The initial socio-technical solution for phishing attack

Abdullah Fajar and Setiadi Yazid

University of Indonesia, Depok Indonesia

abdullah.fajar@ui.ac.id; setiadi@cs.ui.ac.id

Abstract. A phishing attack remains popular among security attacks, which has specific characteristics. The attacks have an impact on the economy and involve user behaviour that makes the attack successful. Many solution framework and program has developed but fails for eliminating the attack except minimizing the impact only. Mitigating and cope processes for reducing phishing attacks involve user education and training to raise higher user awareness. The mitigating process itself has two main steps that are prevention and detection. Many algorithms employ machine learning to overthrow the attack intelligently. The remaining problem of this process is detection time is slower than using blacklist filtering. The paper review social and technical aspects to conclude and identify the potential solution that will be proposed for the next stage of the research. The potential solution will include future data analytics such as an immersive and augmented analytic regardless of computing issues. An immersive and augmented analytics should have the ability to learn from the past data of user and attack behaviour to direct the system and user in combating the attacks. The learning result should give preventive suggestions and evaluate user awareness level.

1. Introduction
Verizon Data Breach report in 2018[1] reports that social engineering attacks using phishing techniques, the attack ties up top three for information security incidents and data breaches. The report believes that the attack is one of the most important topics in information security for several years ahead. Tracing Phishing attack is difficult since it does not present itself as a persistent threat. Today the information security process in the online community is very challenging. The phishing attack is the oldest and easiest method for stealing information. This action addressed for obtaining more personal details.

This paper proposes a solution framework based on comprehensive aspects that involve technical and social approaches. Social Engineering attacks will continually appear in line with technological changing as an open problem. The complexity of the attack requires re-formulation an updated approach to minimize adverse impact.

The next section will discuss the conceptual review that covers technical solutions, economic aspects, and comprehensive solution framework. Later the paper cover discussion of phishing detection and prevention that reviews advance detection that considers user behavior to detect a phishing attack. The final part of this section explains the avoidance and preventive mechanism. The description covers user education and training to raise higher user awareness of phishing attacks through gamified and interactive programs. The paper discusses the solution challenge that includes an intelligent method using machine learning and future data analytics. The last section resumes and describes further work direction for the author or other interested parties.
2. Conceptual review

2.1. Technical solution approach
Technically, social engineering attacks solution consists of prevention and detection stage. Vayanshi and Kumar [2] initiate the framework of circular solutions that described those stages. The prevention stage includes the practice of blocking malicious sites and filtering emails. The detection stage includes enumerating indications of malicious content in a web browser, verification, and certification of systems that are safe from harmful content.

The latest review from two security scientist groups (Aakansha et al. [3] and Nalin & Kostas[4]) has described in their work regarding attacks technique and taxonomy of defense. For comparison, both reviews describe that phishing technique as Figure 1. Referring to Figure 1, Nalin & Kostas use the terms Subterfuge while Aashanka et al. employ the term Malware Based on the distribution of phishing techniques other than social engineering. The grouping of phishing techniques is appropriate to be adopted by Nalin & Kostas. In a broader perspective, Aashanka et al. define another approach of phishing technique.

![Phishing technique](Image)

Even so, the results of the second review show that Aashanka et al. discussed the defense mechanism also while Nalin & Kostas did not. The Defense Mechanism Taxonomy from Aakansha et al. described as follows.
Phishing is difficult to trace or defend against since it does not present itself as obviously malicious. In today’s society, there is a potential risk for the safety of personal credentials when everything put online. Technical protection of phishing may cover website and email protection. Phishing employed for obtaining a wide range of personal details. Anti Phishing Working Group has defined phishing protection described as the figure below.

**Figure 2.** Taxonomy of defense against phishing attacks[3].

According to a report by The Radicati Group[5], there was an average of 269 billion emails sent per day during 2017. There are about 3.1 million emails sent every second of every day. Those many parts of emails believed are phishing. Those parts are the most dangerous of the four main vectors, as stated by Hadnagy[6]. Data breaches are the main objective of phishing. The objective action remains in top 3 positions as released by Verizon[1] in 2018 Data Breach Investigations Report.

