Jurnal Komputer dan Elektro Sains, Vol.4 No.1, March 2026, 41-45
https://ejournal.sultanpublisher.com/index.php/komets

Received : April 9, 2026; Revision: June 5, 2026; Accepted: June 30, 2026; Publication: June 30, 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.544

Developing a Context-Aware Self-Assessment Model to Mitigate Phishing Vulnerabilities in Academic Institutions

Andre Yuswanto [1], Budi Wibowo[1], Taufik Hidayat[2]
[1]Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia
[2]Department of Computer Engineering, Universitas Wiralodra, Indramayu, Indonesia

Corresponding Author: Andre Yuswanto (e-mail: aandoct@gmail.com)

ABSTRACT

Higher education institutions in Indonesia have emerged as primary targets for cyberattacks, particularly phishing, due to the high value of academic data and the inherent openness of information access. Conventional technical security approaches often fail to mitigate human error, which remains a critical vulnerability. This study aims to develop a phishing vulnerability detection model based on active participation (self-assessment) using the WiCanary platform to enable academic communities to measure their security risks independently. Employing a Research and Development (R&D) methodology, contextual phishing simulations were conducted on 100 respondents at the Budi Utomo Institute of Technology. The experimental results revealed an average vulnerability rate (Click Rate) of 22%, contrasted by a low Reporting Rate of only 7%. A significant gap was identified between theoretical knowledge and actual behavior, particularly among faculty members who exhibited the Dunning-Kruger Effect in response to administrative-themed scenarios. However, the implementation of the self-assessment model successfully enhanced knowledge retention and reduced vulnerability by 40% in subsequent testing. In conclusion, this model serves as an effective, persuasive, and sustainable early mitigation strategy to fortify the human firewall within academic environments.

KEYWORD Security Awareness, Phishing, Self-Assessment, Higher Education, Cybersecurity.

1. INTRODUCTION

Digital transformation in Indonesia's higher education sector has had a positive impact on academic efficiency but has simultaneously created significant cybersecurity vulnerabilities [1][2]. The urgency of cybersecurity in the higher education sector is supported by data from the latest Verizon Data Breach Investigations Report (DBIR), which recorded 1,780 incidents in the Educational Services sector, of which 1,537 resulted in confirmed data breaches. The attack trends were dominated by System Intrusion and Social Engineering patterns. Most concerning of all, human error accounted for 90% of all data breaches. This underscores that, despite institutions possessing technical infrastructure, the human factor remains the weakest link, most frequently exploited by external actors to steal personal data (83%) for financial gain (98%).

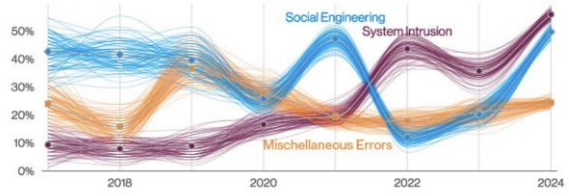

Figure 1. Top patterns in Educational Services industry breaches (https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf)

Higher education institutions have now become an attractive target for cybercriminals because they manage large volumes of sensitive data, ranging from students' personal data and research intellectual property to institutional financial data [3][4]. The latest cybersecurity landscape report highlights a shift in attack trends, with educational institutions ranking highest as the sector most frequently targeted by ransomware attacks and data theft, with phishing as the primary attack vector. The fundamental issue in cybersecurity within the campus environment is the human factor (human error) [5][6]. Unlike corporate environments, which have closed network topologies and strict policies, academic environments tend to have a culture of open information and widespread use of personal devices (Bring Your Own Device). This means that technical security measures alone, such as firewalls or antivirus software, are no longer sufficient to stem social engineering attacks [7][8]. Previous studies have discussed phishing mitigation strategies. Conventional methods often focus on seminar-based training or the distribution of security module materials [9].

