International Journal of Global Research Innovations & Technology (IJGRIT)
ISSN : 2583-8717(Online), Impact Factor: 6.972, Volume 03, No. 03(II), July-September, 2025, pp 68-74

Improving Teachers' Knowledge of Phishing: An Integrative Framework and Test Plan

Jadeja Devangini J.[1*] | Dr. Vishalkumar Pradipkumar Patel[2]

[1]Research Scholar in Computer Science, Monark University, Ahmedabad, India.
[2]Assistant Professor, M. Sc.IT Department, Sardar Patel Institute of Applied Science, Bakrol, Gujarat, India.

*Corresponding Author: phddevanginijadeja@gmail.com

Citation: Devangini J, J. & Patel, V. (2025). Improving Teachers' Knowledge of Phishing: An Integrative Framework and Test Plan. International Journal of Global Research Innovations & Technology, 03(03(II)), 68–74. https://doi.org/10.62823/ijgrit/03.03(ii).8076

ABSTRACT

Phishing remains one of the most common and developing threats in the cyberspace domain, as it relies on social engineering to convince people to help attackers by providing very sensitive information including usernames and passwords, as well as sensitive financial or institutional information. Frequently, phishing attacks take advantage of human psychological triggers such as urgency, authority, and fear, creating the weakest link in cybersecurity protection as human users are targeted. While a large amount of research has focused on phishing awareness and education in corporate and financial settings, there is very little available with regard to education and therefore the individual educator. This is a major oversight, as educators are now routinely responsible for multiple data and sensitive data like student data, academic data and institutional access credentials. Therefore, improving educator cybersecurity awareness at the institutional level is important for a greater institutional information security goal. This research aims to fill this gap by creating a conceptual framework and experimental approach to increase phishing awareness among educators. This framework is grounded by Protection Motivation Theory (PMT), a common psychological theory utilized to provide insight into how an individual is motivated to protect oneself from perceived threats. PMT uses two appraisal processes: threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy, self-efficacy, and response costs). The goal of this research project is to investigate cognitive and emotional responses to threats of phishing and how they impact educator's behavioural intention to recognize and report phishing incidents. To assess the effectiveness of the proposed awareness intervention, the study will employ a quasi-experimental pre-test/post-test design with an intervention group and a control group. The intervention will be interactive, scenario-based phishing awareness training that will provide a real-world phishing scenarios and allow participants to actively engage in various practical exercises, quizzes, and a feedback loop. Participant's phishing awareness levels and behavioural intentions will be measured pre- and post-intervention using validated survey instruments based on PMT constructs. The control group will not receive any training during the experimental phase which will allow for the outcomes to be compared.

***Keywords**: Phishing, Cybersecurity Awareness, Educators, Experimental Design, Digital Literacy.*

Introduction

The growing reliance on digital technologies in educational settings means that educational institutions—and educators in particular—are increasingly exposed to cyber threats, with phishing being one of the most common and damaging. Phishing attacks usually prey on human trust and error and manipulate users into revealing sensitive information or downloading malware. Phishing can yield very serious consequences related to data breaches, identity theft, and financial losses, all of which have been documented in an educational context (Jampen et al., 2020).

Although phishing is a widespread threat, phishing awareness and training initiatives are skewed toward corporate environments, leaving educators more unprepared. Educators, while often aware of the more general threats to cyber security, report that a portion of them have not received formal training on responding to or protecting against phishing (Olowookere et al., 2025). Educators also face unique challenges that differ from the corporate employee, including limited technical comfort, tight constraints in supporting IT budgets, and limited exposure to cybersecurity protocols in the institution (Algarni et al., 2017). These factors culminate in an idiosyncratic risk profile that highlights the need for framed awareness initiatives.

Phishing awareness programs currently in use, including passive informational sessions and simulated phishing campaigns, have had varying degrees of success in reducing threat susceptibility. Some interventions lead to short-term gains in phishing detection, which do not last or result in significant behavioural change (e.g., Canfield et al., 2016). By contrast, educational programs that use interactive and experiential learning components have shown a greater propensity to reduce susceptibility to phishing for longer periods of time (Parsons et al., 2019). Theoretical models like Protection Motivation Theory (PMT) can inform understanding how users evaluate threats and make decisions regarding protective behaviour. For example, PMT suggests users are more likely to engage in protective behaviours following a phishing predisposition when there is a moderate-to-high perceived vulnerability, the recommended response would be effective, and they feel confident in the ability to execute the response (Rogers, 1983).

