection and the user begins his or her response and discloses private information, then phishing is successful.

In summary, criminals can use a number of delivery methods to reach out to victims and deceive them with the use of certain techniques. The primary goal of these criminals is to gather private and sensitive information

about a user.

3. Phishing detection

Phishing detection is a challenging task, although many researchers have been seeking effective solutions to detecting phishing and reducing its impact on victims. However, phishing is becoming more complex and effective. For example, the use of logos in deceptive e-mails makes these e-mails more persuasive to recipients [21]. Researchers have proposed two approaches or techniques to detect phishing attacks: manual phishing detection and automatic phishing detection.

3.1. Manual phishing detections

Manual phishing detection involves human beings detecting phishing attacks manually. Human detection is important for safeguarding important information from intruders. However, the lack of sufficient knowledge, skills, and awareness when it comes to phishing and phishing detection is a challenge faced by manual methods. Educating users how to identify phishing attacks is very important. Several ways have been proposed to deliver the necessary knowledge about phishing detection to users [24-27], such as Mobile game prototypes Anti-phishing Phil, NoPhish, and PhishGuru.

3.1.1. Mobile game prototype

The first type of manual phishing detection is a mobile game prototype used as an educational tool that could help computer users to protect themselves from phishing attacks. The main goal of this tool is to increase users' ability to avoid phishing by motivating them to protect themselves against phishing attacks. Specifically, the game teaches users how to distinguish legitimate URLs from phishing ones. Nalin and his colleagues conducted a study using the think-aloud protocol, together with a pre- and post-test with 20 participants [22]. The main goal was to observe their understanding, knowledge, and awareness of phishing attacks via the mobile game prototype. The results indicated an improvement in accuracy - those who played the mobile game achieved average scores of 56% in the pre-test and 84% in the post-test [22].

3.1.2. Anti-Phishing Phil

Anti-Phishing Phil is another format of training on how to manually detect phishing. It is an online game that utilizes learning science principles and teaches users habits for avoiding phishing attacks. This training involves sessions that include playing the game, reading an anti-phishing tutorial, and reading existing online training materials. The objective of Anti-Phishing Phil is to teach users three ways to detect phishing scams: 1) how to identify phishing URLs, 2) how to check trustworthy or untrustworthy sites in web browsers, and 3) how to use search engines to find legitimate sites. A study undertaken by Sheng and his colleagues detected that 14% of participants in the pre-test looked at the address bar when evaluating before playing the game, while in the post-test, 41% of participants evaluated the web site URL after playing the game [24].

3.1.3. NoPhish

Another training format that teaches users how to manually detect phishing is NoPhish. This training uses instructor-based lessons that provide users with general information about phishing and with the possible results of phishing attacks to indicate the risks and explain how a URL is structured. In the study by Simon and his colleagues [25] the training was given to the participants then openly discussed with the audience. The results demonstrate that training led to a significant improvement in participants' ability to detect phishing and identify legitimate webpages.

3.1.4. PhishGuru

It is another format that educates users to detect phishing manually. A recent study by Jason has developed an embedded training system by sending simulated phishing e-mails to teach users how to avoid such attacks [23]. If users fall victim even once, they see an intervention that teaches them about phishing attacks and how to avoid them, by providing immediate feedback and tips. The main goal of the study was to increase users' security awareness [23]. Alexandra and his colleagues have found that PhishGuru material reduced the end-users' risk of providing sensitive information on phishing webpages by 40% [26].

In summary, user education remains the most effective way to educate users, since they are the most vulnerable link in any security measures. Thus, while training and educational games can help users detect phishing better, they cannot simulate instances of real-life phishing sufficiently. Some studies have noted that such learning opportunities have limitations in terms of real-life applicability, such as small sample sizes, and the fact that participants provided answers they believed were expected, since they knew it was a study. Many users could not differentiate between phishing and legitimate sites [23, 28]. Therefore, there is a need for a unique education program to train employees and K-12 students in to how to identify and avoid all these types of phishing. To overcome these limitations, researchers have developed a new approach, namely automatic phishing detection.

