Guidelines for Developers and Recommendations for Users to Mitigate Phishing Attacks: An Interdisciplinary Research Approach

Javara Allah Bukhsh(✉)

University of Twente, Enschede, The Netherlands
j.allahbukhsh@utwente.nl

Abstract. Phishing attacks are common these days. If successful, these attacks cause psychological, emotional, and financial damage to the victims. Such damages may have a long-term impact. The overall objective of this Ph.D. research is to contribute to mitigating phishing victimization risks by exploring phishing prevalence, user-related risk factors, and vulnerable target groups and by designing (1) guidelines for social website developers focused on internet user vulnerabilities and (2) recommendations for users to avoid such attacks. The Ph.D. research acknowledges that phishing attacks are technical in nature, while the impact is financial and psychological. Therefore, an interdisciplinary research approach focusing on empirical research methods from social sciences (i.e., focus groups and surveys) and computer science (i.e., data-driven techniques such as machine learning) is adopted for the research. In particular, we aim to use a machine learning model for data analytics and quantitative and qualitative research design for psychological analysis. The research outcome of this Ph.D. work is expected to provide recommendations for internet users and organizations developing social-media-based software systems through more phishing aware development practices.

Keywords: Phishing · Repeat phishing · User perspective · Risk factors · Vulnerability · Guidelines · Recommendations · Empirical research methods

1 Introduction

Information and Communication Technology (ICT) is ubiquitous in life today as people increasingly rely on multiple ICT components (e.g., mobile devices, personal computers, and intelligent appliances) in day-to-day life. Specifically, by July 2022, the number of internet users has reached 5.3 billion [1]. However, the widespread digital communication poses several risks and has important implications, including common cyber threats, namely social engineering attacks (phishing), ransomware, and mobile security attacks. Due to the rising number of cyber-attacks, computer privacy and cyber security have become a global concern [2, 3]. As per Statista, a market and consumer data provider [4], in the 2nd quarter of 2022, 5.18 million data records were exposed worldwide.

S. Nurcan et al. (Eds.): RCIS 2023, LNBIP 476, pp. 632–640, 2023.
https://doi.org/10.1007/978-3-031-33080-3_46

The Ph.D. research in this paper is concerned with one of the prominent types of cybercrime, namely *phishing*, which compromises personal information, including banking and credit card details, passwords, and individual files. Lastdrager [5] defined *phishing* as 'a scalable act of deception whereby impersonation is used to obtain information from a target". Each year an increasing number of phishing attacks is reported. According to the Anti-Phishing Working Group (APWG), more than one million phishing cases were reported in the first three months of 2020, which was the highest number of attacks in one quarter until now. It was followed by 384,291 cases reported in March 2022, which was the highest number of attacks in one month thus far [6].

Despite the concerted efforts of government institutions and private organizations to limit phishing victimization, overcoming phishing attacks is still considered to be extremely challenging because of the rapidly evolving technological capabilities available to attackers, and the types of the attacks themselves, e.g. email, social media, mobile phone. So far, many studies have been published on phishing detection and its countermeasures [7, 8]. These mostly focused on technical aspects of overcoming phishing attacks. Unlike prior publications and leveraging the author's background in psychology, this PhD work is interested in the human factors that play a significant role in successful phishing attempts. Our PhD research interest is motivated by the observation of Abroshan et al. [9] that human behavior is one of the most important factors determining the success rate of phishing attacks. Moreover, our research is also motivated by the observation [10] that people can quickly disclose confidential information even when they are being warned or nudged by an awareness campaign. While many national surveys and studies have been conducted on phishing prevalence, on its causes, and on the countermeasures to reduce their success rate [3, 8, 11, 12], a steep rise in phishing attacks is still being reported each year.