Given the different contextual challenges and needs of educators, this study outlines a conceptual framework and experimental design around phishing awareness, geared towards educators. The investigation will build off Protection Motivation Theory in attempting to explore the effect of interactive phishing awareness training on educators' preparedness to identify and respond to phishing.

The research aims to answer the following questions:

- **Does interactive training improve educators' ability to recognize phishing attempts?**
- **Are observed increases in awareness and behavioural intention mediated by PMT-related constructs (e.g., perceived vulnerability, self-efficacy, response efficacy)?**
- **What training formats are most effective in enhancing long-term phishing awareness and reporting behaviour among educators?**

In answering these questions, the study intends to contribute to the design of evidence-informed, theory-driven training interventions that could be incorporated in professional development programs, thereby enhancing the cybersecurity posture of educational institutions.

Literature Review

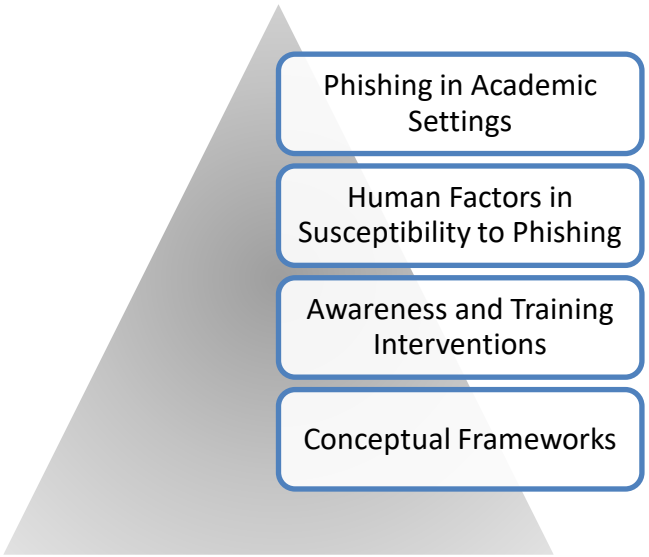

Fig. 1: Shows Literature Review Categories

- **Phishing in Academic Settings**

Due to the numerous holdings of sensitive information—student records, financial information, and proprietary research—and generally, a lower level of cybersecurity protection compared to the financial or medical sectors, educational institutions are becoming more attractive to cyber criminals (Keller et al., 2021). Faculty and staff are commonly inundated with unsolicited emails, which makes them more susceptible to phishing attempts through these emails (Jampen et al., 2020). Case studies from the field have shown that hackers have gained access to email accounts which have led to devastating outcomes, including ransomware attacks, identity theft, unauthorized access to sensitive and proprietary data, and reputational harm to institutions (Rogers & Jones, 2022). These risks signal a need for preventative actions to improve cybersecurity awareness in educational contexts.

- **Human Factors in Susceptibility to Phishing**

A recurring theme in the cybersecurity literature is the acknowledgment of human behaviour as the weakest link in the chain of defence against phishing (Alqaralleh et al., 2020). Individual variability in susceptibility to phishing has been related to age, job function, technical ability, and digital literacy, for example, Parsons et al. (2019) found that individuals without a technical background were significantly more prone to phishing than individuals with a technical background. Educators are generally positioned uniquely because they typically have higher digital literacy than a complete novice, but they also are not professionals in cybersecurity. Their unique status suggests that educators may be positioned to benefit the most from intervention that is contextually appropriate, aligned to their unique educational responsibilities and their role in higher education.

- **Awareness and Training Interventions**

Strategies to reduce exposure to phishing behaviour can be both diverse and varied. Actions designed for knowledge awareness can be passive—such as a poster, newsletter, or dynamic online module, which will provide a bare minimum of knowledge about phishing—but will not always result in behavioural changes to deter phishing attempts (Canfield et al., 2016). Active learning methods—such as simulations, gamified efforts, and role-playing environments—generally have the most impact as an awareness or training opportunity strategy due to their inherent nature of engaging learning activities and the reinforcement of secure actions. Even effective training and awareness methods have the problem of retention: as observed, individuals can become less aware of phishing and security practices if individuals stop receiving periodic engagements (Parsons et al., 2019). This reinforces the idea of selecting effective awareness or training methods but also incorporating periodic refreshers and assessments to maintain awareness.