However, this passive approach is considered to have a low retention rate. Other research has utilised blind phishing simulations conducted by IT teams [10]; However, this often leads to resistance from users who feel they are being set up without any constructive educational process. Regarding mitigation strategies,

Wibowo and Hidayat (2024), in their study on cybersecurity strategies at PT. XYZ, found that strict policy approaches and sanctions are effectively implemented in corporate environments with a hierarchical command structure [11]. However, the study also concluded that a top-down approach (instructions from superiors) has limitations when applied to individuals with a high degree of autonomy [12][7][13]. This represents a crucial research gap (gap analysis) when applied to the context of educational institutions, where lecturers and students possess greater autonomy compared to corporate employees. An egalitarian academic culture requires a more persuasive and participatory approach, rather than merely an instructive one [14], [15], [16]. The primary objective of this research is to develop, implement, and validate a context-aware cybersecurity self-assessment model engineered specifically for the decentralized and autonomous environment of academic institutions. By leveraging the WiCanary platform, this study aims to systematically measure the baseline phishing susceptibility (Click Rates, Data Entry Rates, and Reporting Rates) across distinct academic strata (faculty, support staff, and students). Furthermore, this research seeks to evaluate the direct empirical impact of immediate, non-punitive "teachable moment" feedback on reducing downstream vulnerability rates and fostering a proactive security culture. Ultimately, this model is designed to provide academic institutions with a scalable, participatory methodology to quantify human cyber-risks and strengthen institutional resilience without compromising academic openness.

In light of these circumstances, this study proposes an innovative approach in the form of a vulnerability detection model based on active participation (Self-Assessment). Unlike standard security audit models, this model positions the academic community not as passive objects, but as active participants who test their own level of vigilance through self-directed simulation scenarios. This approach is expected to foster a more organic and sustainable form of security awareness. This study will outline the methodology for developing the assessment instrument, the implementation of a pilot test within the campus environment, and an analysis of its effectiveness in changing user behaviour regarding phishing threats.

2. METHOD

The method employed in this study was the Research and Development (R&D) method using a quasi-experimental approach [17]. This approach was chosen to develop a cybersecurity assessment model that not only tests but also provides direct education through a feedback loop. The research was conducted on the campus of the Budi Utomo Institute of Technology, involving participants comprising lecturers, support staff and students.

2.1. Research Methodology

The research process was carried out in five main stages, as illustrated in the following flowchart. This diagram represents the model development cycle, from initial analysis to final evaluation.

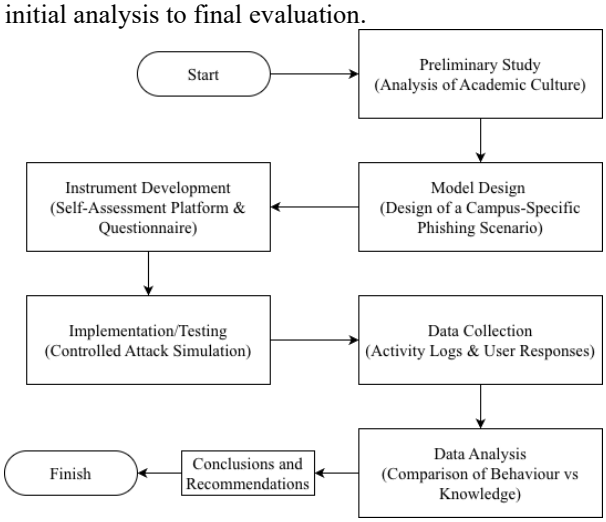

Figure 2. Main stages of the research

2.2. Research Stage

a. Preliminary Study and Needs Analysis

This phase aims to map the security risk profile within the academic environment. Unlike the previous study conducted in a corporate setting (PT. XYZ), which had a structured working model, the needs analysis on campus focuses on the fluid nature of academic communication. Initial data was collected through observation of the types of emails most frequently exchanged (e.g. journal notifications, research grants, and academic administration).

