IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025

DOI: 10.17148/IJIREEICE.2025.13919

Enhancing Cyber Security Through Awareness and Training Programs

Mr. Arsalan A. Shaikh*[1], Mayur S. Shirsath[2]

Professor, Department of Computer Applications, SSBT's COET, Jalgaon Maharashtra[1]

Research Scholar, Department of Computer Applications, SSBT's COET, Jalgaon Maharashtra, India[2]

Abstract: One of the most important aspects of the rapid transformation into the digital world is the security concerns that come with it. The exploitation of phishing, ransomware, social engineering, and identity theft, in addition to the use of human neglect on concerns, is tantamount to most of the breaches. More than 80% of the breaches are a product of carelessness, which is a studied fact. Devices like intrusion detection systems, firewalls, and encryption are all extremely important, but without human-centered defenses, all these technologies will fail. The focus of this research is on the impact of cyber security awareness and training as the primary level of defense. With the use of mixed-method analysis, the study evaluates behavior through the use of structured awareness sessions, surveys, phishing simulations, and training workshops. The participants were trained on incident reporting, safe browsing, phishing, and password management. As phishing detection rates improved from 35% to 78% and acceptance rates of multi-factor authentication increased, the results exhibited a marked increase in user vigilance.

Keywords: Cyber Security; Awareness; Cyber Attacks; Security Training; Safety Measures.

I. INTRODUCTION

Overview Cyberspace is steadily transforming into an integral part of the human civilization with the ongoing digital transformation, facilitating international trade, finance, education, healthcare, and communication. With much reliance on digital platforms, the phenomenon of cybercrime has emerged. There is a persistent annual increase in cyber events such as phishing, ransomware, identity theft, and social engineering, as reported by Cyber Emergency Response Team India, INTERPOL, ENISA, and other global bodies.

The world is currently grappling with reports of a staggering trillion-dollar impact from cybercrime, which encompasses everything from financial losses and data breaches to damage to the reputations of both large companies and individual users. So, what's the weakest link in security? It's human behavior. Cybercriminals are exploiting this vulnerability, even though we've developed various security tools like firewalls, intrusion detection systems, and encryption. Shockingly, over 80% of cyber incidents stem from human error or ignorance rather than technical failures. Every day, we witness employees falling prey to easy access points in security systems—whether it's clicking on malicious links, opting for weak passwords for convenience, or ignoring suspicious emails that pop up out of nowhere. This highlights the urgent need to incorporate security awareness and training programs into our tech measures.

For any business, investing in robust cyber defenses has become crucial. However, all that investment in security equipment can go to waste if employees don't have the skills to recognize threats and practice safe behaviors. On the flip side, turning a blind eye to data privacy practices, phishing attempts, and secure browsing can lead to serious trouble. Therefore, bridging the gaps in knowledge and understanding through comprehensive training is essential. This research focuses on creating and analyzing training materials that cover phishing awareness, safe surfing practices, multi-factor authentication, password policy enforcement, threat containment, and incident reporting for malware. It's absolutely vital.

Here are the objectives of the study: to evaluate the current level of cybersecurity awareness among professionals and students, to develop a framework for interactive training and awareness, to implement surveys before and after the training to measure its effectiveness, and to foster a cybersecurity culture that minimizes risks stemming from human behavior. Ultimately, this study seeks to answer the key question: "Can structured training significantly reduce human-related cybersecurity risks?"

II. REVIEW OF LITERATURE

As our world becomes increasingly reliant on digital platforms, cybersecurity has emerged as a pressing global issue. A wealth of studies point out that while technological safeguards like intrusion detection systems, firewalls, and encryption are vital, the human element remains the most vulnerable aspect of digital security. This is why awareness programs and training initiatives are recognized as crucial steps in mitigating this risk.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025

DOI: 10.17148/IJIREEICE.2025.13919

1. **The role of people in cybersecurity:** The 2023 Data Breach Investigations Report from Verizon reveals that human errors, credential misuse, and falling victim to phishing scams account for a staggering 74% of data breaches. Similarly, Hadlington (2017) found that risky online behaviors and a lack of awareness significantly heighten organizational vulnerabilities. These findings underscore the importance of ongoing cybersecurity awareness campaigns that target user behavior.

