Volume 10, Issue 11, November – 2025 International Journal of Innovative Science and Research Technology
ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25nov1387

Human Firewall Analysis: Assessing Phishing and Malware Awareness Among IT and Non-IT Professionals

Suraj Sunil Shirale[1]

[1]PDEA's Mamasaheb Mohol College, Paud Road, Pune

Publication Date: 2025/12/04

Abstract: This study examines the concept of the "human firewall" as a defence against phishing and malware and contrasts the awareness levels of IT and non-IT corporate employees. Data was obtained through a questionnaire that highlighted past experiences concerning phishing, the confidence level in recognizing suspicious messages, previous training received, and the perceptions of why certain groups are targeted more frequently.

The results show clear differences between the two groups. IT employees where more confident phishing attempts were recognizable. This was primarily because the majority had received formal training in cybersecurity from the organization. Conversely, non-IT staff cited training that was little or non-existent, thus leading to lower confidence and the belief that limited awareness made them easier targets. Nonetheless, both groups seeing the value of training was appropriate and that employees could serve as a human firewall.

The findings suggest that even though IT staff are better prepared, the non-IT employees are still at a considerable risk. Structured awareness and training initiatives should be expanded to all organizations, in all departments, not just the technical teams, to help reduce the risk of phishing and malware.

Keywords: *Human Firewall, Phishing Awareness, Malware, IT vs Non-IT Workforce, Cybersecurity Training, Social Engineering.*

How to Cite: Suraj Sunil Shirale (2025). Human Firewall Analysis: Assessing Phishing and Malware Awareness Among IT and Non-IT Professionals. *International Journal of Innovative Science and Research Technology*, 10(11), 2433-2438. https://doi.org/10.38124/ijisrt/25nov1387

I. INTRODUCTION

Cyber-attacks such as phishing and malware continue to rise, creating a serious real-world problem for organizations of all sizes. Even with strong technical security tools, attackers frequently bypass defenses by targeting people instead of systems. This makes cybersecurity awareness essential because a single wrong click can expose sensitive data, disrupt business operations, or open the door for larger attacks.

Humans remain an easy target since many employees—especially outside the IT department—lack clear training on how to identify suspicious emails, malicious files, or manipulative social engineering techniques. IT professionals, on the other hand, are regularly exposed to security tools and guidelines, which usually gives them a higher level of confidence and awareness.

Comparing IT and non-IT employees is important because both groups play different roles in daily operations, yet both interact with digital systems. Any gap in their awareness creates weak points that attackers can exploit.

The aim of this research is to measure and compare phishing and malware awareness between IT professionals and non-IT individuals. The study seeks to answer the main question: How do IT and Non-IT employees differ in cybersecurity awareness, and does their learning come from organizational training or self-learning?

II. LITERATURE REVIEW

Some of the most enduring threats to organizations across sectors entail phishing and the use of malware. Such attacks are not purely technical; they engage the 'human element', making staff the initial line of defence. This situation has spawned the idea of the 'human firewall', where staff awareness, their decisions, and their vigilance keep threats at bay.

➢ *Phishing as a Human-Centric Threat*

Among the most common ways attackers gain first access to a network is through phishing. Research has shown that phishing emails are specifically engineered to exploit a person's trust, to create a feeling of urgency, or to take advantage of a situation where a sender is unaware or IT staff

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25nov1387

are untrained about phishing to exploit a system weakness. Non-IT employees are often the targets of phishing attacks, a situation described in the literature, as untrained phishing targets. This lack of awareness is a major factor in the successful phishing of non-technical employees.

➢ *Malware Awareness and Organizational Gaps*

Malware is another major threat to an organization's security. Reports indicate that attackers often use disguised malicious files as a means to compromise untrained employees. While IT staff often have a greater understanding of malware prevention, untrained employees are more susceptible to compromise malware infections and threatening attacks.

➢ *Training and Security Culture*

A common thread in the literature on cybersecurity is the need for properly structured awareness programs. Studies show the organizations that conduct mandatory phishing simulations, workshops, and refresher trainings have a noteworthy decrease in the number of successful attacks. Unfortunately, this training is frequently limited to the IT departments, meaning that non-IT staff and teams are left quite vulnerable. This lopsided training leads to an uneven "human firewall," in which IT staff possess strong defensive awareness while the rest of the organization operates with weak defences.