The present PhD research initiative is set out to help both public and private institutions tackle and reduce the impact of phishing attacks. To this end, there are two significant areas that we aims to work on:

First, exploring and understanding of phishing prevalence, risk factors, and vulnerable target groups. Developing more profound knowledge of victims will enable us to propose and design robust countermeasures. Furthermore, this knowledge would serve as foundation to create recommendations to make internet users more aware about their risky behavior, i.e., sharing credentials with strangers and its consequences in future.

Second, developing specific guidelines for 'attentive' software systems that manage the user's attention for risky behavior, based on known risk factors and phishing techniques. Such guidelines are expected to be helpful to software developers while designing software in the best interest of users' security and privacy.

The context of this Ph.D. work includes both user victimization and *repeat* victimization (i.e., becoming victim more than once) due to phishing. We deliberately include repeat victimization, because on one side scholars acknowledge its importance [13], while on another side, it is an under-researched phenomenon [14]. As per Milani et al. [15], in 2018, ten percent of repeated data breach events were reported. Moreover, Wittebrood & Nieuwbeerta [16] indicated that previous victimization and routine activity increase the chance of repeat victimization. While the literature on cybercrime has mainly

focused on cyber victimization generally [17, 18], little attention has been given so far to studying the phenomena of repeat phishing.

This doctoral paper is structured as follows: Sect. 2 provides background on (repeat) phishing and its causes. It summarizes literature on phishing prevalence and its socio-demographic vulnerabilities. Section 3 presents the motivation of this Ph.D. project. Section 4 formulates the research goal and identifies research questions to support this goal. Section 5 describes (i) the interdisciplinary research method to answer the research questions and (ii) the research design that will be implemented to achieve the results. Section 6 discusses findings that have been obtained so far and sheds light on work implemented these days. Finally, Sect. 7 summarizes our progress and our immediate next steps and plans in the long run.

2 Background

Users' insufficient awareness, advances in phishing email technology, and human errors are prominent reasons behind successful phishing attacks [9]. Existing empirical studies [19, 20] indicate the following user vulnerability factors, among others, for phishing attacks: user age and gender, level of education, duration of internet usage, dispositional (e.g., individual aspects) and situational (e.g., environment and others) aspects, phishing awareness and victim personality factors. Furthermore, studies also highlighted personality factors, e.g., those included in the Big Five Personality Theory, behind successful phishing [21, 22]. These authors reported that narcissistic, female users are more frequently tricked through phishing attacks and possess a higher level of conscientiousness, than male users. Moreover, a few people are targeted more often by phishing attacks, significantly if they have fallen victim to a phishing attack in the past. Although there is a consensus among scholars that a few internet users are at risk of repeat exploitation by offenders, little so far has been done to consolidate the published knowledge on the prevalence of repeat phishing and its risk factors among individuals and organizations. The current Ph.D. research intends to bridge this gap of knowledge. To this end, we expect our Ph.D. work to bring two contributions: the first is a framework for understanding the human factors involved in victimization and repeat victimization due to phishing, and the second is to design (1) guidelines for developers to help them design software systems in such a way that leads to users avoiding victimization due to phishing, and (2) recommendations for users to prevent (repeat) victimization due to phishing.

3 Research Goal and Questions

This Ph.D. project is meant to add up to the collective efforts of scholars working towards protecting users against phishing attacks. In line with this, the PhD project's goal is twofold: (1) using acquired knowledge on user vulnerabilities that takes socio-demographic and cultural differences into account, provide recommendations for increasing privacy awareness to people; and (2) based on the knowledge acquired on user vulnerabilities and phishing techniques, provide guidelines for developers of ssoftware systems that manage the user's attention for risky behavior and recommendations for

users to avoid victimization. To achieve our research goal, we designed the following research questions (RQs) for this Ph.D. work:

RQ1: What are the prevalence, sociodemographic correlates, and risk factors of users' vulnerabilities toward phishing, according to published literature?
RQ2: What is the prevalence of repeat phishing victimization in relation to sociodemographic and the users' vulnerabilities, according to publicly available data sources?
RQ3: Are there cultural differences in security and privacy awareness across countries?
RQ4: What guidelines and recommendations can be designed to minimize the vulnerability of internet users to phishing attacks, based on a combination of the knowledge acquired in answering RQ1, RQ2 and RQ3, insights obtained from a focus group discussion with phishing victims, and a model developed using the previous results and tested against real-world phishing attacks?
RQ5: To what extent are these guidelines usable and useful in practice?