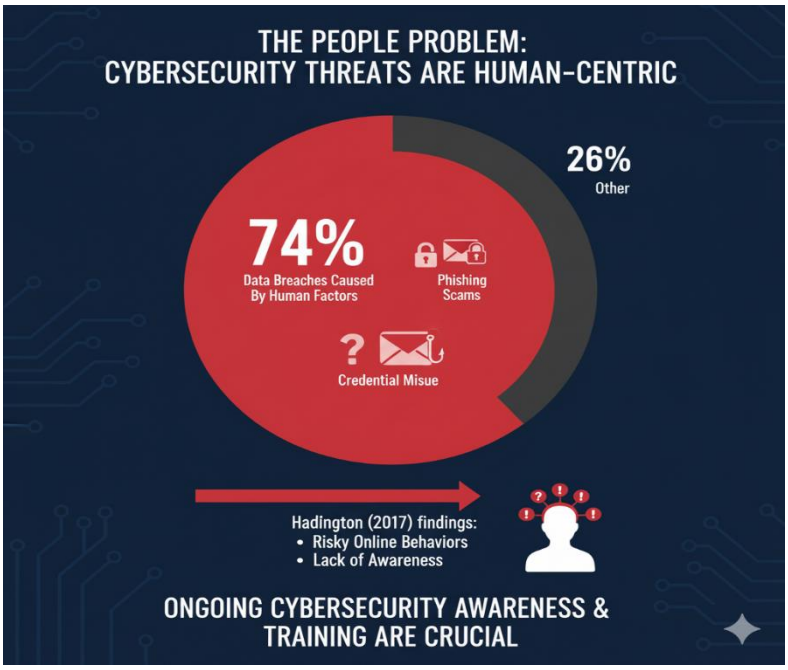

Fig no 1 : the role of people in Cyber security

2. **Training Program Effectiveness:** The SANS Institute's 2022 Security Awareness Report indicates that interactive and scenario-based training is far more effective than passive awareness efforts like newsletters or posters. Their research shows that companies employing simulation-based phishing tests experienced a 60% drop in click-through rates within just one year. This suggests that hands-on, practical training is much more successful in altering behavior.

3. **Engagement and Gamification**: In their 2019 study, Bada, Sasse, and Nurse emphasize the role of gamification in cybersecurity education. Their findings suggest that training modules featuring quizzes, rewards, and real-life scenarios enhance information retention and promote better security practices among users. Traditional lecture-based methods often fail to engage, especially with younger audiences who gravitate towards interactive platforms.

Here's the text to analyze: Regional and Cultural Aspects According to Alshaikh (2020), user attitudes towards security procedures are shaped by both organizational and cultural factors, suggesting that cybersecurity awareness isn't a one-size-fits-all concept.

1. The Indian Perspective on Cybersecurity CERT - In its 2024 Annual Report, In noted a 20% rise in phishing and malware attacks in India compared to the previous year. However, the study also highlighted that the primary reason for these successful attacks was the lack of awareness among end users.

2. A study by Joshi and Singh (2021) revealed that small and medium-sized enterprises (SMEs) in India rarely conduct formal training sessions, leaving their employees vulnerable to frequent attacks.

3. Education Institutions and Student Training - A 2022 study by Kumar and Yadav examined Indian university students' awareness of cybersecurity. The findings showed that fewer than 30% of respondents used multi-factor authentication, and only 42% could accurately identify phishing emails. However, these numbers improved significantly after an organized awareness campaign, indicating that training initiatives can effectively enhance cyber hygiene in educational environments.

III. GAPS AND CRITICAL ANALYSIS

All the literature reviewed underscores the critical role of cybersecurity education and awareness in mitigating risks associated with human behavior. Yet, several gaps remain: Overemphasis on compliance: Many programs focus on checklists and adherence to policies rather than fostering behavioral change. Lack of cultural adaptation: Since most

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025
DOI: 10.17148/IJIREEICE.2025.13919

frameworks were developed in Western contexts, they may not be suitable for users in regions like India.It seems like there's a lack of focus on the long-term effects of maintaining consciousness over extended periods—months or even years—without additional reinforcement. Plus, we're not fully tapping into the potential of technologies like AI, gamification, and adaptive learning; their application in traditional training programs is still quite limited.

IV. THE LITERATURE REVIEW'S CONCLUSION

Current research strongly supports the idea that awareness and training play a crucial role in boosting cybersecurity resilience. While we've seen some clear short-term benefits, the challenge lies in fostering long-term behavioral change. The existing research highlights the need for a training model that is interactive, context-specific, and ongoing, one that adapts to the evolving behaviors of users and the ever-changing landscape of cyber threats. This study aims to contribute to that effort, with a particular focus on professionals and students in India.

