Issues in Information Systems
Volume 25, Issue 2, pp. 339-345, 2024

DOI: https://doi.org/10.48009/2_iis_2024_127

Assessing university students' attitudes towards phishing email reporting tools: a research proposal

Brad Fowler, *Georgia College & State University, brad.fowler@gcsu.edu*
Bryan Marshall, *Georgia College & State University, bryan.Marshall@gcsu.edu*
Peter Cardon, *University of Southern California, cardonl@marshall.usc.edu*

Abstract

Phishing attacks are a significant threat to organizations, including universities. Effective defense mechanisms, such as phishing reporting software embedded in email systems, enable users to report suspicious emails. While faculty and staff are generally obligated to defend against these threats, students do not share this responsibility. This research proposal aims to explore university students' attitudes towards using phishing reporting features in their email systems. Understanding these attitudes can provide valuable insights for improving the adoption and effectiveness of such features among students. The study's findings could have practical implications for enhancing the protection of university networks and systems from phishing attacks. Additionally, the research will contribute to the broader field of technology acceptance, specifically regarding email reporting systems in educational environments. By examining factors such as perceived ease of use and perceived usefulness, this study seeks to inform strategies for increasing student engagement with phishing defenses, ultimately contributing to a more secure academic cyber environment.

Keywords: phishing reporting, technology acceptance model (TAM), university cybersecurity, student attitudes

Introduction

Phishing is a pervasive cyberattack strategy that affects organizations across all sectors. Phishing attacks allow attackers to gain access to an organization’s networks and systems. Through this access, attackers can compromise systems, steal data, access organizational and employee funds, and conduct ransomware attacks for extortion. The FBI's Internet Crime Complaint Center received 300,497 phishing complaints in 2022 (Federal Bureau of Investigation, 2023). The Anti-Phishing Working Group published a report in 2023 detailing $50 billion in losses due to phishing attacks against business organizations (Anti-Phishing Working Group, 2023). Universities are as much at risk from phishing attacks as any other organization. Duke University’s Office of Information Technology reported blocking 65 million fraudulent emails in August 2022 (Keegan, 2022).

For many organizations, extensive cybersecurity training is required for all employees (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Organizations create multi-faceted training programs to maximize awareness of phishing threats to both the organization and the employees themselves (Zhang, Egelman, Cranor, & Hong, n.d.). Universities face a unique challenge because students are not employees. Students are the product of the university’s overall mission, but they are not responsible for achieving that mission. Therefore, it is not a natural function of a student’s duty to protect their university.Many organizations

employ phishing email reporting as one part of a holistic approach to phishing defense. Phishing email reporting features can be embedded into email systems as added features. These features allow users to report email they receive that they find suspicious. Previous studies have found that crowd-sourcing-based practices are effective in phishing defense (Lain, Kostiainen, & Capkun, 2021).

This study proposes a research methodology created to better understand students' attitudes towards the acceptance of phishing reporting features in their university email systems. The completion of the study could provide scholarly and practical contributions to the field of Information Systems. Currently, no study has used established acceptance models to test students' attitudes towards phishing reporting features. Results from a completed study could also help to inform university security professionals on efforts to increase student use of phishing reporting features in their email systems. The execution of this research methodology would seek to answer the following questions:

RQ1: *To what extent does perceived ease of use affect students' intention to use phishing reporting features in university email systems?*

RQ2: *To what extent does perceived usefulness affect students' intention to use phishing reporting features in university email systems?*

The following sections of this paper include a review of the relevant literature, an explanation of the research model used in this study, the research methodology, expected contributions, and conclusions.

Literature Review

Like all organizations, universities face a clear and present threat from phishing. Students can be targets of phishing attempts and should be trained to identify potential attacks (Bailey, Mitchell, & Jensen, 2008). Yoro et al. (2023) found that traditional factors such as age, gender, and perceived safety impact students' susceptibility. Frauenstein (2019) discovered that students are likely to experience phishing attacks through email and social media and are especially vulnerable to attacks that present authoritative postures or exploit emotional triggers. Lemay, Basnet, and Doleck (2020) tested a model to better understand how perceived phishing threats influence detection efficacy, finding that fear of phishing attacks and anxiety did not lead students to obtain more learning or protection.