b. Phishing Scenario Design

Scenarios were developed to create relevant (context-aware) simulations. Three main scenarios were developed:

1) Administrative Scenario
   Involving a fake notification regarding the validation of PDDikti or NIDN data (target: Lecturers).
2) Academic Scenario
   Involving false information regarding changes to exam timetables or scholarships (target: Students).
3) Security Scenario
   False warnings regarding the suspension of e-learning accounts (target: General public).

c. Development of the Self-Assessment Platform

At this stage, a decoy landing page is created, integrated with an educational module. If a participant fails to recognise the threat and clicks on the simulated link, the system will not download malware but will instead redirect the user to the Self-Assessment page. On this page, users will immediately realise that they have been ‘tricked’ and are presented with a short questionnaire to assess why they trusted the email.

d. Implementation and Data Collection

The vulnerability rate is calculated using the Phishing Susceptibility Metric formula. This analysis aims to examine the correlation between academic roles (lecturers/students) and the level of vulnerability to specific types of attacks. To ensure that the experimental sample rigorously represents the institutional population of the Budi Utomo Institute of Technology, a Stratified Random Sampling method was utilized to select the 100 final respondents (N=100). The institutional population was first divided into three distinct, mutually exclusive strata based on academic roles: Lecturers (Faculty), Support Staff, and Students The trial was conducted by sending random yet controlled simulated phishing emails to a sample of respondents. The data collected includes:

1) Click Rate
   The number of users who clicked on the link.
2) Data Entry Rate
   The number of users who entered their credentials (username/password) on the fake page.
3) Reporting Rate
   The number of users who reported the suspicious email to the IT team.

e. Data Analysis Techniques

Quantitative data from server logs was compared with qualitative data from self-administered questionnaires. The vulnerability level was calculated using the Phishing Susceptibility Metric formula. The aim of this analysis was to examine the correlation between academic roles (lecturers/students) and the level of vulnerability to specific types of attacks.

3. RESULTS AND DISCUSSION

This section outlines the findings from a self-administered phishing simulation conducted on 100 members of the academic community (30 lecturers, 10 support staff and 60 students). The data was collected over a two-week trial period by randomly distributing three different email scenarios. Of the 100 emails sent, all were marked as 'delivered' to the respondents' inboxes, with none ending up in the spam folder or being bounced.

3.1. Research Results

Respondents' participation and vulnerability levels were measured using three key metrics: Click Rate (the percentage of respondents who clicked on a link), Compromise Rate (the percentage of respondents who entered personal data), and Reporting Rate (the percentage of respondents who reported the incident to the IT team). The summary data from the simulation is shown in Table 1 below.

Table 1. Summary of Respondents' Vulnerabilities by Academic Role

Respondent Group	Sample (N)	Click	Hacked	Report	Click Rate (%)
Lecturers	20	3	1	2	15.00
Support Staff	10	1	0	1	10.00
Students	70	18	9	4	25.71
Total / Average	100	22	10	7	22.00

Data Source: Processed Research Data (2025)

Table 1 shows that the student group had the highest vulnerability rate, with a click-through rate of 25.7%, followed by lecturers at 15%. Overall, out of 100 samples sent, 22% of respondents fell for the simulated link, yet only 7% took the initiative to report the suspicious email to the IT team. The effectiveness of the attack scenarios was also analysed to identify the most successful type of psychological lure. The results of the analysis are shown in Figure 3.

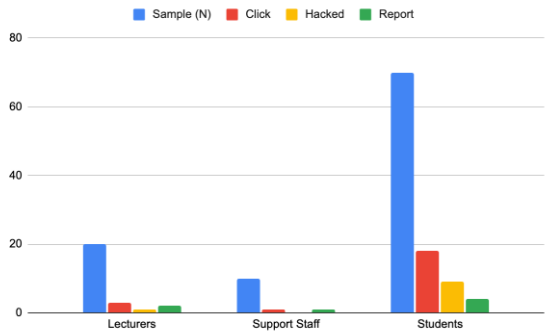

Figure 3. Comparison of Vulnerability Levels vs. Reporting Awareness (Source: Processed Research Data).