➢ *Comparative Studies on IT vs Non-IT Awareness*

Comparative studies show that because of the frequent exposure to the security policies and tools, IT professionals have a higher confidence and competency in spotting phishing attempts. Conversely, non-IT employees, particularly in the admin, finance, and HR spheres, are high-value contenders for cyber attackers as they process highly sensitive data yet receive little to no technical guidance. Several studies indicate attackers specifically target non-IT employees because they are wrongly viewed as the organizational 'weakest link' and thus, lack the most defensive capabilities.

➢ *Research Gap and Study Relevance*

While previous research has discussed social engineering, phishing trends, and the relevance of cybersecurity training, fewer have directly explored the difference in awareness and behaviours between IT and non-IT employees situated in the same construct. There is limited understanding of how training, confidence, and exposure impact the effectiveness of the human firewall in these two groups. This study seeks to address this gap by systematically comparing phishing and malware awareness between IT and non-IT employees, with findings that may facilitate more inclusive and effective cybersecurity training programs.

III. METHODOLOGY

➢ *Research Design*

The current study utilizes a differentiating survey-based research design in the comparison of phishing and malware awareness between IT and non-IT corporate employees. The focus here is the identification of gaps in knowledge, training received, and perceptions of vulnerabilities in employees as human firewalls.

➢ *Data Collection*

The researcher employed an online survey in the form of a structured questionnaire distributed via online channels (e.g. Google Forms). This is a multiple-choice and opinion-based questionnaire that encompasses the following areas:

- Demographics (position, sector, and working experience).
- Exposure to phishing (range of suspicious emails received).
- Threat identification (self-assessment of inability to detect phishing/malware).
- Training and awareness (cyber defence training received).
- Perceptions of vulnerabilities (why certain demographics are frequently targeted).
- Importance of training (attitude on the relevance of awareness training).

➢ *Sample and Participants*

The participants were divided into two main groups:

- Group A – IT Professionals: Employees working in cybersecurity, IT support, software engineering, or other technical roles.
- Group B – Non-IT Employees: Employees from corporate roles such as HR, finance, sales, and administration.

A purposive sampling approach was used to ensure representation from both technical and non-technical fields.

➢ *Data Analysis*

The collected responses were analysed using descriptive statistics (percentages, frequency counts) to identify patterns and differences between the groups. Comparative analysis was used to highlight disparities in training, awareness levels, and perceptions. Graphical representations (bar charts, pie charts) were prepared to illustrate key findings.

➢ *Ethical Considerations*

The study maintained the principles of voluntary participation and confidentiality. Participants were informed that the data collected would be used solely for academic research purposes, with no personally identifiable information disclosed.

IV. RESULTS AND FINDINGS

➢ *Overview of Respondents*

A balanced response sample was received from both the IT sector and non-IT corporate respondents. Most IT professionals were in early career stages. However, non-IT respondents had diverse experience, including several with more than six years. This facilitated the acquisition of a balanced perspective across a diverse workforce.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25nov1387

➢ *Exposure to Phishing Attempts*

- IT Professionals:

Most IT respondents (over 80%) reported that they had previously received suspicious or phishing emails.

- Non-IT Employees:

In contrast, a non-negligible proportion of non-IT respondents were "not sure" whether or not they had experienced phishing attempts. This points to phishing attempts being present in a non-IT environment and a lack of awareness or difficulty in recognizing hostile content.

This demonstrates that while the exposure to phishing attempts is present in both groups, IT personnel are more likely to identify and remember such instances.

➢ *Confidence in Identifying Threats*

IT professionals overall have the highest confidence, with many ratings themselves as "very confident" in identifying phishing or malware threats. Non-IT respondents, on the other hand, tended to lack self-confidence more, with several stating they were "not confident" or "not sure." This implies that confidence levels in recognizing threats are a function of the awareness and training received.