Fig. 1. The scope of this PhD research: a Mind Map

Figure 1. Shows a mind map that is grounded on our RQs and puts together the inputs and outputs of this Ph.D. work and the research activities. As Fig. 1 indicates, phishing will be explored from different perspectives and by employing different research techniques. The area in green, following the line labeled Systematic literature review **SLR (Victims)** means that the phishing victimization phenomenon will be examined in order to know the prevalence and risk factors of phishing and repeat phishing. In another perspective labeled as **Data Analysis (Victims)**, in orange, phishing will be investigated through data analysis of secondary data belonging to a more significant population, i.e., the Dutch population. It is planned that at the end of the study, we will be able to know the figures of prevalence and sociodemographic vulnerability of phishing and repeat phishing. It will also help us understand the Dutch population's awareness of the privacy and security of their confidential data.

In the **Privacy & Security (Victims),** a cross-cultural study will be conducted in two countries, i.e., the Netherlands and Pakistan, that will give us approximate figures of privacy awareness about both countries. Furthermore, in the area labeled **Guidelines (Developers) Recommendations (Users)**, in blue color, we indicate that based on the results of the empirical work to be done until that point (i.e. the studies that the author will do to answer RQ1, RQ2 and RQ3), we plan to create two artefacts. First of all, a set of guidelines will be designed for software developers that highlight the risk factors of phishing victims. The intention behind these guidelines is to be considered by developers for implementation while designing social media websites, in order to minimize user vulnerability to phishing attacks. Moreover, a case study will be designed with software professionals to validate the usefulness of proposed guidelines. Second, a set of recommendations will be developed for users that emphasize the victimization risk factors and help users to avoid phishing attacks in the future. In addition, these recommendations will be shared with educational and professional institutions in the Netherlands and Pakistan to specific audiences as part of actions to increase the awareness of phishing attacks among people.

4 Research Methodology

As this Ph.D. work happens at the intersection of multiple disciplines (information systems, psychology and crime science), this research project adopts interdisciplinary research methodology. Below, Fig. 2 explains the research methodology concerning these disciplines and the specific research techniques that are planned to be applied in order to get the answer for each RQ. We will address our *RQ1* and *RQ2* by using two approaches: a systematic literature review (SLR) and an analysis of secondary data using machine learning (ML). The systematic literature review is conducted by using Siddaway's practices [23] designed for systematic reviews. The systematic literature review explores the prevalence of (repeat) phishing and the socio-demographics of victims. In this systematic literature review, we complemented findings from published peer-reviewed studies with results reported in several national surveys on the prevalence of phishing and victim demographics. At the time of writing this doctoral paper, the systematic literature review is in the stage of being finalized for submission to a journal. Through the systematic literature review, we learned that there are no exact figures in the literature about the prevalence of (repeat) phishing. As we didn't find any concrete answer to the vulnerable demographics of phishing victims, we plan to continue with a data-driven approach. We will analyze secondary data using ML methods to predict prevalence and user vulnerability concerning users' demographic and particular risky behavior.

For *RQ3*, we will design a quantitative study using the method of survey research [24] to uncover the privacy awareness and sensitivity toward user confidential information. Moreover, we will perform a cross-cultural study between two countries, Pakistan (PAK) and the Netherlands (NL), to account for possible (cultural) differences in phishing victimization. (Note that in the leftmost side of Fig. 1, NL and PAK indicate the two countries.)