Konradt et al. [7] and Cho et al. [8] have analyzed the economic impact of cybercrime perpetrators. They resume economic analyses application able to direct a deeper understanding of cybercrime. Later, the application determines how to cope with cybercrime effectively. Furthermore, it could gain more insight from the behavior of cybercrime perpetrators. This knowledge used to analyze the effectiveness of countermeasures. The conclusion state countermeasures are effective when they aim at the revenue stream of cybercrime attackers.

**Figure 3.** Anti phishing prevention and detection techniques.

2.2. **Social and economic aspect consideration**

According to a report by The Radicati Group[5], there was an average of 269 billion emails sent per day during 2017. There are about 3.1 million emails sent every second of every day. Those many parts of emails believed are phishing. Those parts are the most dangerous of the four main vectors, as stated by Hadnagy[6]. Data breaches are the main objective of phishing. The objective action remains in top 3 positions as released by Verizon[1] in 2018 Data Breach Investigations Report.

Konradt et al. [7] and Cho et al. [8] have analyzed the economic impact of cybercrime perpetrators. They resume economic analyses application able to direct a deeper understanding of cybercrime. Later, the application determines how to cope with cybercrime effectively. Furthermore, it could gain more insight from the behavior of cybercrime perpetrators. This knowledge used to analyze the effectiveness of countermeasures. The conclusion state countermeasures are effective when they aim at the revenue stream of cybercrime attackers.
2.3. Comprehensive solution framework

Gupta and Pieprzyk [9] have proposed a socio-technical solution as well as Vayanshi and Kumar[2]. The difference between them lay in the solution type. Gupta and Pieprzyk proposed practical model while Vayanshi and Kumar proposed solution framework. Gupta and Pieprzyk proposed a hybrid of blacklisting, heuristics, and moderation based phishing prevention, while Vayanshi and Kumar proposed a circular solution for phishing challenges, as shown in Figure 4.

![Figure 4. Phishing solution framework](image)

The similarities between them in the early phase that both papers proposed preventive phishing for blocking a website and email filtering. Gupta and Pieprzyk improve the black and whitelisting by controlling and moderation technique, while Gupta and Peiprzyk recommend machine learning technique to filter email and block a website.

3. Phishing detection and prevention

3.1. Advanced detection

There are various new techniques for phishing detection recently, specially designed where accuracy is extremely important[3]. The blacklisting and whitelisting approaches have low FP rates and incapable of the detection of zero-hours phishing attacks. These approaches can detect only about 20% of such attacks. Machine learning and data mining approaches give the best results in phishing detection. However, these approaches are time-consuming, even for a small dataset.

Several techniques have been developed by considering user behavioral (Lee, et.al [10], Rao & Pais [11], Rao & Pais[12]). Zhang and Gupta[13] state in their paper that user behavior in phishing attacks influenced by user attributes and online experience. For example, Dong et al. [14] have proposed user behavior phishing detection based on users’ online behaviors such as visited websites, and the user’s perceived usefulness websites. The works claim that the method able to consistently detect phishing webpages regardless of how they implemented as long as they ask for authentication credentials.

3.2. Avoidance and preventive mechanism

Aldawood and Skinner recently have reviewed various social engineering cybersecurity threats in diverse environments [15]. The solution has proposed by many researchers includes that focused on phishing attack prevention. User education is also a requirement to lower the phishing attacks, besides
improvements in the interfaces that give warnings or the automatic removal of malicious content before the end-users would be a more promising approach.

Nevertheless, to date, Alsharnoubly resume various amounts of literature work has discussed that incapability to interact with the systems as one of the major reasons why people still fall for phishing attacks [16]. Previous research has shown that both academic and government organizations have made a significant effort to deliver end-user education to enable public understanding of the importance of cybersecurity, especially in anti-phishing context[17]–[21]. The study results showed a significant improvement in participants' phishing avoidance behavior in their post-test assessment.

Phishing education needs to be considered as a means to combat this threat, as reviewed by Kaur et al. [22], and an example is given by Alsharnouby[16]. Arachchilage reports on a design and development of a mobile game prototype as an educational tool helping computer users to protect themselves against phishing attacks [23].