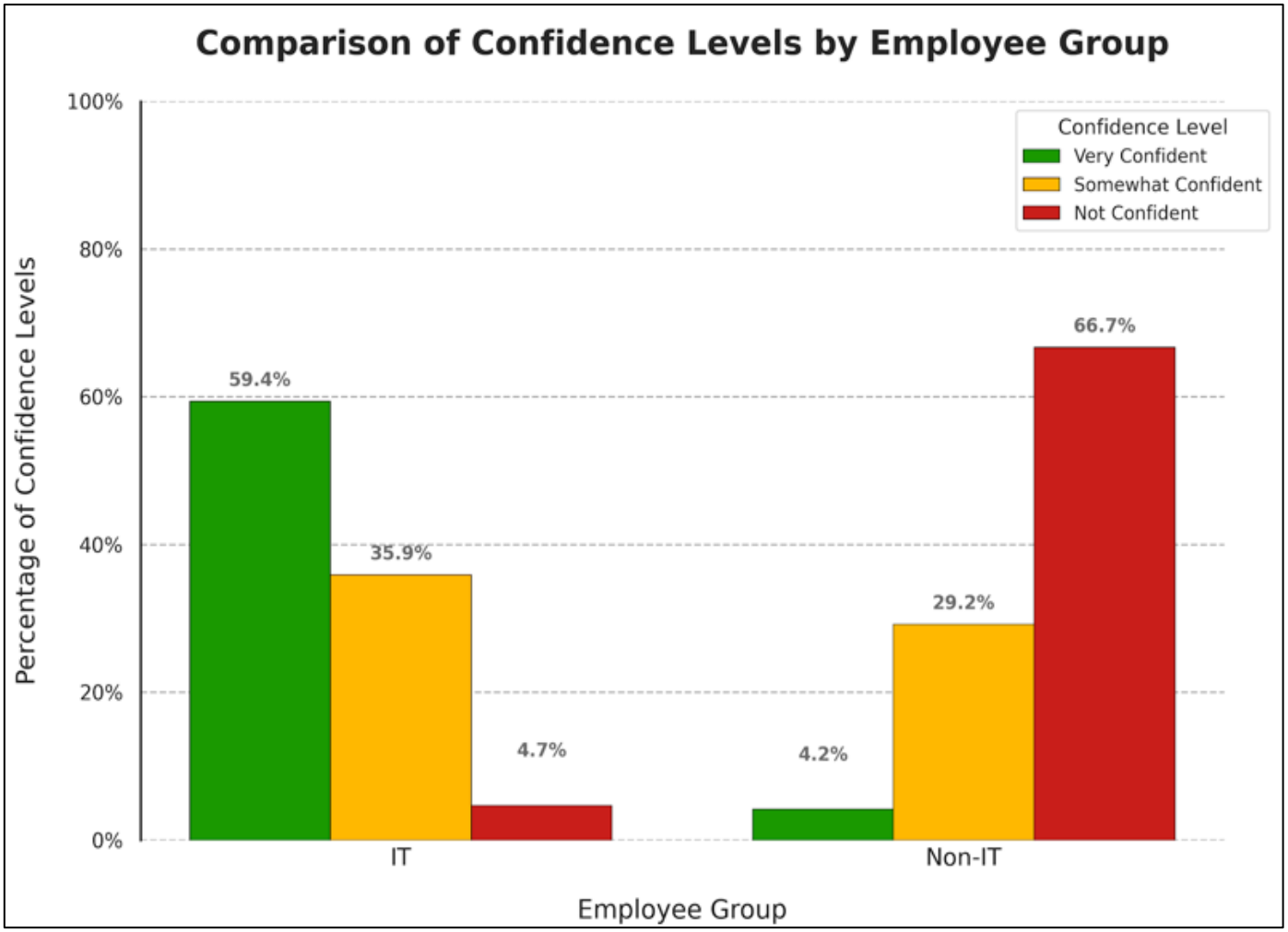

Fig 1 Comparison of Confidence Levels by Employee Group

➢ *Cybersecurity Training*

- *IT Professionals:*

Results from the survey show that 75% of IT employees had directly received cybersecurity training provided by their organization, while for 20.31%, this was achieved through self-learning or external learning. A mere 4.69% reported having no cybersecurity training.

This means that most IT professionals have structured exposure to concepts on cybersecurity, which enhances preparedness.

- *Non-IT Employees:*

In the case of non-IT employees, 66.7% reported no formal cybersecurity training, 29.3% had learned through external or self-learning sources, with only 4.2% having actually received company-provided training.