3.2. Automatic phishing detection

Attackers take advantage of human curiosity, lack of knowledge to manipulate their victims. Due to the challenges and limitations of manual phishing detection, there is an increasing number of approaches to automatic phishing detection that have been proposed to help individuals, companies, and organizations protect potential or existing customers from fraud, protect one's reputation, and avoid blackmail, financial loss, and identity theft [27]. Thus, as the internet grows in scale, automatic phishing detection is essential to provide end-users with timely protection. Automatic phishing detection can be categorized into four types based on the techniques they use, including blacklist, hybrid features, visual similarity, and heuristic approach. An overview of each approach is presented below.

3.2.1. Blacklist approach

The blacklist approach is a technique for automatic phishing detection that maintains a list of known malicious website URLs in a dataset. When a person visits a specific URL, the web browser sends the site information to

the blacklist database and compares the value of the URL with values from a malicious dataset, which determines whether the URL is already existing in the blacklist database [28].

This technique establishes whether a website is legitimate or not. An example of a search engine blacklist is Google Safe Browsing and Site Advisor. The main challenge with this kind of technique is that blacklists cannot cover all phishing websites. Therefore, it will not be able to detect any new phishing website that is not currently included in a blacklist [29].

3.2.2. Hybrid features approach

The hybrid features approach is another kind of automatic e-mail phishing detection. It analyzes certain features such as e-mail header structure, e-mail URL information, e-mail script function, and e-mail psychological features before making a judgment. Example of these features extracted from emails [30] include blacklist words in the title, the number of "%" characters or "@" symbols in a URL, and the number of domains. The approach uses the Support Vector Machine (SVM) classifier in order to detect any phishing e-mails. Phishing attacks deceive people primarily by using the recipient's psychological weaknesses, such as curiosity, trust, anxiety, and other psychological traps. Thus, the hybrid features approach is able to detect some of these psychology-related words.

3.2.3. Visual similarity approach

The visual similarity approach is a kind of phishing detection that works based on effective cascading style sheet (CSS) features of web pages. This approach extracts features from web pages, and identifies the similarity between the phishing pages and the legitimate webpages. Visual similarity has three main steps for detection: extracting and representing effective CSS features, computing similarity scores by using the DOM tree algorithm, and detecting phishing pages. It uses 9,307 real-world phishing web pages collected from PhishTank to test this approach.

3.2.4. Heuristic approach

The heuristic approach is an automatic method for phishing site detection that uses certain features that URL contain. The proposed approach in [31] extracted 26 URL-based features from URLs and used those features to determine whether a site was a legitimate or phishing site. This technique uses a number of machine learning algorithms, such as support vector machine (SVM), naive Bayes, and decision tree.

In summary, these proposed techniques could improve phishing detection, protect personal information, and reduce damage caused by phishing attacks without any involvement of users. However, some proposed techniques have limitations, as illustrated in the next section.

Table 2: Pros and cons of educational tools.

Tool name	E-mail	Website	URL	Pros	Cons	Sample Study Result
Game prototypes			X	All participants believed that the mobile game prototype was somewhat effective in teaching how to distinguish good URLs from bad ones.	Limited display size of the mobile phone might have caused a problem for participants, especially those with visual impairment.	Participants who played the mobile game scored 56% in the pre-test and 84% in the post-test. The study results demonstrated a significant improvement of participants' phishing avoidance behavior in their post-test assessment
Anti-Phishing Phil		X	X	Uses learning science principles; effectiveness demonstrated	Real-life applicability low	The researchers found that those who played the game were better able to detect fraudulent websites, compared to those who did not play the game
NoPhish		X	X	Effectiveness demonstrated	Real-life applicability low	Participants who used NoPhish were more effective in detecting phishing URLs, particularly over a longer period of time, than those who did not use it.
PhishGuru	X	X		Users learn by doing. Immediate feedback	Few participants who completed all the three conditions. Participants were careless and talked among themselves during training.	This approach led to a 45% reduction in falling for phishing even a month after being trained.

Table 3: Pros and cons of automatic phishing detection techniques.

Tool name	E-mail	Website	URL	Pros	Cons
Blacklist			X	Enhances performance	Time consuming. Slow speeds at which the blacklists approach updates. Cannot cover all phishing websites, because a recently created fake website takes considerable time before it is listed in database
Hybrid Features	X		X	Enhances performance	Small sample test. Limited psychological keywords in dataset.
Visual Similarity	X		X	High detection rate	Takes a long time to compare CSS properties. Some authentic websites are detected as phishing sites.
Heuristic		X	X	Able to detect new and temporary phishing sites. High accuracy. Can detect phishing websites that couldn't be detected by a blacklist approach.	Time consuming. URLs can only provide limited information to examine.

