Beyond Technology: Investigating the Impact Of Phishing Emails on Human Behavior and Decision-Making in Educational Institutions

Bhim Chandra Gautam*
Sudan Jha**

ABSTRACT

Phishing emails remail a persistent and evolving threat, particularly in educational institutions, where sensitive data and intellectual property are frequently targeted. Attackers create successful phishing by exploiting human vulnerabilities by sending out trustworthy-looking emails which leads to severe consequences for educational institutions. Phishing emails are beyond the technical aspects of cybersecurity and more towards cyber awareness of users. Decision making process and responses of staff, faculty and students towards phishing emails sheds to non-technical factors contributing to successful phishing attempts. We identify key psychological triggers and contextual influences that lead to compromised security. This research explores the need for comprehensive strategists and develop the strategy in the context of human behavior for phishing emails which address human behavior in cybersecurity and behavior modification to mitigate the risks of phishing attacks in educational institutional.

Keywords : Phishing Emails, Human Behavior, Educational Institutions, Cybersecurity, Decision-Making, Social Engineering, Security Awareness, Psychological Triggers

**Bhim Chandra Gautam is PhD scholar at Faculty of Computer Science and Engineering, Kathmandu University.*
***Prof. Sudan Jha, PhD is Professor in AI at Faculty of Computer Science and Engineering, Kathmandu University.*

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

1. INTRODUCTION

Phishing in education institution is likely to happen in huge target as there are different categories of students and it is quite easy for attacker to attract them into phishing activities. Attacker designed to deceive individuals into divulging sensitive information, has been growing in sophistication and in high frequency in education sector. Most of the cybersecurity focuses on core technical countermeasures such as email filters, encryption, and anti-malware software, phishing largely exploits human vulnerabilities. Faculty members, administrative staff, and students are often the targets, with attackers using psychological manipulation to gain access to institutional networks and its access.

Today's most of the education institutions relay heavily on digital platforms for communications, record-keeping, and academic research, human-centric cybersecurity breaches can have far-reaching consequences. Phishing is not only a technical issue but also a human behavioral one, influenced by trust, urgency, curiosity, and other psychological factors. This research aims to identify the factors affecting decision-making and the behaviors that lead to phishing email compromises in educational institutions rather than others industries. Mainly with the behavior aspects of students, faculty and administrative staffs who uses emails for their day-to-day activities, who are always open to phishing attacks from emails.

2. LITERATURE REVIEW

The most prevalent and damaging forms of cyber-attacks has been phishing attacks, particularly in environments where personal and sensitive data are abundant, such a as educational institutions. The increasing use of emails ad digital communication tool in academic settings has opened significant avenues for phishing attempts [1]. This section shows how such attacks effects students, teachers, and administrative staff. The literature also explores how human behaviors, decision-making processes, and institutional cybersecurity strategies contribute to the vulnerability.

2.1 Phishing in Educational Institutions

Cybercriminals have been making educational institutions prime targets after banking sector due to the vast amount of sensitive data they have, including students records, financial information, research data, and intellectual property. Phishing aims to disclosing login credentials, personal information, or financial data. In June of 2023, a ransomware attack on the University of Machester resulted in the exfiltration of PII for staff, alumni, and students, plus a 250GB data set that contained the health records of 1.1 million NHS patients. It appears the breach was the result of a VPN exploit, as the university removed access to their GlobalProtect VPN shortly after the incident occurred [2].

Diverse set of vulnerabilities are created as there is wide array of users a college or university

https://www.nepjol.info/index.php/njmsr https://doi.org/10.53056/njmsr-2025.8.1.003

-from students and faculty to administrative staff – frequent exchange of emails which is fundamental aspect of daily operations. In college/ Universities Business Email Compromise (BEM), a hacker gains controls of a one of the internal email accounts and uses that access for financial gain. Threat actor start to send out fake emails requesting for different purpose and gain a golden trust. Which in later on even used for transfer of funds from any party to nay third-party vendors with which educational institutional have business.