- **Conceptual Frameworks**

Theoretical frameworks are invaluable in shaping our understanding of how users behave in cybersecurity situations. One theory, Protection Motivation Theory (PMT), has been and continues to be a leading, well-accepted model of explaining how people evaluate threats and their decisions on protective actions (Rogers, 1983). PMT suggests that an individual engages in protective behaviour based on two cognitive processes: the threat appraisal and coping appraisal. The threat appraisal process involves evaluating the severity of a perceived threat and the individual's vulnerability to it, while coping appraisal process involves evaluating the response efficacy of the protective behaviour, self-efficacy to execute the behaviour, and costs of completing the behaviour.

In the context of phishing, PMT suggests that a person is more likely to engage in some "secure" behaviour, such as reporting phishing emails or avoiding malicious links, when they believe phishing is a serious threat, they are personally vulnerable, the secure behaviour will be effective, and they can execute the behaviour (Chen et al., 2021). The constructs of PMT can support the design of interventions that inform but also empower educators to respond to the phishing threats appropriately.

Conceptual Framework

In this study, we present a conceptual framework founded on Protection Motivation Theory (PMT) that explores the processes by which phishing awareness training improves the ability of educators to recognize and respond to phishing attempts. Specifically, the framework examines PMT constructs as mediators between training intervention and behavioural outcomes regarding recognition and response to phishing.

Variables

- **Independent Variable**

The central independent variable is the training intervention, which was operationalized as two training conditions: a control group that experienced no or passive training and an interactive training group that experienced active learning strategies, such as simulations and role-playing exercises.

- **Mediators**

Inspired by PMT there are four mediating variables:

  - **Self-efficacy:** Belief in one's ability to recognize and respond to phishing attempts.
  - **Perceived severity:** One's belief about the severity of the consequences of being a phishing victim.
  - **Perceived vulnerability:** The degree to which individuals believe they are personally vulnerable to receive phishing attempts.
  - **Response efficacy**: The degree to which one believes the recommended protective behaviours (such as reporting suspicious email) can reduce phishing risk.

- **Dependent Variable**

The outcome of interest is the ability to recognize and respond appropriately to phishing attempts, measured through behavioural intention and actual performance on phishing detection tasks.

- **Theoretical Foundation and Hypotheses**

In reference to PMT, the study hypothesizes that interactive training can improve phishing detection directly and indirectly because of its effect on cognitive appraisals related to PMT. Therefore, the following hypotheses will be examined:

H_1: Educators that participate in interactive phishing awareness training will show a greater increase in their ability to detect phishing compared to the control group.

H_2: The relationship between the training intervention and phishing detection, where there is an increase in detection, will be mediated by PMT factors—self-efficacy, perceived severity, perceived vulnerability, and response efficacy.

H_3: Among interactive training's formats, role-playing and phishing simulations will be more effective than passive type instructional methods.

This conceptual framework supports a greater understanding of how specifically designed awareness interventions can be enhanced to improve cybersecurity behaviour of educators in cognitive and behavioural aspects.