This clearly testifies to a large training inequality, where the non-IT departments remain largely unsupported in cybersecurity readiness. Conclusion: The gap in percentages confirms that cybersecurity training for IT teams is top of mind for organizations, whereas non-IT staff have limited or no exposure, thus creating a wide awareness gap.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25nov1387

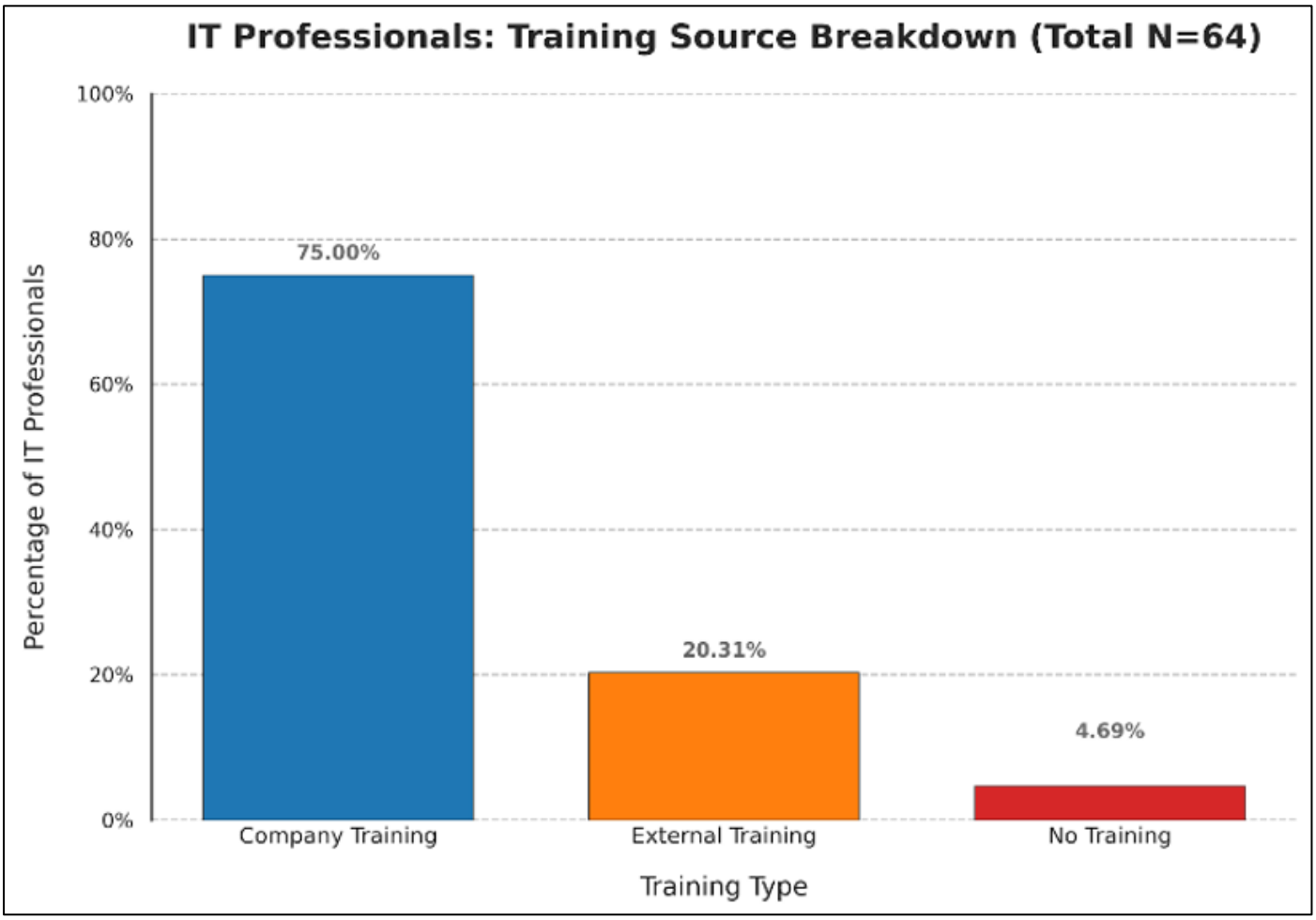

Fig 2 IT Professionals: Training Source Breakdown (Total N=64)