2.2 Phishing and Human Vulnerability in Education Settings

Due to common psychological and behavioral traits phishing attacks are successful. Phishing attacks rely on "heuristic-based" decision making, limited information with individuals force to make a quick judgment and take action. In busy educational environments where individuals are bombarded with multiple tasks and communications, leading to decision being made under cognitive overload. Human susceptibility to phishing is a function of several factors, including cognitive biases, stress, lack of training, and overconfidence.

According to a 2023 study by Shukla and Sharma, Educational institutions are especially vulnerable because of the diversity of their users: Faculty and teachers are typically experts in their fields but may lack advanced knowledge of cybersecurity. Students, lack awareness of common phishing tactics and are often targeted with emails that appear to offer services such as scholarships, internships, or technical support. Administrative staff are particularly susceptible to phishing emails disguised as routine administrative tasks, such as budgetary approvals or account verifications [3].

2.3 Phishing and Teachers in Educational Institutions

Teachers play a critical role in the daily operations of educational institutions, often relying heavily on email for communication with students, administrators, and external bodies. Phishing campaigns targeting teachers usually exploit position of authority or impersonate senior administrators to trick then into sharing sensitive information. According to a 2023 study by Akinola, teachers are particularly susceptible. It was found that nearly 35% of the teachers surveyed had clicked on links in phishing emails or entered personal information when prompted, largely due to the perceived legitimacy of the email's source [4].

2.4 Phishing and Students in Educational Institutions

Students are among the most frequently targeted groups in phishing attacks on educational institutions. Lack of cybersecurity awareness and experiences in identifying phishing scams students are most vulnerable. Spoofed email addresses, misleading URLs, and attachments which are the basic phishing techniques on which digital-native modern students are unfamiliar. Scholarship offers, tuition payments portals, and internship opportunities and their urgency and relevance of these emails lead students to respond without thoroughly verifying the sender's legitimacy.

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

2.5 Phishing and Administrative Staff

Administrative staff in educational institutions are responsible for managing the day-to-day operations of the institution, including financial transactions, student records, and internal communication. Phishing campaigns targeting these staff members often involve spear-phishing tactics, where emails are tailored to mimic legitimate internal communications. A study has found that administrative staff are at higher risk of phishing due to the high volume of emails they handle daily, which often leads to decreased diligence in verifying email authenticity. The study also highlights that phishing attempts targeted at administrative staff often include malicious attachments or links that install malware, potentially compromising entire institutional systems [5].

2.6 Role of Human Behavior in Phishing Susceptibility

As attacker primarily exploit cognitive biases and behavioral patterns, phishing emails often trigger emotional responses such as fear, urgency, or curiosity, leading to quick and unthinking actions by recipients. The fear of missing out or fear of penalties has been shown to be a common motivator that compels individuals to respond to phishing emails, even when they posses basic knowledge of phishing risks.

A key element in phishing success is decision fatigue, where the individual is mentally overloaded and thus more likely to make a hasty decision without fully considering the consequences. This is particularly relevant in educational institutions where administrative staff, faculty, and students are constantly managing multiple tasks and priorities [5].

Gaps in security from Phishing in Educational Institutions

While there is a growing body of research on phishing in educational institutions, most studies focus on the technological aspects of phishing defenses. There is less emphasis on understanding the behavioral and psychological factors that influence phishing susceptibility. Existing literature does not sufficiently explore how different populations within educational institutions—such as teachers, students, and administrative staff—respond to phishing emails differently. Moreover, while phishing awareness programs are frequently cited as necessary, there is limited research on how to effectively design such programs to address human vulnerabilities specifically in academic environments [6,7,8,9,10].