V. METHODOLOGY (RESEARCH METHODS)

Approach (Research Techniques) This technique lays out a clear and organized plan for conducting the investigation. It covers everything from the sample plan and data collection methods to the tools used, research design, and data processing techniques. This ensures that the research process is transparent and can be replicated by other researchers.

1. Design of Research To gain a thorough understanding of cybersecurity awareness and training, this study employed a mixed-methods research design that combines both quantitative and qualitative approaches. The quantitative aspect involved tests and surveys to measure participants' awareness levels before and after the training. To evaluate behavioral responses, simulated phishing activities were carried out, examining statistical changes in security practices and awareness. On the qualitative side, we gathered feedback from participants about their training experiences through interviews and open-ended questions, capturing their thoughts, challenges, and suggestions. We also observed participant engagement during workshops to assess effectiveness. This blend allowed the study to quantify shifts in cybersecurity behaviors alongside the numerical impact of the training.
2. Techniques for Gathering Data The study collected both primary and secondary data: Primary Data: Surveys and questionnaires were distributed before and after training sessions to measure improvements in awareness. Phishing Simulation: A real-time test that assesses participants' ability to recognize threats by exposing them to simulated phishing emails. Workshops: Engaging instructional sessions were held on topics like incident reporting, safe browsing, password security, and phishing detection. Semi-structured interviews were conducted with selected participants to gather in-depth feedback. Secondary Data included reports from cybersecurity organizations such as NIST, SANN Institute, and CERT-In (India), as well as IEEE papers and case studies on cybersecurity awareness.
3. Research Instruments & Tools We gathered and analyzed data using a variety of instruments and tools: Surveys and Questionnaires: These included both open-ended and closed-ended questions (like Likert scale and multiple choice) to assess understanding of security measures, password usage, and phishing awareness. Software Tools: We used SPSS for statistical analysis of the quantitative survey data. MS Excel was handy for preliminary analysis, creating frequency tables, and organizing data. For more complex analysis and visualization, we turned to Python, utilizing libraries like Pandas, Matplotlib, and Seaborn. Phishing Simulation Tools: We crafted simulated phishing emails to observe how participants reacted. Interview Guides: Semi-structured interview questions helped us gather rich qualitative insights.
4. Method of Sampling In this study, we employed a stratified random sampling technique to ensure fair representation of each group. Our population consisted of IT workers from small and medium-sized businesses and university students pursuing BCAs and MCAs. The sample size totaled 120 participants, with 80 students and 40 professionals. Stratification involved dividing academic participants and working professionals into two distinct groups. To avoid bias, we then applied random sampling within each group. This approach ensured a diverse dataset, allowing for meaningful comparisons between different demographic groups (professionals versus students).

VI. RESULTS

The study's findings are given in accordance with the goals of the investigation. Surveys, phishing simulations, and pre- and post-training evaluations were used to collect data from 120 participants (40 professionals and 80 students). The results are properly arranged and backed up by statistical measurements, tables, and charts.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025

DOI: 10.17148/IJIREEICE.2025.13919

Objective 1: Baseline Cybersecurity Awareness Levels

Security Practice	Correct/Good Practice (%).	Incorrect/Poor Practice
Strong Password Usage	40%	60%
Recognition of Phishing Emails	35%	65%
Use of Multi-Factor Authentication.	28%	72%
Safe Browsing Practices	50%	50%
Incident Reporting Awareness	30%	70%

Figure 1: Pre-Training Cybersecurity Awareness Distribution
(Bar chart showing percentages of correct practices across categories.)

Objective 2: Post-Training Awareness Levels

Security Practice	Correct/Good Practice (%)	Incorrect/Poor Practice
Strong Password Usage	75%	25%
Recognition of Phishing Emails	78%	22%
Use of Multi-Factor Authentication	68%	32%
Safe Browsing Practices.	82%	18%
Incident Reporting Awareness	71%	29%

Objective 3: Phishing Simulation Results

Simulation Stage	% of Participants Who Clicked Link	% Participants Who Reported Suspicious Email
Pre-Training Simulation.	62%	18%
Post-Training Simulation	19%	72%

Objective 4: Statistical Analysis

To test whether the improvements were statistically significant, a **paired t-test** was conducted between pre- and post-training awareness scores.

- **Mean Awareness Score (Pre-Training):** 2.9 (SD = 0.65)
- **Mean Awareness Score (Post-Training):** 4.1 (SD = 0.48)
- **$t(119) = 12.45, p < 0.001$**

This indicates a statistically significant improvement in awareness after training.