While Broadhurst, Skinner, Sifniotis, Matamoros-Macias, and Ipsen (2019) did not find a correlation between training and understanding of phishing threats, they found that international students and underclassmen were more likely to be victimized. They also found that spear phishing emails and emails tailored to the student were more successful. Similarly, Okokpujie, Kennedy, Nnodu, and Noma-Osaghae (2023) found that spear phishing and tailored emails had greater success in targeting students, with 70% of students likely to fall for a phishing attack. Since both staff and students are required to have email accounts, phishing creates a large attack vector.

Case and King (2016) identified a decrease in reported phishing attacks among university undergraduates but an increase in phishing victimizations. Althobaiti, Jenkins, and Vaniea (2021) found that email attack reporting in a university environment was problematic due to the potential volume of reports, suggesting that universities should implement automation into their reporting systems. Increased automation could streamline the process and improve the overall effectiveness of phishing defenses.

Research Model

To effectively test the adoption of phishing reporting features in email systems, this study will use the Technology Acceptance Model (TAM). TAM was developed to examine how external variables impact behavioral intentions (Davis, 1989). As seen in Figure 1, TAM measures how antecedents influence behavioral intention and, ultimately, actual usage of a technology. It accomplishes this through three main constructs.

These constructs are:

- Perceived Ease of Use (PEOU) – the degree to which a student believes that it would be easy to use a phishing reporting feature in an email system.
- Perceived Usefulness (PU) – the degree to which a student believes that using a phishing reporting feature in an email system will mitigate the threat of phishing attacks.
- Behavioral Intention (BI) – the degree to which a student believes that they will or will not use a phishing reporting feature in their email system.

TAM has been used effectively in past studies that addressed university students' intentions to adopt technologies. TAM has been used extensively to study student adoption of e-learning and learning management systems (Bazelais, Doleck, & Lemay, 2018; Essel & Wilson, 2017; Lemay, Basnet, & Doleck, 2020; Mailizar, Burg, & Maulina, 2021; Šumak, Heričko, Pušnik, & Polančič, 2011). For instance, multiple studies have been conducted on students' adoption of mobile banking applications (Govender & Sihlali, 2014; Kumar, Lall, & Mane, 2017).

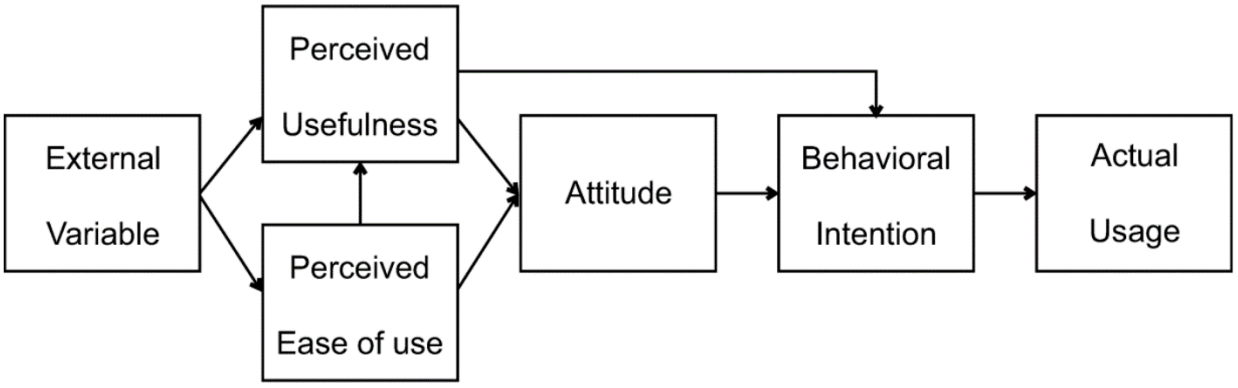

Figure 1. Technology Acceptance Model

Research Methodology

Since this phenomenon has not been tested using TAM prior to this study, we will test both the model and the hypotheses. The study will employ a survey instrument to test the model and hypotheses. Measurement items will be adapted from previous studies with modifications to wording to fit the phenomena. Each item will be measured using a 7-point Likert scale. The scale will have a range of 1 being "strongly disagree" to 7 being "Strongly agree. The survey will be distributed to university students at a regional university in

the southeastern area of the United States. Given the nature of the study, university students are the target population to be sampled. It will be important to get a representative sample based on the moderating variables in the model. The focus on a representative sample will ensure that the study has external validity and, therefore, can be generalized to other areas of research.