Tools that aim to combat phishing attacks must take into account how and why people fall for them to be effective[24]. Previous work suggests that people may be vulnerable to phishing schemes because their awareness of the risks is not linked to perceived vulnerability or to use strategies in identifying phishing emails. The paper has explored what factors are associated with falling for phishing attacks in a role-play exercise.

4. Solution challenge discussion
Summer and Yuan [25] state that the biggest challenge in phishing attacks to deal with context-aware phishing. This attack exploits many resources, not only from user email but expanded to social media and social network conversation. The attacker uses a mechanism of data mining to gather specific related information before executing an attack. Overcoming these problems need to specify a comprehensive solution in both social and technical aspects. Summer and Yuan also direct that the future work requires several processes such as mitigation process and program, user education, and training utilizing game and interactive software. In terms of detection techniques, a vast number of researches use an intelligent approach, such as a machine learning algorithm.

Regarding the conclusion about solution challenge in a phishing attack, Vincent [26] points out there is no one-size-fits-all solution to preventing and mitigating phishing. He suggests the security teams should save themselves time and stress by leveraging threat intelligence. On the other hand, the challenge of threat intelligence lay on attack vector and indicator reconnaissance, as stated by Conti et al. [27]. Threat Intelligence system shall have the capability of recognizing the point of attacks and the system vulnerabilities. The cybercriminal may exploit the vulnerabilities. An immersive or augmented analytic technique in security assessment requires to overcome the cybercriminals which use advanced anti-forensics and evasion methods in their malicious code.

Based on the previous description, there are several important notes should be considered overcoming phishing attacks. The first note that should be memorized is that no one-size-fits-all solution to prevent and mitigate phishing. The second note is that the human factor plays important factor in successful phishing attack. The third note is that the social and technical solution has been grown to overcome the attack but should be considering the intelligent technique that system can be learned from time to time to recognize attack vector and indicator and also able to evaluate the level of user awareness regarding the phishing attack.

A comprehensive solution should take attention to aspects of the phishing attack. A total solution must consider attack identification, which will analyze that influence the design. The solution architecture for a phishing attack can describe as follows:
The architecture has 3 blocks; the first block feeds the knowledge and information lead from several sources. The sources for deep learning come from several sources, such as Infrastructure Profile, User Activity, Previous Attack, and Social Media Activity.

The second block uses the result of the previous block. The intelligent technique block employs a machine learning method. The process applies to blacklist and whitelisting to suspicious content. The objective of this stage is to employed a comprehensive technique for content detection. The last block act like an interface and a service. The block implemented in various means such as a browser plugin or an application.

5. Conclusion and future direction

This paper has discussed the phishing challenge solution that results in several conclusions. The first conclusion resume that phishing attack becomes more intelligent. An intelligent attack raises the difficulty of quick detection. The second conclusion is a successful attack indicated that user behavior plays an important role. The last conclusion observes the solution has grown continually. Since there is no one-size-fits-all solution, some researcher suggests applying threat intelligence management to overcome the attacks. Threat intelligence management must consider an attack vector and indicator reconnaissance. Finally, preliminary solution architecture has described as potential future work and drawn as an initial model. Detail explanation will be the future work of this research area.

References

[1] “2018 Data Breach Investigations Report: the year of ransomware,” Comput. Fraud Secur., vol. 2018, no. 5, p. 4, 2018.
[2] I. Vayansky and S. Kumar, “Phishing – challenges and solutions,” Comput. Fraud Secur., vol. 2018, no. 1, pp. 15–20, 2018.
[3] B. B. G. Aaankshka, T. Ankit, K. Jain, and D. P. Agrawal, “Fighting against phishing attacks: state of the art and future challenges,” Neural Comput. Appl., vol. 28, no. 12, pp. 3629–3654, 2017.
[4] B. B. G. Nalin and A. G. A. Kostas, “Defending against phishing attacks: taxonomy of methods, current issues and future directions,” Telecommun. Syst., vol. 67, no. 2, pp. 247–267, 2018.
[5] S. Radicati and Q. Hoang, “Email Statistics Report, 2017-2021,” Email Stat. report, 2017-2021 - Exec. Summ., vol. 44, no. 0, p. 4, 2017.
[6] C. Hadnagy, Social Engineering: The Science of Human Hacking, Second. Wiley, 2018.
[7] C. Konradt, A. Schilling, and B. Werners, “Phishing: An economic analysis of cybercrime perpetrators,” Comput. Secur., vol. 58, pp. 39–46, 2016.
[8] J. H. Cho, H. Cam, and A. Oltramari, “Effect of personality traits on trust and risk to phishing