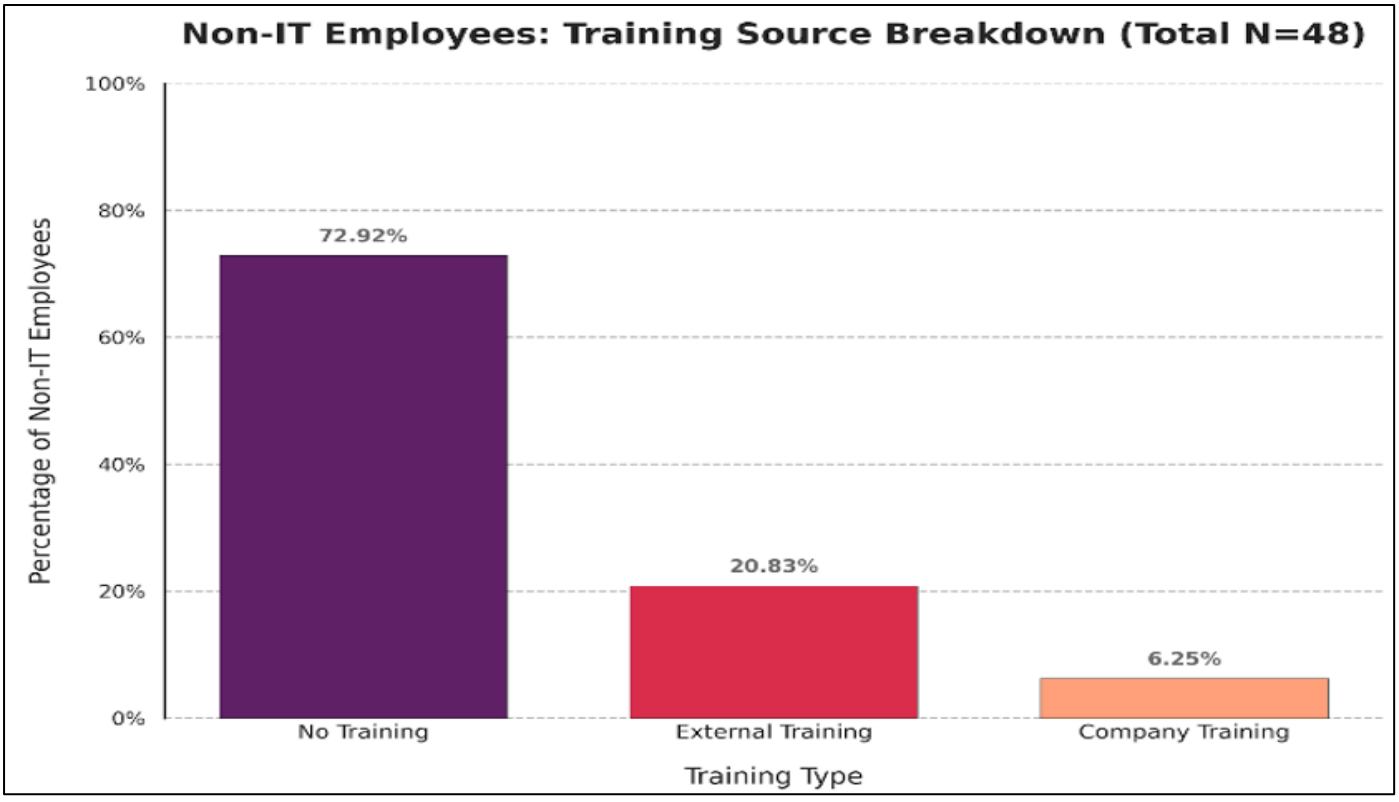

Fig 3 Non -IT Employees: Training Source Breakdown (Total N=48)

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25nov1387

➢ *Perceptions of Vulnerability*

In discussions with employees from non-IT departments as to why they are often targets, two key themes emerged:

- Non-IT Employees felt they were "easier to deceive" from an attacker's perspective given their limited exposure,
- IT Professionals cited "lack of training/awareness" as the key reason.

Therefore, both groups identify an exposed non-IT employee as a target and weaker link to an organizational security perimeter.

➢ *Human Firewall Perspective*

The overwhelming majority of respondents from each of the two groups agreed or strongly agreed that, with the right training, employees could function as a "human firewall." This demonstrates an acknowledgment that, alongside the technical measures that are put in place, human awareness and behaviour are pivotal to stopping a cyberattack.10

➢ *Key Insights*

- Training = Higher Confidence: Compared to untrained non-IT counterparts, IT staff with comprehensive training demonstrated significantly greater confidence.
- Awareness Gap: Recognizing phishing attempts is a significant challenge for non-IT professionals leaving them exposed and frequently targeted.
- Shared Agreement: Both sides recognized training as instrumental in developing a "human firewall."
- Organizational Challenge: The lack comprehensive security awareness training leaves non-IT employees exposed.

V. DISCUSSION

In this study, I noted that while non-IT staff showed a lack of training and were therefore more vulnerable to cyber predators, IT personnel showed more confidence. IT personnel also had more training and experience.