This research aims to fill these gaps by focusing on the human elements of phishing in educational settings and exploring how behavioral training can mitigate the risks. By studying how various user groups interact with phishing attempts and analyzing their decision-making processes, this study seeks to contribute to more effective, behaviorally-informed cybersecurity practices in educational institutions.

https://www.nepjol.info/index.php/njmsr https://doi.org/10.53056/njmsr-2025.8.1.003

3. METHODOLOGY

The methodology employed in this research is a multifaceted approach that integrates quantitative and qualitative data collection, controlled phishing simulations, and advanced statistical and behavioral analysis to investigate the effects of phishing emails on human behavior within educational institutions. This section presents a detailed, technical breakdown of the procedures and algorithms applied throughout the research [11, 12].

3.1 Survey Design and Data Collection

The data collection process was conducted across several higher education institutions, targeting three key user groups: administrative staff, faculty members, and students. The methodology involved a combination of surveys, controlled phishing email simulations, and psychological analysis to assess phishing susceptibility and decision-making processes.

3.1.1 Survey instrumentation

A Structured survey was designed, incorporating Linkert-scale questions and multiple-choice response to quantitatively measure:

- **Cybersecurity Awareness Level (CAL):** Using a 5-point scale, respondents were asked about their familiarity with common cybersecurity threats, particularly phishing. The awareness score A_i for each individual i was computed as:

$$A_i = \frac{1}{n}\sum_{k=1}^{n} r_{ik}$$

Where r_{ik} represents the response score to question k and n is the total number of questions assessing cybersecurity awareness.

- **Phishing Experience (PE):** Respondents were asked about past encounters with phishing attacks, with the frequency of response (f_i) and response outcomes recorded. The phishing experience score was determined using:

$$PE_i = \frac{f_i}{N}$$

Where N is the number of phishing-related questions.

- **Risk Perception (RP):** Perceived risk when handling suspicious emails was evaluated using questions designed to gauge the likelihood of identifying potential phishing attempts. The average risk perception score was calculated by normalizing response values.

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

3.1.2 Controlled phishing simulations

In selected departments controlled phishing simulations were run to quantitatively measure real-time interactions with phishing emails. These simulations involved sending emails with various phishing tactics, including urgency, authority, and curiosity triggers. The following metrics were collected:

- **Response Rate (RR):** The proportion of recipients who interacted with the phishing email, defined as:

$$RR = \frac{n_{clicked}}{n_{sent}}$$

where $n_{clicked}$ is the number of recipients who clicked on the phishing link, and n_{sent} is the total number of phishing emails sent.

- **Response Time (T_r):** The time taken by each recipient to interact with the phishing email, measured in seconds. The distribution of response times was analyzed using a log-normal distribution model to underst and patterns in behavior.
- **Phishing Trigger Type (P_t):** Emails were designed with different psychological triggers, such as urgency, curiosity, and authority. The probability of response for each trigger type was modeled using logistic regression:

$$P(R = 1|T) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 T_1 + \beta_2 T_2 + \beta_3 T_3)}}$$

Where $T_1, T_2,$ and T_3 represent urgency, curiosity, and authority triggers, respectively, and $\beta_0, \beta_1, \beta_2, \beta_3$ are the regression coefficients.

3.2 Psychological and Behavioral Analysis

This section focuses on understanding the psychological and cognitive biases that leads to phishing email interactions. Behavioral data from both the survey and simulations were used to identify underlying factors influencing susceptibility.

3.2.1 Cognitive Bias Models

Cognitive biases were examined to assess their influence on decision-making. Three key biases were studied:

- **Authority Bias (B_a):** The probability of responding to emails perceived as coming from figures of authority was modeled using Bayes' Theorem:

$$P\ (B_a|R) = \frac{P(R|B_a)P(B_a)}{P(R)}$$

https://www.nepjol.info/index.php/njmsr https://doi.org/10.53056/njmsr-2025.8.1.003

where $P(R|B_a)$ is the likelihood of a response given authority bias, and $P(B_a)$ is the prior probability of authority bias influencing decisions.