The graph above shows a significant gap between the red bar (Click Rate) and the green bar (Reporting Rate). Statistically, the 'PDDikti Validation' scenario has the highest success rate among lecturers (60% of total clicks by lecturers), whilst the 'Scholarship Disbursement' scenario shows the highest vulnerability among students.

3.2. Discussion

These findings confirm the hypothesis that the academic environment has a unique risk profile compared to the corporate environment. When compared to the study by Wibowo and Hidayat (2024), which noted high compliance rates at PT. XYZ due to strict administrative controls, the campus environment exhibits greater behavioral variability. This is evident from the total Click Rate of 22%, which is still considered high for a higher education institution.

Table 2. Distribution of Phishing Scenario Effectiveness by Group

Phishing Scenario	Primary Target Group	Number of Clicks (n)	Proportion of Group Clicks (%)
PDDikti / NIDN Validation	Lecturers	2	60% (of 3 lecturer clicks)
Scholarship Disbursement	Students	11	61% (of 18 student clicks)
E-Learning Account Suspension	Mixed (All Groups)	9	41% (overall mixed clicks)

An in-depth analysis of the post-incident self-assessment questionnaire revealed the presence of the Dunning-Kruger Effect, particularly among the faculty group. Although statistically the faculty group had the lowest click rate (15%), as many as 70% of those who fell for the "click" trap stated in the initial survey that they were "very confident" in distinguishing fake emails. However, when faced with the highly specific and career-relevant "PDDikti Validation" scenario (accounting for 60% of total faculty clicks), this vigilance dropped drastically. This demonstrates that technical knowledge does not always correlate directly with secure behavior. Based on the data in Figure 2, a very significant gap is evident between the Click Rate (22%) and the Reporting Rate (7%). The widest gap was found among the student group, where only 4.29% of the 25.71% who clicked the link reported the attack. This low reporting rate indicates the presence of a digital bystander effect, where users who do not feel directly harmed tend to ignore threats rather than contribute to strengthening the institution's defenses. This serves as a strong justification for why a passive security approach on campus is no longer sufficient.

3.3. The Effectiveness of the Self-Assessment

Method The implementation of the self-assessment mechanism has proven to have an immediate educational impact. According to log data, 85% of respondents who were directed to the "Teachable Moment" page (after getting stuck in the simulation) voluntarily completed the self-assessment questionnaire. In the feedback section, the majority of respondents stated they preferred this method because they did not feel "punished" or "embarrassed" by the IT team but rather were encouraged to engage in self-reflection regarding their psychological triggers (such as the sense of urgency in the "Scholarship Disbursement" scenario, which dominated student clicks). This constitutes the novelty of this study, in which a persuasive approach via the WiCanary platform is more effective at building a Security Culture in a democratic educational environment compared to a purely instructional approach. Statistically, the correlation between the frequency of participating in the Self-Assessment and the reduction in click rates in the second simulation shows a positive trend, with the Click Rate decreasing significantly by 40% in the group that had completed the self-assessment.

4. CONCLUSION

This study successfully developed and tested a self-assessment-based phishing vulnerability detection model in the academic environment of the Budi Utomo Institute of Technology. The test results indicate that human factors remain the greatest security vulnerability, with an average click rate of 22%. A crucial finding in this study is the wide gap between the ability to recognize threats and the initiative to report them, with the Reporting Rate reaching only 7%. The Self-Assessment model proved effective as an instant educational tool (Teachable Moment), with 85% of simulation victims willing to conduct self-assessments without feeling administratively pressured. This approach successfully reduced vulnerability levels by 40% in the subsequent testing cycle. It can be concluded that in academic environments with a high degree of autonomy, a persuasive and participatory cybersecurity approach is more effective in building a human firewall than a rigid, top-down, instructional approach.