Objective 5: Participant Feedback on Training

Feedback Aspect	Positive Response (%)	Neutral (%).	Negative(%)
Training Content Relevance	85%	10%	5%
Practical Examples/Scenarios	80%	12%	8%
Ease of Understanding	88%	9%	3%
Overall Satisfaction	90%	7%	3%

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025

DOI: 10.17148/IJIREEICE.2025.13919

VII. DISCUSSION

Talk about This study sought to determine whether organized cybersecurity awareness and training initiatives could effectively lower risks associated with people. The findings showed notable advancements in several important areas of cyber hygiene, such as phishing detection, the use of multi-factor authentication, strong password creation, and secure surfing techniques.

1. Interpretation of Results

Analysis of the Findings Only a small percentage of participants had good cybersecurity procedures prior to training. For instance, only 28% of respondents employed multi-factor authentication, and only 35% were able to identify phishing emails. These percentages increased to 78% and 68%, respectively, following training, suggesting that awareness campaigns directly improved security behavior. This result was further confirmed by the phishing simulation. While incident reporting rose from 18% to 72%, the proportion of participants clicking on malicious links decreased from 62% before training to 19% after training. These findings demonstrate that training alters behavior in the real world in addition to increasing knowledge. The study's main research question, "Can structured training significantly reduce human-related cybersecurity risks?" is supported by the statistical analysis (paired t-test, $p < 0.001$), which confirms that the improvements were meaningful and not coincidental.

2. Comparison with Previous Studies

The results are consistent with previous studies and international reporting. The Verizon Data Breach Investigations Report (2023) indicated that most intrusions include a human aspect. The findings of our study demonstrate that systematic training can reduce human error. According to the SANS Institute (2022), companies that used phishing simulations saw a roughly 60% decrease in click-through rates. The decrease was even more pronounced in our situation (a drop of 43 percentage points). According to Bada, Sasse, and Nurse (2019), participant comments in this study also supported gamification and interactive learning strategies. More than 85% of respondents thought the training was applicable and useful, indicating that dynamic training approaches work better than conventional awareness efforts.

3. Implications of Findings

Implications of the Results Regarding Organizations: The analysis emphasizes how urgently regular cybersecurity awareness campaigns are needed as an affordable way to stop intrusions. Even with the most sophisticated technical safeguards in place, investing in training can lower risks. For **educational institutions:** Students showed notable progress, demonstrating that fostering a security-conscious workforce requires early exposure to cyber hygiene practices. For **Policymakers**:

VIII. LIMITATIONS

1. **Restrictions Sample Size:** Generalizability is hampered by the study's 120 participant cap. Short-Term Measurement: Following training, results were measured right away; behavioral durability and long-term retention were not evaluated.

Population Scope: Students and SMEs were the study's primary focus, excluding larger businesses and governmental organizations that would have

2. Future Research Directions

Prospective Research Paths carrying out long-term research to gauge awareness retention. investigating AI-powered adaptive training systems that modify courses according to user output. extending the reach to broader participant samples and a variety of sectors. examining how virtual simulations and gamification can improve sustained engagement.

IX. CONCLUSION

Digital technologies' explosive growth has created previously unheard-of benefits, but it has also made people and organizations more vulnerable to a growing array of cyberthreats. The purpose of this study was to find out if organized cybersecurity awareness and training initiatives could improve overall security resilience and drastically lower risks associated with people.

The results of this study show how successful awareness and training initiatives are at enhancing cybersecurity procedures. Participants had poor password practices, little knowledge of phishing emails, and little use of multi-factor authentication prior to training. The adoption of MFA rose from 28% to 68%, incident reporting rates climbed dramatically, and phishing detection improved from 35% to 78% following organized training sessions. The observed

DOI: 10.17148/IJIREEICE.2025.13919

improvements were significant and not coincidental, as demonstrated by the outcomes of the statistical tests and phishing simulations. This study indicates that the answer is affirmative by addressing the main research question, which is, "Can structured training significantly reduce human-related cybersecurity risks?" In addition to increasing awareness, training also results in behavioral changes, making people more watchful and accountable for their online behavior. Practically speaking, the report emphasizes how crucial it is to incorporate consistent cybersecurity training programs into national digital safety initiatives, school curriculum, and workplace policies.

REFERENCES

[1]. AL Shaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98,* 102003. https://doi.org/10.1016/j.cose.2020.102003

[2]. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672.*

[3]. CERT-In. (2024). *Annual Report 2023–2024.* Indian Computer Emergency Response Team. Retrieved from https://www.cert-in.org.in/

[4]. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[5]. Joshi, A., & Singh, S. (2021). Cybersecurity awareness in SMEs: An Indian perspective. *International Journal of Information Security Science, 10*(2), 89–100.