- **Urgency Bias (B_u):** The susceptibility to urgent messages was analyzed using a time-based response function, where the likelihood of immediate interaction increased exponentially with perceived urgency:

$$P(B_u|t) = 1 - e^{-\lambda t}$$

Where t is the time since the phishing email was sent, λ is the urgency parameter estimated from response data.

- **Familiarity Bias (B_f):** Familiarity with the sender in^{i}reased the likelihood of response. The familiarity score (f_i) for each respondent was calculated based on past interactions with similar email patterns using a cosine similarity measure:

$$F_i = \frac{\sum_j s_{ij} \cdot t_{ij}}{\sqrt{\sum_j s_{ij}^2} \cdot \sqrt{\sum_j t_{ij}^2}}$$

where s_{ij} and t_{ij} represent the frequency of previous email interactions between recipient i and sender j.

3.2.2 Behavioral factors

Behavioral factors, such as multitasking, stress, and workload, were modeled using latent variables in a structural equation model (SEM). These factors were hypothesized to indirectly influence phishing susceptibility by altering decision-making capacities.

- **Multitasking Index (MI):** The multitasking index was calculated based on respondents' self-reported multitasking behavior and time spent on concurrent tasks, using a weighted average:

$$MI_i = \frac{\sum_k w_k t_{ik}}{\sum_k wk}$$

where w_k represents the importance of task k and t_{ik} is the time spent on task k by individual i.

3.3 Analysis Techniques

3.3.1 Statistical analysis

Statistical methods were used to correlate survey responses with simulation results. A multiple linear regression model was applied to quantify the impact of various factors on

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

phishing susceptibility:

$$S_i = \alpha + \beta_1 A_i + \beta_2 PE_i + \beta_3 RP_i + \varepsilon_i$$

Where S_i represent the susceptibility score of individual i, A_i is the awareness score, PE_i is the phishing experience score RP_i is the risk perception score, and ε_i is the error term. The coefficients $\beta_1, \beta_2, \beta_3$ were estimated using ordinary least squares (OLS) regression.

3.3.2 Mahine learning classification

A machine learning approach was employed to classify individuals based on their susceptibility to phishing. We implemented a Random Forest classifier with phishing simulation data as input features. The algorithm used the following steps:

- **Feature Extraction:** Key features, including response time, phishing trigger type, and individual characteristics (awareness, experience, risk perception), were extracted.
- **Training the Model:** The Random Forest algorithm was trained using labeled data from simulation results:

$$y = f(X)$$

where X represents the feature matrix and y is the binary response variable (clicked or not clicked).

Model Evaluation: The model's performance was evaluated using accuracy, precision, recall, and F1-score metrics.

This methodology employs a robust technical approach combining surveys, controlled simulations, cognitive and behavioral models, statistical regression, and machine learning techniques. The integration of quantitative and qualitative data provides a comprehensive analysis of how phishing emails influence human behavior and decision-making within educational institutions. The algorithms and models presented in this section are crucial for identifying key vulnerability factors and designing targeted interventions to mitigate phishing risks.

4. RESULT AND DISCUSSION

4.1 Key Factors Influencing Phishing Susceptibility

The results indicate that serval human factors significantly contribute to the success of phishing attacks in educational institutions:

Psychological triggers such as authority bias and urgency were dominant factors leading to phishing success.

https://www.nepjol.info/index.php/njmsr https://doi.org/10.53056/njmsr-2025.8.1.003

Lack of adequate training on recognizing phishing attempts. Nearly 92% of the surveyed population admitted they had not received recent or adequate phishing awareness training.

Workload and multitasking: Responders under high pressure or heavy workloads were more likely to interact with phishing emails without thoroughly analyzing them.