For *RQ4*, we plan two pieces of research that build upon each other. First, we will conduct qualitative research [24] in which focus groups will be used to gather information

from phishing victims. Our focus will be to discover why users become victimized through phishing. What are the commonly observed behaviors that become the reason for their victimization? Moreover, what could be the psychological tricks and information that, if people know before attacks, even if they are aware of cybercrime, will help them to avoid such attacks? Our plan is to analyze the results by using content analysis [24].

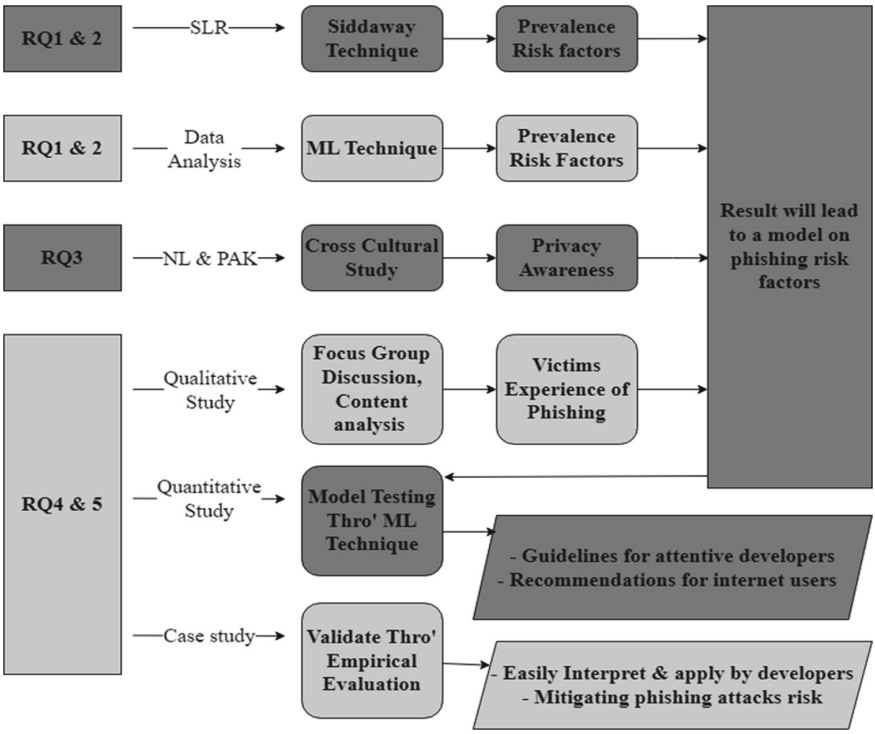

Fig. 2. Methodological overview of the Ph.D. Project

Second, based on the previous study's results, we will make a model using risky behaviors and information to avoid attacks and test that model on random internet users using a survey method. The data of this study will be analyzed by using machine learning techniques.

Our second study results will serve two purposes: (1) we will make guidelines (e.g., use of password strength indicators and use brief terms of services) for software developers to guide their software development processes that account for users' vulnerabilities. These guidelines are expected to be helpful while designing software for internet users. (2) we will make recommendations for internet users to avoid victimization and will share these with public and private institutions interested in and responsible for creating and maintaining users' awareness to avoid phishing victimization. For example, the school boards. We expect that the research to be done in order to answer RQ4, will provide foundation for these organizations to come up with educational measures and policies that are helpful for users when dealing with phishing attacks.

Finally, for answering *RQ5*, we plan to design empirical evaluation research process with software practitioners that will help us understand the extent to which the proposed guidelines are useful and usable. For example, we will evaluate how easy developers can interpret and apply the guidelines, and how effective the developed software is in mitigating phishing attack risks. For this, we will do a perception-based evaluation with practitioners from companies that develop, e.g., social media platforms or social media based software systems (such as blogging sites and social review sites). We will ground our perception-based evaluation study on the UTAUT theoretical model [25] that has been suitable to contexts such as the one of this Ph.D. work and that has been operationalized by means of evaluation questions that address the usefulness and utility aspects of any IT-related artefacts, including guidelines such as ours.