Proposed Methodology

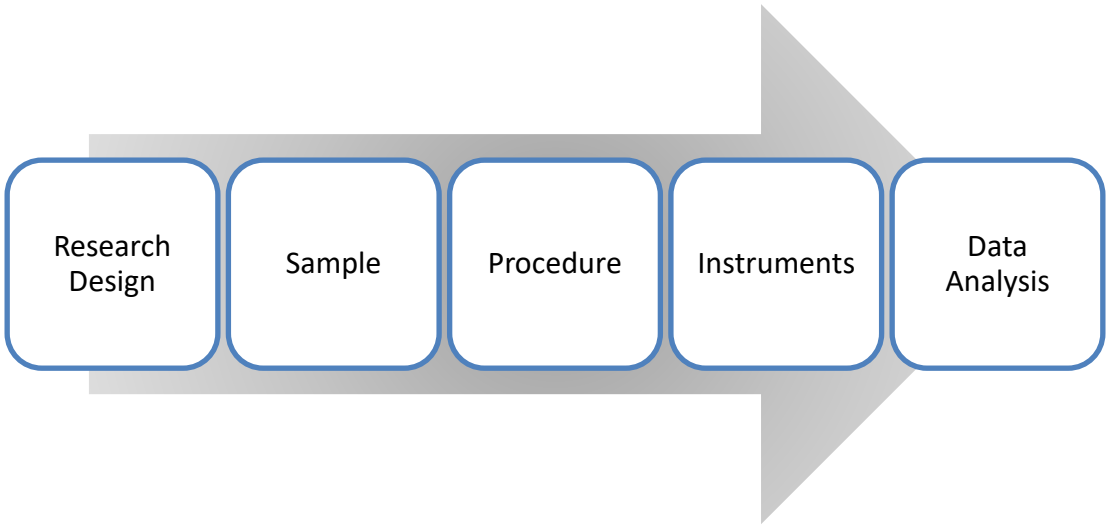

Fig. 2: Process of Proposed Methodology

Research Design

This research will utilize a quasi-experimental pre-test/post-test design with experimental and control groups. Participants will be randomly assigned to either the experimental group, receiving interactive phishing awareness training, or the control group, receiving passive training. This design allows us to determine a change in phishing awareness and behavioral intention due to the training intervention.

Sample

The sample will be approximately 100 educators from both secondary and tertiary educational institutions. Participants will be randomly assigned to either an experimental or control group, achieving equivalency between groups and reducing selection bias. This sample size will allow for sufficient statistical power to obtain a meaningful test of effects.

Procedure

- **Pre-Test**

Participants will complete a baseline phishing awareness survey and will be exposed to a group of simulated phishing emails. These emails will be used to assess phishing detection skills at baseline.

- **Intervention**
  - **Experimental group:** Participants are exposed to interactive training consisting of phishing simulations, group discussion, and scenario-based exercises. The training is meant to actively engage learners in the material.
  - **Control group:** Participants will receive passive training primarily focused on informational handouts and static educational materials regarding the risks of phishing and prevention.
- **Post-test**

After the intervention, participants will fulfill the same phishing awareness survey and simulated phishing tasks that were presented at pre-test to assess participants' degree of improvement in detection accuracy and awareness.

Instruments

- **Phishing Awareness Survey**

Based on Parsons et al. (2019), the instrument evaluates participants' awareness of phishing threats, as well as strategies to avoid phishing.

- **Simulated Phishing Scenarios**

To objectively assess participants' ability to identify phishing attempts and take appropriate action, realistic phishing email scenarios will be implemented.

- **PMT-Based Questionnaire:**

A validated measure of Protection Motivation Theory constructs (perceived severity, perceived vulnerability, response efficacy, and self-efficacy) will be used to account for cognitive and motivation elements of protection motivation behaviour.

Data Analysis

- **Statistical Tests**

We will use paired-sample t-tests to evaluate within-group differences in phishing awareness and detection performance from the pre-test to the post-test data collection timepoints. We will analyse between-group differences using analysis of covariance, while controlling for pre-test/baseline scores.

- **Mediation Analysis**

To test for the mediating effects of PMT constructs on the relationship between training type and phishing detection, we will conduct mediation analyses following published statistical methods (e.g., Baron & Kenny approach or structural equation modeling).

We expect that participants in the experimental group with interactive phishing awareness training will have significantly more phishing detection and awareness than participants in the control group. Participants in the experimental group will see improvements in their performance-based detection accuracy and behavioural intention-based reporting of suspicious emails.

In addition, we expect these improvements to be mediated through Protection Motivation Theory (PMT) constructs, specifically increased perceptions of vulnerability and severity, self-efficacy, and beliefs of effectiveness of protective behaviours. In this respect, we expect motivation and cognition to play an important role of influencing changes that occur above and beyond changes in knowledge.

Of the various interactive training formats, we believe that role-playing and phishing simulations will lead to the largest increases in phishing awareness and phishing response effectiveness. We expect these experiential learning activities will lead to more engagement, increase educational experiences, and builds educator confidence when responding to phishing, all of which will lead to longer-lasting and more impactful outcomes.