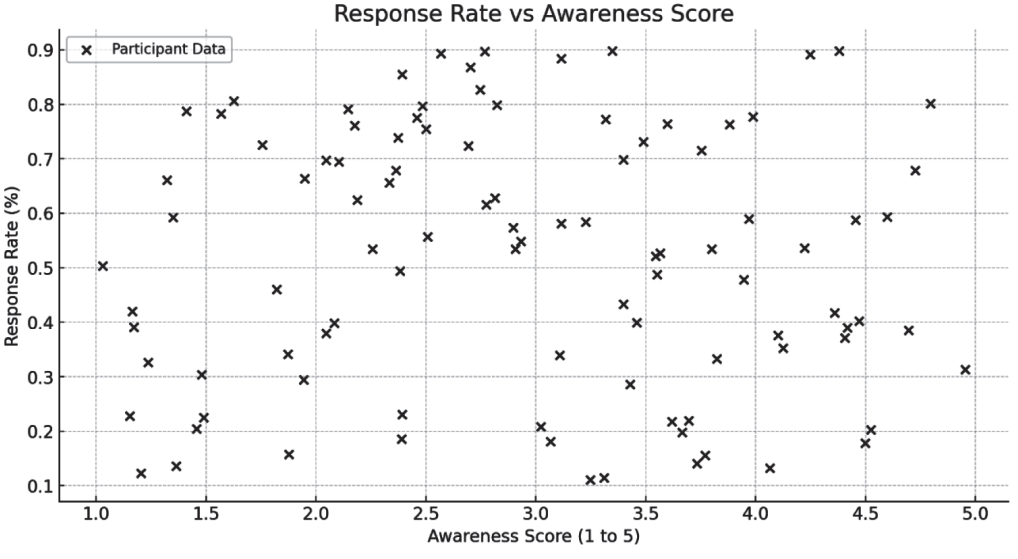

Fig1: Response Rate vs Awareness Score

The scatter plot shows no significant correlation between awareness scores and response rates (correlation: -0.02). This indicates that higher awareness does not necessarily prevent interactions with phishing emails, suggesting other behavioral factors at play.

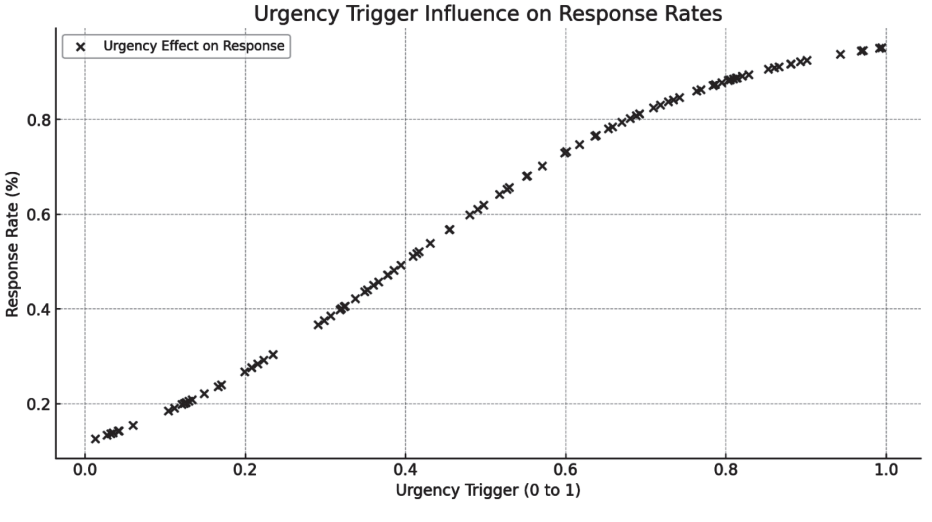

Fig2: Urgency Trigger Influence on Response Rates

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

The logistic regression plot highlights a strong relationship between urgency triggers and response rates. Higher urgency probabilities significantly increase the likelihood of responses, supporting the hypothesis that urgency biases contribute to phishing.