Figure 5. Phishing building block solution.
vulnerability: Modeling and analysis,” 2016 IEEE Int. Multi-Disciplinary Conf. Cogn. Methods Situat. Aware. Decis. Support. CogSIMA 2016, pp. 7–13, 2016.

[9] G. Gupta and J. Pieprzyk, “Socio-technological phishing prevention,” Inf. Secur. Tech. Rep., vol. 16, no. 2, pp. 67–73, 2011.

[10] L. Lee, K. Lee, Y. Juan, H. Chen, and Y. Tseng, “Users’ Behavioral Prediction for Phishing Detection,” no. 1, pp. 337–338, 2014.

[11] R. S. Rao and A. R. Pais, “Detecting Phishing Websites using Automation of Human Behavior,” pp. 33–42, 2017.

[12] R. S. R. B and A. R. Pais, “An Enhanced Blacklist Method to Detect Phishing Websites,” pp. 323–333, 2017.

[13] Z. Zhang and B. B. Gupta, “Social media security and trustworthiness: Overview and new direction,” Futur. Gener. Comput. Syst., vol. 86, pp. 914–925, 2018.

[14] X. Dong, J. A. Clark, and J. L. Jacob, “Defending the weakest link: phishing websites detection by analysing user behaviours,” pp. 215–226, 2010.

[15] H. Aldawood and G. Skinner, “Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review,” Proc. 2018 IEEE Int. Conf. Teaching, Assessment, Learn. Eng. TALE 2018, no. December, pp. 62–68, 2019.

[16] M. Alsharnouby, F. Alaca, and S. Chiasson, “Why phishing still works: User strategies for combating phishing attacks,” Int. J. Hum. Comput. Stud., vol. 82, pp. 69–82, 2015.

[17] C. J. Gokul, S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Lodha, “PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness,” pp. 169–181, 2018.

[18] 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.

[19] A. Díaz, A. T. Sherman, and A. Joshi, “Phishing in an Academic Community: A Study of User Susceptibility and Behavior,” 2018.

[20] M. J. A. Miranda, “Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach,” vol. 14, no. 2, pp. 5–10, 2018.

[21] A. Karakasiliotis, S. M. Furnell, and M. Papadaki, “Assessing end-user awareness of social engineering and phishing,” Proc. 7th Aust. Inf. Warf. Secur. Conf., pp. 60–72, 2006.

[22] Kaur, S. Singh, and H. Kumar, “Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches,” J. Netw. Comput. Appl., vol. 112, no. September 2017, pp. 53–88, 2018.

[23] N. A. G. Arachchilage, S. Love, and C. Maple, “Can a Mobile Game Teach Computer Users to Thwart Phishing Attacks?,” Int. J. Informatonics, vol. 6, no. 3/4, pp. 720–730, 2016.

[24] J. S. Downs, M. Holbrook, and L. F. Cranor, “Behavioral Response to Phishing Risk,” pp. 37–44, 2007.

[25] S. Sumner, “Mitigating Phishing Attacks: An Overview Computer Science,” pp. 72–77, 2019.

[26] A. Vincent, “Don’t feed the phish: how to avoid phishing attacks,” Netw. Secur., vol. 2019, no. 2, pp. 11–14, 2019.

[27] M. Conti, T. Dargahi, and A. Dehghantanha, “Cyber threat intelligence: Challenges and opportunities,” Adv. Inf. Secur., vol. 70, pp. 1–6, 2018.