Data analysis will consist of two parts. The first part will evaluate the model to ensure that the relationships between the constructs are valid and that the survey items accurately measure each construct. The second part will test the hypotheses. To analyze both the structure and hypotheses, we will use Partial Least Squares Structural Equation Modeling (PLS-SEM). PLS-SEM is a popular statistical analysis methodology because it can perform factor analysis, path analysis, and hypothesis testing within a single statistical package. Hair, Ringle, and Sarstedt (2011) suggest that PLS-SEM is a "silver bullet" for multivariate statistical analysis. The SmartPLS statistical analysis software platform will be used for data analysis.

Through SEM analysis, we will check the model for validity and reliability. Checking the content validity of the model will ensure that it thoroughly measures the phenomena. Since TAM has been used extensively in Information Systems research, we believe it will be sufficient for testing the phenomena. Construct validity will be verified through an assessment of the model's convergent and discriminant validity, which are tested using confirmatory factor analysis. Convergent validity assesses how accurately the measurement items align with the constructs they are intended to measure. Valid relationships between measurement items and constructs must have factor loadings greater than .7 (Hair, Hult, Ringle, & Sarstedt, 2013).

Discriminant validity tests the relationships between measurement items and constructs that they are not intended to measure. It is assessed using the square root of the average variance extracted (AVE). The reliability of the model will be assessed using Cronbach's α, AVE, and composite reliability. The appropriate values for these measurements are .7 or higher for Cronbach's α, .6 or higher for AVE, and .6 or higher for composite reliability (Hair et al., 2013). Hypotheses will be tested using PLS-SEM, with the null hypothesis accepted for p-values < .05 at a 5% significance level (Hair et al., 2013).

Discussion

This study seeks to provide two distinct contributions. First, it aims to offer practical contributions to the work of university security professionals by creating new knowledge about student attitudes towards phishing email reporting features in their email systems. Since students comprise a significant population at any university and are major users of email systems, university security professionals may use the insights from this study to determine the viability of adoption initiatives. They may also use this study to tailor their messaging to students to increase awareness, adoption, and usage. The second expected contribution is the extension of acceptance models and testing to the area of phishing email reporting features. To date, no study has tested phishing email reporting features in student email systems. Results from this study may be generalizable to other, similar populations outside academia or to student populations in other countries and cultures.

Conclusion

Phishing emails continue to be a significant battle ground in cyber defense. Security professionals have the monumental task of securing all aspects of organizational systems and networks. Phishing attacks create an especially difficult defense scenario because every member of the organization must play a role in keeping the organizational systems and networks secure. Security professionals must implement a holistic framework of defense tactics to cover the entire attack vector. Pieces of this framework include physical

tools, such as firewalls and intrusion detections systems. They also rely on user awareness and response training. Phishing email reporting features embedded into organizational email systems allow security professionals to identify attacks quicker and to mitigate them faster. As the use of these features increases, the more effective they are in defense of phishing attacks. University students are not incentivized in the same manner as organization employees are to act in the best interests of the university. This proposal seeks to create a research study that will better understand student attitudes towards adopting phishing email reporting features in their university email systems. To accomplish this, we propose the use of a well-established model for technology acceptance (TAM), using a standard quantitative survey instrument, to test explore the phenomenon. The collected data will be analyzed using confirmatory factor analysis and statistical hypothesis testing.

We expect future avenues of research following this study to extend acceptance testing of phishing email reporting features to other acceptance models, like UTAUT and UTAUT2, or models that test continuous use. Acceptance of phishing email reporting features in email systems may also be extended to other populations beyond university students.

References

Althobaiti, K., Jenkins, A. D. G., & Vaniea, K. (2021). A case study of phishing incident response in an educational organization. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 1-32. https://doi.org/10.1145/3476079

Anti-Phishing Working Group. (2023, November). Phishing activity trends report (2nd quarter 2023). Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf

Bailey, J. L., Mitchell, R. B., & Jensen, B. K. (2008). Analysis of student vulnerabilities to phishing.