4. Limitations of existing studies and future research

It has been almost 30 years since the first phishing attacks were recognized in early 1990. Diverse solutions have been developed by researchers with an intention to minimize the impact of phishing attacks, but whenever a solution to overcoming these vulnerabilities is proposed, phishers find some weaknesses of that solution. Thus, most of the proposed approaches have limitations such as being time-consuming, failing to detect new phishing attacks, failing to include HTML and JavaScript of web pages to detect phishing, and lacking accuracy.

4.1. Blacklist approach limitations

Possibly the main limitation of this approach is that it is time-consuming, due to the slow speeds at which the blacklists update. As a result, the system takes a lot of time to present its results. Even though phishing sites have an average lifetime of a few days or several hours, the updating process of blacklists can be slow because of the long steps it takes to access the web pages. Furthermore, it has been demonstrated that certain safe sites are falsely included in the blacklists. Moreover, the blacklists cannot cover all phishing websites, since a recently created fake website takes considerable time before being listed in database. As a future direction, expanding the database size and designing effective infrastructure would help keep the database up to date by deleting any website that has been removed from the web and by detecting any new phishing website. Future work should concentrate on ways to measure the effect of adding user training based on software mistakes.

4.2. Hybrid features approach limitations

There are a number of limitations to this approach. For example, the psychological features dataset has limited keywords, which leads to potentially open questions such as: If the recipient's psychological keywords database is increased, will it detect e-mail phishing more effectively? Another limitation is a small sample used to test the approach; researchers selected only 500 phishing e-mails and 500 legitimate e-mails. They used 60% of the dataset for training purposes and the remaining 40% for testing purposes.

4.3. Visual similarity approach limitations

This approach has certain key limitations. One is that detecting phishing based on CSS rules may have an influence on accuracy, because some authentic websites are detected as phishing sites. Another challenge is that this approach is time-consuming - it takes a lot of time to compare CSS properties such as color, font-size, font-family, and border of the webpage elements with authentic page. False-negatives have demonstrated that certain authentic websites are sometimes identified as phishing sites.

Possible future directions for research to solve these limitations pose some interesting questions. For example, how can this approach match images that have been rotated, and what techniques need to be implemented to prevent manipulation of images by attackers?

4.4. Heuristic approach limitations

The main limitation of this technique is that it is time-consuming due to the large number of features it contains. This technique needs more time to generate classifiers and perform classification. The second challenge with regard to this approach is that URLs can provide only limited information as indicators of phishing, which influences the phishing detection accuracy result. In some cases, the URL can remain the same, and the content of the site can be changed. This challenge could be overcome by including HTML and JavaScript features of webpages to obtain more accurate results than those of URL-based features.

Future research should carefully consider the potential implications of the following questions: What

mechanisms can reduce the number of predictive features and improve phishing detection performance? What tools should be put in place to lower false positive rate? How can other features of JavaScript and HTML be incorporated in order to enhance performance?

In summary, it is still difficult to prevent these kinds of attacks. These limitations and challenges should encourage researchers to design more effective and self-adaptive systems to overcome these vulnerabilities.

5. Conclusion

Phishers have come up with new methods to deceive their victims and obtain information such as usernames, passwords, and credit card information. They may also redirect users to fake web pages. Phishing attacks can make use of different techniques to deceive victims into disclosing private information. Phishing has been a threat in the cyber world for many decades, and it is still a threat today. Phishing practices are one of the most popular security challenges, particularly as they continue to make copies of legitimate sites. There are different types of phishing, all of which aim to steal sensitive data for financial gain, blackmail, or other purposes. However, most of the anti-phishing techniques face certain limitations. In order to reduce phishing attacks, more effort is required from researchers to increase user awareness and make victims less susceptible.

References

[1] S. Ali, N. Islam, A. Rauf, and I. U. Din, “Privacy and Security Issues in Online Social Networks,” J. Futur. Internet, pp. 1–12, 2018.

[2] P. Simulation and A. Module, “A literature survey on social engineering attacks: Phishing attack,” Int. Conf. Comput. Commun. Autom., pp. 537–540, 2016.