The study clearly shows that awareness and confidence go hand in hand. IT employees were better at identifying phishing and malware attempts mainly because they had regular exposure to cybersecurity training. In contrast, many non-IT employees lacked formal training, which directly affected their confidence and ability to judge suspicious emails or links. Both groups, however, agreed that with proper training, employees can act as an effective "human firewall," reinforcing the idea that cybersecurity is not only a technical concept but also a human responsibility.

The findings also highlight the imbalance in how organizations deliver security training. Most structured learning is limited to IT teams, leaving non-IT staff more vulnerable and more frequently targeted by attackers who exploit this training gap. Non-IT employees themselves felt they were easier to deceive, while IT respondents pointed to lack of awareness as the main reason behind successful attacks. These insights show that cyber threats succeed not because systems fail, but because human-centric training is uneven across departments. Strengthening cybersecurity, therefore, requires broader, organization-wide awareness programs, not just technical solutions.

➢ The level of awareness and training that a person receives is the strongest determinant of that person's confidence and preparedness.
➢ The greatest gap remains with non-IT employees, who have not been adequately equipped with training, communication, and routine exercises.
➢ The human firewall is a credible and viable line of defence, but only if organizations adopt a holistic approach to training and make it organization-wide.

VI. CONCLUSION

The research investigated the awareness about phishing and malware among IT and non-IT employees in relation to how well they serve as a human firewall. The results clearly indicate a gap in their preparedness: IT professionals were more confident and aware, since they are routinely trained in cybersecurity, whereas non-IT staff had lower levels of awareness, with many not having structured training in the area. Consequently, non-IT employees tended to become more vulnerable and sometimes unsure about identifying phishing or malware attempts.

Employees in both groups wanted to learn and had a desire to receive more cybersecurity guidance. This realization signifies that cybersecurity is not just a technical responsibility, but has to be an organization-wide affair. Thus, strong training programs across departments would reduce human error and make the ecosystem resilient to cyberattacks.

RECOMMENDATIONS

In light of the findings from this study, the following can help improve an organization's cybersecurity posture:

➢ *Organizational Cybersecurity Training*

Implement more structured training for non-IT departments. Implement phishing training simulations and malware identification workshops as well as refresher training.

➢ *Regularly Held Awareness Campaigns*

Share and discuss real instances of phishing and malware attacks. Promote reporting of suspected wrongdoing.

➢ *Building a Culture of Security*

Disseminate cybersecurity content and discussions via the organization's internal channels. Identify and appreciate employees who demonstrate cybersecurity awareness.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25nov1387

➢ *Monitoring and Feedback*

Conduct frequent surveys to measure the level of awareness and understanding. Institute training for new and emerging threats.

REFERENCES

[1]. usecure (n.d.). Social Engineering Explained: Reduce Your Employee Cyber-Security Risk. https://blog.usecure.io/employee-social-engineering

[2]. Terranova Security (2024, Nov 29). 9 Examples of Social Engineering Attacks. https://www.terranovasecurity.com/blog/examples-of-social-engineering-attacks

[3]. Hox Hunt (2024, Nov 11). What is a Human Firewall? Examples, Strategies etc. https://hoxhunt.com/blog/human-firewall

[4]. White Spider (2025, Jun 30). The Human Firewall: The real threat behind AI and social engineering. https://whitespider.com/blog/human-firewall-the-real-threat-behind-ai-and-social-engineering/

[5]. Proofpoint (2022, Aug 24). Social Engineering Training: Essential Topic. https://www.proofpoint.com/us/blog/security-awareness-training/essential-cybersecurity-awareness-training-topics-social-engineering

[6]. Secureframe (2025, Oct 29). 85+ Social Engineering Statistics to Know for 2026. https://secureframe.com/blog/social-engineering-statistics

[7]. Threat COP (2022, Jun 13). Social Engineering Attacks: Techniques and Prevention. https://threatcop.com/blog/social-engineering-attack/

[8]. The Hacker News — *"AI-Powered Social Engineering: Reinvented Threats"* (Feb 07 2025) https://thehackernews.com/2025/02/ai-powered-social-engineering.html The Hacker News

[9]. Bleeping Computer — *"5 reasons why attackers are phishing over LinkedIn"* (Nov 10 2025) https://www.bleepingcomputer.com/news/security/5-reasons-why-attackers-are-phishing-over-linkedin/