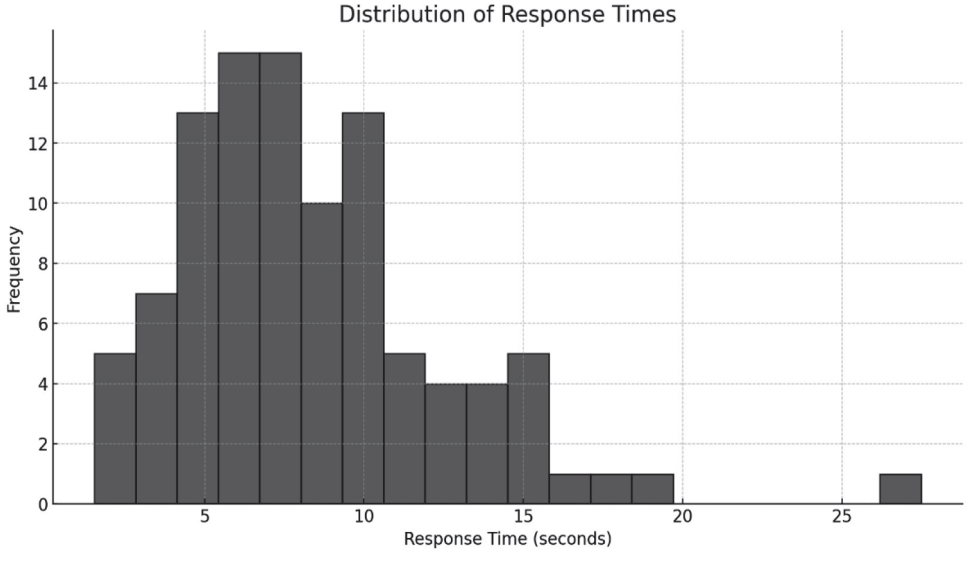

Fig3: Distribution of Response Times

The histogram of response times reveals a skewed distribution with most responses occurring within a short timeframe. This suggests that quick, impulsive decisions are common when responding to phishing emails.

4.2 Behavioral Impacts on Decision-Making

Many respondents mentioned they clicked on phishing emails because they were multitasking or in a rush. This highlights the importance of behavioral context in phishing susceptibility. Decision fatigue, where individuals are overwhelmed by numerous daily decisions, emerged as a crucial factor, leading to reduced diligence in verifying suspicious emails. Which also showed that awareness alone is not sufficient unless reinforced through continual, scenario-based training.

5. RECOMMENDATIONS

This study bridges that gaps by analyzing how urgency tactics, cognitive biases and decision making under pressure contribute to phishing susceptibility. Additionally, while major education institutions implement basic email security measures, the lack of targeted, behavior-driven training programs remains a major practical challenge. Above findings shows that human-centered innervations and technical controls both are necessary aspects to develop phishing control environment. Furthermore, education institutions with a cybersecurity culture encourage

reporting show lower phishing success rate, reinforcing the need for policy-level changes.

5.1 Behavioral Training and Awareness Programs

Given that phishing often target human vulnerabilities, this research recommends periodic behavioral training focused on raising awareness of common phishing tactics. Scenario-based exercises, which simulate real phishing attempts, can be particularly effective in improving decision making under pressure.

5.2 Cross-Disciplinary Collaboration

Educational institutions should involve cybersecurity professionals, behavioral psychologists, and communication experts in crafting messages and training that resonate with the human experience. Collaborative research into human behavior in response to phishing can provide deeper insights into developing effective countermeasures.

5.3 Continuous Monitoring and Feedback

Implementing feedback mechanism, where users are informed when they engage with a phishing attempt, can help reinforce correct behavior. Institutions should adopt an approach where phishing awareness is treated as an ongoing priority, not a one-time event.

5.4 Recommendations for Different Stakeholders

For Students:

- » Participate in phishing awareness programs and trainings with real-world context.
- » Use browser security extensions to detect phishing threats.

For Faculty and Staff

- » Establish quick reporting mechanisms for suspicious emails, reducing response time.
- » Promote communication practices: verifying sensitive request via phone call.

For IT Administrators

- » Deploy behavior analytics to monitor phishing threats in real time.
- » Enhance email filtering rules and deploy different policy for using emails as per department and its requirements.