[3] D. Zhang, Z. Yan, H. Jiang, and T. Kim, “A domain-feature enhanced classification model for the detection of Chinese phishing e-Business websites,” Inf. Manag., vol. 51, no. 7, pp. 845–853, 2014.

[4] D. N. C. Louise O’Hagan, Prof. Vincent Cunnane, “Angler phishing: criminality in social media,” ECSM 2018 5th Eur. Conf. Soc. Media, no. Limerick Institute of Technology, 2018.

[5] Abbasi, F. M. Zahedi, and Y. Chen, “Phishing Susceptibility : The Good , the Bad , and the Ugly,” Conf. Intell. Secur. Informatics, no. 2, pp. 169–174, 2016.

[6] Benishti, “Devastating phishing attacks dominate 2017,” Haymarket Media Group, 2017. [Online]. Available: https://www.scmagazineuk.com/article/1474174. [Accessed: 26-Jul-2019].

[7] Symantec, “Website security threat report,” 2015.

[8] T. Halevi, N. Memon, and O. Nov, “Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks,” Ssrn, 2015.

[9] Hu and G. Wang, “Revisiting Email Spoofing Attacks,” Cornell Univ., 2018.

[10] S. S. Junxiao Shi, “Phishing,” pp. 1–14, 2012

[11] R. G. N, “A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing A!acks,” Master Diss., 2018.

[12] M. Jone, “Scam calls on the rise! 95% of people have been targeted in past six months,” Komando.com, 2017. [Online]. Available: https://www.komando.com/happening-now/408294/scam-

calls-on-the-rise-95-of-people-have-been-targeted-in-past-six-months.

[13] Kumar, "Best Plan to Protect Against Phone Phishing Attack," Am. J. Comput. Sci. Inf. Technol., vol. 3, no. 5, pp. 167–172, 2015.

[14] Kumar, "Best Plan to Protect Against Phone Phishing Attack," Am. J. Comput. Sci. Inf. Technol.

[15] J. L. P. F. and CTO, "2019 phishing trends and intelligence report," 2019.

[16] M. Jakobsson, "The Human Factor in Phishing What Will Consumers Believe ?," pp. 1–19.

[17] E. Velasquez, "What Is Angler Phishing and How Can You Avoid It?," Experian Inf. Solut. Inc, 2018.

[18] F. International, "Angler Phishing: The Risks and Dangers of Fake Social Media Brand Profiles – Part 1," 2017.

[19] Proofpoint, "Angler Phishing Protection," 2018.

[20] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Expert Systems with Applications Phishing detection based Associative Classification data mining," Expert Syst. Appl., vol. 41, no. 13, pp. 5948–5959, 2014.

[21] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, "Phishing attacks and defenses," Int. J. Secur. its Appl., vol. 10, no. 1, pp. 247–256, 2016.

[22] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," Comput. Human Behav., vol. 60, pp. 185–197, 2016.

[23] J. Hong, "The state of phishing attacks," Commun. ACM, vol. 55, no. 1, p. 74, 2012.

[24] S. Sheng et al., "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish," SOUPS '07 Proc. 3rd Symp. Usable Priv. Secur., pp. 88–99, 2007.

[25] S. S. B et al., "Teaching Phishing-Security: Which Way is Best?," Int. Fed. Inf., vol. 428, no. Springer International Publishing Switzerland 2016, pp. 135–149, 2016.

[26] Kunz, M. Volkamer, S. Stockhardt, S. Palberg, T. Lottermann, and E. Piegert, "NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks," p. 509, 2016.

[27] Vayansky and S. Kumar, "Phishing – challenges and solutions," Comput. Fraud Secur., vol. 2018, no. 1, pp. 15–20, 2018.

[28] Y. Zhu, J. He, Y. Heights, and C. Science, "Social Phishing," Commun. ACM 50, pp. 1–7, 2018.

[29] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," *Comput. Sci. Rev., vol. 17, pp. 1–24, 2015.*

[30] Z. Yang, C. Qiao, W. Kan, and J. Qiu, "Phishing Email Detection Based on Hybrid Features," IOP Conf. Ser. Earth Environ. Sci., vol. 252, p. 042051, 2019.

[31] J. Lee and D. Kim, "Heuristic-based Approach for Phishing Site Detection Using URL Features," *Adv. Comput. Electron. Electr. Technol., pp. 131–135, 2015.*