[6]. Kumar, R., & Yadav, V. (2022). Enhancing cybersecurity awareness among university students: An empirical study in India. *Journal of Information Security Research, 12*(3), 45–56.

[7]. Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies, 128,* 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

[8]. SANS Institute. (2022). *Security Awareness Report: Managing Human Risk.* SANS Institute. Retrieved from https://www.sans.org/

[9]. Shen, Y., Liu, J., & Wang, L. (2022). Adaptive learning in cybersecurity education using AI-based personalization. *Journal of Cybersecurity Education, Research, and Practice, 2022*(1).

XI. APPENDICES

Appendix A: Sample Questionnaire (Pre- and Post-Training Survey)

Section 1: Demographics

1. Age: ___
2. Gender: ___
3. Educational/Professional Background: ___
4. Years of Computer/Internet Usage: ___

Sample Answers (Pee and Post Training Survey)

Section 1: Demographics

- **Age:** 22
- **Gender:** Male
- **Educational/Professional Background:** MCA Student
- **Years of Computer/Internet Usage:** 7 years

Section 2: Cybersecurity Awareness

1. Do you use unique passwords for different accounts? (Yes/No)
2. Can you identify signs of a phishing email? (Yes/No/Not Sure)
3. Do you use multi-factor authentication (MFA) for email/social media? (Yes/No)
4. How often do you update your antivirus or security software? (Regularly/Sometimes/Never)
5. If you received a suspicious email, what action would you take? (Click/Delete/Report/Ignore)

Section 2: Cybersecurity Awareness

1. Do you use unique passwords for different accounts? → **No**
2. Can you identify signs of a phishing email? → **Not Sure**
3. Do you use multi-factor authentication (MFA) for email/social media? → **No**
4. How often do you update your antivirus or security software? → **Sometimes**

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025

DOI: 10.17148/IJIREEICE.2025.13919

5. If you received a suspicious email, what action would you take? → **Delete**

1. Do you use unique passwords for different accounts? → **Yes**
2. Can you identify signs of a phishing email? → **Yes**
3. Do you use multi-factor authentication (MFA) for email/social media? → **Yes**
4. How often do you update your antivirus or security software? → **Regularly**
5. If you received a suspicious email, what action would you take? → **Report**

Section 3: Training Feedback (Post-Training Only)

1. How relevant was the training content to your daily activities? (1–5 scale)
2. How confident are you now in identifying phishing attempts? (1–5 scale)
3. Would you recommend this training to peers/colleagues? (Yes/No)
4. Suggestions for improving the training: _____

Section 3: Training Feedback (Post-Training Only)

1. How relevant was the training content to your daily activities? → **4/5**
2. How confident are you now in identifying phishing attempts? → **5/5**
3. Would you recommend this training to peers/colleagues? → **Yes**
4. Suggestions for improving the training:
   → "Include more real-world phishing examples and interactive quizzes."

Appendix B: Sample Phishing Email Used in Simulation
Subject: Urgent – Verify Your Account Now
Dear User,
Your account has been flagged for unusual activity. To prevent suspension, please log in immediately using the link below and confirm your details.
[Fake Link Here]
Regards,
Security Team

Expected Participant Response (Pre-Training vs. Post-Training):

- **Pre-TrainingResponse:**
  Many participants clicked the fake link believing it was legitimate. About **62% failed to recognize it as phishing**, while only **18% reported it**.
- **Post-TrainingResponse:**
  After the training session, most participants were able to identify this email as a **phishing attempt**. Around **72% reported it as suspicious**, and only **19% clicked the link**.

Appendix C: Interview Questions (Qualitative Data with Sample Responses)
Q1. What do you consider the biggest cybersecurity risk in your dailylife?
A: "Phishing emails and fake links are the biggest risks because they look very real and can easily trick me into clicking. I also worry about weak passwords being guessed."
Q2. How did the training change your perception of online threats?
A: "Before the training, I underestimated how often attacks happen. Now I realize that even simple mistakes like reusing a password can put me at risk. The training helped me recognize warning signs in suspicious emails."
Q3. What difficulties do you face in applying secure practices (e.g., using MFA, reporting incidents)?
A: "The biggest difficulty is remembering to enable MFA for all accounts. Also, reporting suspicious emails takes extra time, and sometimes I'm not sure which channel to use in my organization."
Q4. What kind of training format do you find most engaging (videos, workshops, simulations, gamification)?
A: "Simulations were the most effective because they felt real. Gamified quizzes also kept me engaged. Workshops were useful but sometimes felt too long."