For Institutional Leaders and Policymakers

- » Establish and conduct mandatory cybersecurity workshops for all faculty, staff and students.
- » Collaborate with cybersecurity organizations for real-world threat intelligence sharing.

6. DISCUSSION

This study findings reinforce that phishing attacks exploit human cognitive biases and decision-making abilities as vulnerabilities, showing that human factors just as critical

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

as technological defense in cybersecurity. AI-based detection, multifactor authentication and email filtering to spam provide technical barriers, these measures are bypassed when users unknowingly engage with phishing content. Previous research highlights how social engineering techniques, urgency tactics and familiarity-based deception increase phishing success rates in which this research also aligns. Therefore, educational institutions must integrate behavior science into cybersecurity strategies.

Comparing these results with past studies, Using clustering algorithms to group emails into campaigns was a promising approach but that couldn't handle the human behavior aspects activities on phishing emails. Use of documentation and information techniques for users previous used but they did not have any significantly improve perception making it was necessary to explore more on the phishing emails outside of controlled attack and providing training to the students, faculty and academic staff in any education organization form anu despite of any background and discipline of education. Though the digitization after the COVID-19 period has shifting in education sector making upcoming generation ready while facing the competitive environment of the today's world. After which many security challenges were faced by education sector such as data theft, spam, malwares, phishing and access control using emails. Data analyzing and scanning them at a pace mechanism proposed using machine learning act as preventive model then also a significant phishing was observed in education industry which was there because of human behavior response upon the received emails from unknown as well as known email addresses.

Click-through rates on phishing emails has been reducing while implementing the continuous phishing simulation, real-time feedback mechanism along with scenario-based training. But while working in limited time duration and emails from higher authority with mention to reply in provided time interval increase the rate of being victim of phishing in the context of academic staff whereas in the case of students it was more likely to be there in case of submission of assignments on time for the grades and upcoming scholarships opportunities with apply in very less time couldn't address by above. Widespread use of Office365 for Education and G-Suite for Education increase the use of emails in education industry as well as it has highly increased the risk of phishing emails after the COVID. The implementation of Google's perspective API or Microsoft Azure AI enhances text-based phishing analysis, allowing the system to differentiate between legitimate urgent emails and phishing attempts but it is very behind the activities which comes under human behaviors during the phishing attacks which is shown by this research.

As the evolving tactics of cybercriminals, future research should focus on adaptive AI-driven training models that personalize phishing awareness based on user behavior patterns. In case of educational institutions gamified cybersecurity learning and behavioral analytics could retain in phishing awareness programs.

Workload and multitasking have great impact on phishing emails, this research also that

https://www.nepjol.info/index.php/njmsr https://doi.org/10.53056/njmsr-2025.8.1.003

many technical and automated solution as well as filtering techniques of phishing emails and higher awareness does not necessarily prevent interactions with phishing emails where individual behavior play the vital role for decision making in case of phishing emails.

7. CONCLUSION

Phishing emails cause significant changes in day-to-day activities of students, teachers and academic staff in any education industry. Consequently, it is imperative to consider the phishing emails for that. This research examined the importance of human behavior of users in cyber security, including its causes, challenges, and appropriate approaches. This research has demonstrated that attackers, manipulate psychological triggers such as urgency, authority, and opportunity. The research emphasizes that phishing susceptibility is not just a technical issue but a behavioral one, deeply influenced by how users interact with emails which they have received. Behavioral context such as the urgency in assignment submissions, authority driven requests from teachers and administrators, scholarship opportunities plays a critical role in determining of user falling into phishing attacks. This making it very difficult for students, academic staff and teachers to differentiate between legitimate and malicious emails. This highlights the importance of behavioral context in phishing.