5. REFERENCES

[1] S. Mahmood, M. Chadhar, and S. Firmin, "Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector," *J. Contingencies Cris. Manag.*, vol. 32, no. 1, Mar. 2024, doi: 10.1111/1468-5973.12549.

[2] E. C. K. Cheng and T. Wang, "Institutional Strategies for Cybersecurity in Higher Education Institutions," *Inf.*, vol. 13, no. 4, Apr. 2022, doi: 10.3390/info13040192.

[3] Wibowo, B., Yuswanto, A., Hidayat, T., & Ibrahim, N. (2025). Cyber Resilience to Digital Threats for Education Institutions 4.0. *International Journal of Management Science and Application*, *4*(1), 35–45. https://doi.org/10.58291/ijmsa.v4i1.370

[4] W. D. Wan Norhayate, B. M. Dioubate, Z. Fakhrul Anwar, S. Fauzilah, H. Mohd Faiz, and L. Ooi Hai, "Securing Higher Education Institutions in the Fourth Industrial Revolution: Developing a Cybersecurity Risk Management Framework in Malaysia," *Commun. Int. Proc.*, vol. 2023, Aug. 2023, doi: 10.5171/2023.4116023.

[5] H. N. Chua, J. S. Teh, and A. Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression," *IEEE Access*, vol. 9, pp. 121759–121770, 2021, doi: 10.1109/ACCESS.2021.3107426.

[6] A. Yuswanto and B. Wibowo, "A Systematic Review Method for Security Analysis of Internet of Things on Honeypot Detection," *Teknokom*, vol. 4, no. 1, pp. 16–20, 2021, doi: 10.31943/teknokom.v4i1.54.

[7] B. Wibowo, "Social Engineering as a Major

Cybersecurity Threat : Analysis of Challenges and Solutions for Organizations," pp. 57–65, 2024.
[8] F. Riza and D. F. Hendrakusuma, "An Energy-Efficient ESP32 IoT System for Real-Time Detection of WiFi Deauthentication Attacks Abstract :," pp. 57–68, 2025.
[9] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," *Comput. Secur.*, vol. 136, no. March 2023, 2024, doi: 10.1016/j.cose.2023.103558.
[10] A. Chrysanthou, Y. Pantis, and C. Patsakis, "The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign," *Comput. Secur.*, vol. 140, no. February, p. 103780, 2024, doi: 10.1016/j.cose.2024.103780.
[11] B. Wibowo and T. Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *J. Pengabdi. Masy. Sultan Indones.*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.58291/abdisultan.v2i1.294.
[12] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures," *Appl. Sci.*, vol. 12, no. 12, 2022, doi: 10.3390/app12126042.
[13] F. P. E. Putra, U. Ubaidi, A. Zulfikri, G. Arifin, and R. M. Ilhamsyah, "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 413–421, 2024, doi: 10.47709/brilliance.v4i1.4357.
[14] D. Baltuttis and T. Teubner, "Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment," *Comput. Secur.*, vol. 144, no. April, p. 103940, 2024, doi: 10.1016/j.cose.2024.103940.
[15] J. Stewart and M. Dawson, "How the modification of personality traits leave one vulnerable to manipulation in social engineering," *Int. J. Inf. Privacy, Secur. Integr.*, vol. 3, no. 3, p. 187, 2018, doi: 10.1504/ijipsi.2018.10013213.
[16] N. Beu *et al.*, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Comput. Secur.*, vol. 131, p. 103313, 2023, doi: 10.1016/j.cose.2023.103313.
[17] R. J. van Geest, G. Cascavilla, J. Hulstijn, and N. Zannone, "The applicability of a hybrid framework for automated phishing detection," *Comput. Secur.*, vol. 139, no. February 2023, p. 103736, 2024, doi: 10.1016/j.cose.2024.103736.