Bazelais, P., Doleck, T., & Lemay, D. J. (2018). Investigating the predictive power of TAM: A case study of CEGEP students' intentions to use online learning technologies. Education and Information Technologies, 23(1), 93-111. https://doi.org/10.1007/s10639-017-9587-0

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 4-23. https://doi.org/10.52306/2578-3289.1006

Case, C., & King, D. (2016). Phishing: Are undergraduates at risk and prepared? Issues In Information Systems, 17(1), 80-88.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319. https://doi.org/10.2307/249008

Essel, D. D., & Wilson, O. A. (2017). Factors affecting university students' use of Moodle: An empirical study based on TAM. International Journal of Information and Communication Technology Education, 13(1), 14-26. https://doi.org/10.4018/IJICTE.2017010102

Federal Bureau of Investigation. (2023, November 29). Internet Crime Complaint Center releases 2022 statistics. Retrieved from https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

Frauenstein, E. D. (2019). An investigation into students' responses to various phishing emails and other phishing-related behaviours. In H. Venter, M. Loock, M. Coetzee, M. Eloff, & J. Eloff (Eds.), Information security (Vol. 973, pp. 44-59). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_4

Govender, I., & Sihlali, W. (2014). A study of mobile banking adoption among university students using an extended TAM. Mediterranean Journal of Social Sciences, 5(7), 451. https://doi.org/10.5901/mjss.2014.v5n7p451

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). A primer on partial least squares structural equation modeling (PLS-SEM). SAGE Publications. Retrieved from https://books.google.com/books?id=IFiarYXE1PoC

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. Journal of Marketing Theory and Practice, 19(2), 139-152. https://doi.org/10.2753/MTP1069-6679190202

Keegan, H. (2022, September). Duke hit by largest email phishing attack since 2020. The Chronicle. Retrieved April 14, 2024, from https://www.dukechronicle.com/article/2022/09/duke-phishing-email-attack-largest-since-2020-office-of-information-technology

Kumar, V. V. R., Lall, A., & Mane, T. (2017). Extending the TAM model: Intention of management students to use mobile banking: Evidence from India. Global Business Review, 18(1), 238-249. https://doi.org/10.1177/0972150916666991

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology, 10(2), 1-31. https://doi.org/10.1145/1754393.1754396

Lain, D., Kostiainen, K., & Capkun, S. (2021, December 14). Phishing in organizations: Findings from a large-scale and long-term study. arXiv. Retrieved April 19, 2024, from http://arxiv.org/abs/2112.07498

Lemay, D. J., Basnet, R. B., & Doleck, T. (2020). Examining the relationship between threat and coping appraisal in phishing detection among college students. Journal of Internet Services and Information Security, 10(1), 38-49. https://doi.org/10.22667/JISIS.2020.02.29.038

Mailizar, M., Burg, D., & Maulina, S. (2021). Examining university students' behavioural intention to use e-learning during the COVID-19 pandemic: An extended TAM model. Education and Information Technologies, 26(6), 7057-7077. https://doi.org/10.1007/s10639-021-10557-5

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (A case study of a Nigerian leading university). International Journal of Sustainable Development and Planning, 18(1), 255-263. https://doi.org/10.18280/ijsdp.180127

Šumak, B., Heričko, M., Pušnik, M., & Polančič, G. (2011). Factors affecting acceptance and use of Moodle: An empirical study based on TAM. Informatica, 35, 91-100.

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. International Journal of Electrical and Computer Engineering, 13(2), 1922-1931. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). Phinding phish: Evaluating anti-phishing tools.

Appendix A

Measurement Items

Perceived Usefulness (PU) Adapted from Šumak et al.
PU1 – I would find phishing email reporting features useful for phishing defense.
PU2 – Using phishing email reporting features enables me to be more secure.
PU3 – Using phishing email reporting features for phishing defense increases my security.
PU4 – If I use phishing email reporting features, I will decrease my chances of getting hacked.

Perceived Ease of Use (PEOU) Adapted from Šumak et al.
PEOU1 – My interaction with phishing email reporting features would be clear and understandable.
PEOU2 – It would be easy for me to become skillful at using phishing email reporting features.
PEOU3 – I would find phishing email reporting features easy to use.
PEOU4 – Learning to operate phishing email reporting features is easy for me.

Attitude Toward Using Technology (ATU) Adapted from Šumak et al.
ATU1 – Using phishing email reporting features is a bad idea.
ATU2- phishing email reporting features makes security more interesting.
ATU3 – Using phishing email reporting features is fun.
ATU4 – I like using phishing email reporting features.

Behavioral Intention (BI) Adapted from Šumak et al.
BI1 – I intend to use phishing email reporting features in the next 6 months.
BI2 – I predict I would use phishing email reporting features in the next 6 months.
BI3 – I plan to use phishing email reporting features in the next semester.