Discussion

This research highlights the importance of theory-based, interactive interventions uniquely designed for educators to increase phishing awareness and promote lasting behaviour change. In contrast to conventional training methods that focus on passive knowledge transfer, this conceptual design highlights the needs for motivation and active participation as necessary drivers for sustainable positive changes in cyber-security behaviours. The study is grounded in Protection Motivation Theory which places cognitive appraisals -- perceived vulnerability, severity, and self-efficacy -- at the canter of the mechanisms that mediate or facilitate the intervention's effectiveness in training programs.

The potential results have significant implications for institutional cyber-security policy and the design of continuing educational initiatives at the institutional level. Creating interactive phishing awareness components to routine training can significantly improve the resiliency of educators to the risk associated of cyber-attacks in institutions, ultimately protecting students' and institutional sensitive data. Lastly, the findings could be leveraged to create more granular and contextualized case for cybersecurity education addressing the contemporary challenges of educators which many in the field remain unserved.

Nevertheless, there are some limitations that should be discussed. The use of self-reported measures of phishing awareness and behavioural intentions carries the risk of social desirability bias, which in turn could lead to overstating reported improvements. There is also the risk of self-selection bias—the possibility that individuals who chose to take part in the study may already have existing levels of cybersecurity awareness and/or motivation—that could affect the generalizability of the study's results. In addition, there are differences across educational institutions, such as differences in resources, infrastructure and culture that may influence the applicability of findings in different contexts.

In terms of addressing these limitations, longitudinal follow-up studies should be completed to track the ongoing nature of awareness gains, and the sustainability of observed behavioural changes over time. Research in this area would provide useful information on how often refresher training would be required to maintain an optimal level of vigilance. Future research could also explore ways to scale the interactive training interventions to other groups, including students—who represent a significant component of the overall digital ecosystem in schools and universities—and test their effectiveness against the online phishing threat.

Conclusion

Educators are an important yet under-studied group regarding phishing awareness and cybersecurity education. This study provides a framework that is rooted in theory to not simply improve knowledge, but develops educators' ability to recognize and respond to phishing morally and securely, by adding Protection Motivation Theory to rigorous experimental design. Advancing motivational and cognitive strategies, while observing behavioural outcomes, will provide a more advanced approach to deeper behavioural change.

This study's implication is greater than the educator alone; it is a step toward the greater institutional resiliency against cyber threats and a safer environment in educational spaces. Ultimately, increasing the cybersecurity awareness of educators not only protects educator and institution level data, but supports the moral and security of a digital classroom as a whole, to the benefit of students and the community at large.

References

1. Algarni, A., Xu, Y., & Chan, T. (2017). Susceptibility to phishing attacks: A behavioral decision-making perspective. *Computers in Human Behavior, 68*, 129–141. https://doi.org/10.1016/j.chb.2016.11.011

2. Alqaralleh, B., Alsmadi, I., & Batarfi, O. (2020). Cybersecurity awareness for university students: A case study. *Journal of Information Security and Applications, 55*, 102590. https://doi.org/10.1016/j.jisa.2020.102590

3. Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors, 58*(8), 1158–1172. https://doi.org/10.1177/0018720816666073

4. Chen, H., Beaudoin, C. E., & Hong, T. (2021). Cybersecurity behaviors and protection motivation theory: A literature review. *Computers & Security, 104*, 102212. https://doi.org/10.1016/j.cose.2021.102212

5. Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. *Computers & Security, 88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

6. Keller, K., Kim, H., & McCracken, J. (2021). Cybersecurity risks in higher education: The need for comprehensive policies. *Journal of Higher Education Policy and Management, 43*(6), 645–659. https://doi.org/10.1080/1360080X.2021.1958574

7. Olowookere, T. A., et al. (2025). Cybersecurity awareness among radiography educators in Africa. *BMC Medical Education, 25*(1), 755. https://doi.org/10.1186/s12909-025-03755-9

8. Parsons, K., et al. (2019). Human factors in phishing susceptibility: Understanding individual differences. *Journal of Information Security, 10*(3), 255–270. https://doi.org/10.4236/jis.2019.103015

9. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology* (pp. 153–176). Guilford Press.

10. Rogers, S., & Jones, P. (2022). Cybersecurity challenges in universities: A case study analysis. *Education and Information Technologies, 27*(3), 3101–3118. https://doi.org/10.1007/s10639-021-10762-4.