5 Current Results

Thus far, our performed systematic literature review has uncovered the following research challenges concerning phishing victimization: (1) aggregating finding from various empirical studies about phishing victims is hard due to the diversity of research methods employed and types of phishing analyzed; (2) while literature acknowledges the urgent need to investigate repeat phishing victimization, only a few studies focused on this phenomenon and the related risk factors; (3) findings from empirical studies are inconclusive regarding the human factors responsible for phishing victimization. An example of the latter is that survey research on sociodemographic vulnerability indicates that male users are more victimized than female users through phishing attacks, while case study research indicates the opposite. As current literature is very limited to draw any conclusions, we plan further empirical studies to explore phishing phenomena so that we are able to come up with some meaningful solutions (e.g., recommendations and guidelines) able to protect more individuals from victimization.

6 Conclusion and Progress of the Research

The phenomenon of phishing victimization and repeat victimization is only partly understood as it has been researched until now in a fragmentary way, either from technical standpoint or holistically from cybercrime standpoint, while the risks due to human factors evaded the scholar's attention. To the best of our knowledge, this PhD research is one of the first initiatives that addresses this gap and creates a model for understanding the phishing victimization risks due to human factors as well as proposes guidelines for developers to help design software systems that reduce or prevent phishing victimization of users. Unlike existing works, this Ph.D. research takes the perspective of individual users and their contexts. Until now, we completed a systematic literature review on the prevalence of repeat victimization and its social demographics. Currently, we are working towards getting authorized access to secondary data from a large public organization in the Netherlands, in order to measure the prevalence of phishing and to analyze the sociodemographic vulnerability of phishing victimization among the Dutch population. It is a specialized government institution that keeps the records of millions of Dutch citizens about phishing victimization.

In parallel, we are thinking over strategies to collect phishing victimization data from Twitter. The purpose of the Twitter data is to check people's vulnerability based on their social demographic. We plan to take the social profile of people who claim phishing victimization. The data acquisition task through Twitter is in progress, with 50% completion at the time of writing this paper.

Acknowledgement. This Ph.D. work is carried out under the supervision of Dr. Marten van Sinderen and Dr. Maya Daneva of the University of Twente, the Netherlands.

References

1. Statista: Internet and social media users in the world 2022, Statista (2022). https://www.statista.com/statistics/617136/digital-population-worldwide/. Accessed 30 September 2022
2. Cyber Security Breaches Survey 2020. GOV.UK (2020). https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020. Accessed 14 Apr 2021
3. Proofpoint: State of the Phish Report: Attack Rates Rise, Account Compromise Soars. Proofpoint (2019). https://www.proofpoint.com/us/corporate-blog/post/2019-state-phish-report-attack-rates-rise-account-compromise-soars. Accessed 01 Oct 2022
4. Statista: Data records breached worldwide 2022, Statista (2022). https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/. Accessed 30 Sep 2022
5. Lastdrager, E.E.H.: Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Sci. **3**(1), 1 (2014). https://doi.org/10.1186/s40163-014-0009-y
6. APWG:APWG | APWG 1Q 2022: Phishing Reaches Record High; APWG Observes One Million Attacks Within the Quarter – For the First Time – in the First Quarter of 2022 (2022). https://apwg.org/apwg-1q-2022-phishing-reaches-record-high-apwg-observes-one-million-attacks-within-the-quarter-for-the-first-time-in-the-first-quarter-of-2022/. Accessed 01 Oct 2022
7. Aleroud, A., Zhou, L.: Phishing environments, techniques, and countermeasures: a survey. Comput. Secur. **68**, 160–196 (2017).https://doi.org/10.1016/j.cose.2017.04.006
8. Huang, H., Zhong, S., Tan, J.: Browser-side countermeasures for deceptive phishing attack. In: 5th International Conference on Information Assurance and Security, IAS 2009, September 2009, pp. 352–355 (2009). https://doi.org/10.1109/IAS.2009.12
9. Abroshan, H., Devos, J., Poels, G., Laermans, E.: Phishing attacks root causes. In: Cuppens, N., Cuppens, F., Lanet, J.-L., Legay, A., Garcia-Alfaro, J. (eds.) Risks and Security of Internet and Systems. LNCS, vol. 10694, pp. 187–202. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76687-4_13
10. Junger, M., Montoya, L., Overink, F.-J.: Priming and warnings are not effective to prevent social engineering attacks. Comput. Hum. Behav. **66**, 75–87 (2017). https://doi.org/10.1016/j.chb.2016.09.012
11. Garera, S., Provos, N., Chew, M., Rubin, A.D.: A Framework for Detection and Measurement of Phishing Attacks, pp. 1–8 (2007)
12. Hutchings, A., Hayes, H.: Routine activity theory and phishing victimisation: who gets caught in the 'Net'? Current Issues Crim. Justice **20**(3), 433–452 (2018). https://doi.org/10.1080/10345329.2009.12035821
13. Canham, M., Posey, C., Strickland, D., Constantino, M.: Phishing for long tails: examining organizational repeat clickers and protective stewards. SAGE Open **11**(1), 215824402199065 (2021). https://doi.org/10.1177/2158244021990656