Phishing attacks exploit more than just technological vulnerabilities – which capitalized on human behavior, cognitive biases, and decision-making under pressure. This highlights the critical role that these human factors play in successful phishing attempts within educational institutions. It is evident that effective defense against phishing requires a blend of technological solutions and human-centered interventions. By understanding and addressing the behavioral aspects of phishing, educational institutions can develop a more resilient cybersecurity culture, capable of withstanding the evolving tactics of cyber attackers.

https://doi.org/10.53056/njmsr-2025.8.1.003 https://www.nepjol.info/index.php/njmsr

REFERENCES

Althobaiti, K., Wolters, M. K., Alsufyani, N., & Vaniea, K. (2023). Using clustering algorithms to automatically identify phishing campaigns. *IEEE Access, 11,* 96502–96513. https://doi.org/10.1109/ACCESS.2023.3310810.

Marques, E., & Sousa, C. (2023). Phishing prevention in one HEI: Case study with students in one higher education institution. *Proceedings of the 2023 18th Iberian Conference on Information Systems and Technologies (CISTI) (1–6). IEEE.* https://doi.org/10.23919/CISTI58278.2023.10211824.

Shukla, S., & Sharma, A. (2023). Machine learning use case for cyber security in the education industry. *Proceedings of the 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (141–147). IEEE. https://doi.org/10.1109/ICSCSS57650.2023.10169266.

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity education and awareness among parents and teachers. *A survey of Bahrain. IEEE Access, 12,* 86596–86617. https://doi.org/10.1109/ACCESS.2024.3416045.

Irzam, F. Z. M., & Taherdoost, H. (2024). Cybersecurity KPIs in higher institutions: A systematic review. *Proceedings of the 2024 International Conference on Expert Clouds and Applications (ICOECA) (276–287). IEEE.* https://doi.org/10.1109/ICOECA62351.2024.00058.

Ciupe, C., & Orza, B. (2024). Reinforcing cybersecurity awareness through simulated phishing attacks: Findings from an HEI case study. *Proceedings of the 2024 IEEE Global Engineering Education Conference (EDUCON) (1–4). IEEE.* https://doi.org/10.1109/EDUCON60312.2024.10578700.

İş, H. (2024). LLM-driven SAT impact on phishing defense: A cross-sectional analysis. *Proceedings of the 2024 12th International Symposium on Digital Forensics and Security (ISDFS) (1–5). IEEE.* https://doi.org/10.1109/ISDFS60797.2024.10527274.

Skula, J., Bohacik, J., & Zabovsky, M. (2020). Use of different channels for user awareness and education related to fraud and phishing in a banking institution. *Proceedings of the 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA) (606–612). IEEE.* https://doi.org/10.1109/ICETA51985.2020.9379220.

Rege, G., Spence, G., Bleiman, R., Mitchell, S., & Latko, J. (2024). Bridging the 'town and gown' divide: Experiential learning for students via a community cyber hygiene training program. *Proceedings of the 2024 IEEE Integrated STEM Education Conference (ISEC) (1–6). IEEE.* https://doi.org/10.1109/ISEC61299.2024.10664800.

Jagadeesan, S., Sameer, D., Singh, R., Ojha, R., Ibrahim, R. K., & Alazzam, M. B. (2023). Implementation of artificial intelligence with cyber security in an e-learning-based education management system. *Proceedings of the 2023 4th International Conference*

on Computation, Automation and Knowledge Management (ICCAKM) (1–5). IEEE. https://doi.org/10.1109/ICCAKM58659.2023.10449611.

Matovu, R., Nwokeji, J. C., Holmes, T., & Rahman, T. (2022). Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. *Proceedings of the 2022 IEEE Frontiers in Education Conference (FIE)* (1–9). IEEE. https://doi.org/10.1109/FIE56618.2022.9962519.

Venegas-Chávez, T. E., Olivares-Bautista, S., Wlodarczyk, A., Pon, C., Flores, V., & Martínez-Peláez, R. (2024). Cybersecurity culture assessment at a university in Chile: A pilot study. *Proceedings of the 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (572–576). IEEE.* https://doi.org/10.1109/ICETSIS61505.2024.10459379.