14. Correia, S.G.: Patterns of online repeat victimisation and implications for crime prevention. In: 2020 APWG Symposium on Electronic Crime Research (eCrime), November 2020, pp. 1–11 (2020). https://doi.org/10.1109/eCrime51433.2020.9493258
15. Milani, R., Caneppele, S., Burkhardt, C.: Exposure to cyber victimization: results from a Swiss survey. Deviant Behav. 1–13 (2020).https://doi.org/10.1080/01639625.2020.1806453
16. Wittebrood, K., Nieuwbeerta, P.: Criminal victimization during one's life course: the effects of previous victimization and patterns of routine activities. J. Res. Crime Delinq. **37**(1), 91–122 (2000). https://doi.org/10.1177/0022427800037001004
17. Brown, C.F., Demaray, M.K., Secord, S.M.: Cyber victimization in middle school and relations to social emotional outcomes. Comput. Hum. Behav. **35**, 12–21 (2014). https://doi.org/10.1016/j.chb.2014.02.014
18. Whitty, M.T.: Predicting susceptibility to cyber-fraud victimhood. J. Financ. Crime **26**(1), 277–292 (2019). https://doi.org/10.1108/JFC-10-2017-0095
19. Darwish, A., Zarka, A.E., Aloul, F.: Towards understanding phishing victims' profile. In: 2012 International Conference on Computer Systems and Industrial Informatics, December 2012, pp. 1–5 (2012). https://doi.org/10.1109/ICCSII.2012.6454454
20. Parsons, K., Butavicius, M., Delfabbro, P., Lillie, M.: Predicting susceptibility to social influence in phishing emails. Int. J. Hum. Comput. Stud. **128**, 17–26 (2019). https://doi.org/10.1016/j.ijhcs.2019.02.007
21. Curtis, S.R., Rajivan, P., Jones, D.N., Gonzalez, C.: Phishing attempts among the dark triad: patterns of attack and vulnerability. Comput. Hum. Behav. **87**, 174–182 (2018). https://doi.org/10.1016/j.chb.2018.05.037
22. Halevi, T., Memon, N., Nov, O.: Spear-phishing in the wild: a real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. SSRN Electron. J. (2015).https://doi.org/10.2139/ssrn.2544742
23. Siddaway, A.P., Wood, A.M., Hedges, L.V.: How to do a systematic review: a best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. Ann. Rev. Psychol. **70**(1), 747–770 (2019). https://doi.org/10.1146/annurev-psych-010418-102803
24. Oakley, J.G.: Access. In: Waging Cyber War, pp. 101–114. Apress, Berkeley (2019). https://doi.org/10.1007/978-1-4842-4950-5_8
25. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**(3), 425–478 (2003). https://doi.org/10.2307/30036540