



Pakistan Journal of Criminal Justice

ISSN: 2958-9363 ISSN (E): 2958-9371

Volume 6, No.7, 2026, 10-17

DOI: <https://doi.org/10.59075/pjcj.v6i7.201>

Journal Homepage: <https://journals.centeriir.org/index.php/pjcj>

Public Awareness Of AI-driven Cybersecurity and Social Engineering Threats: A Survey-Based Assessment of Karachi's Educated Population

Ahtashamul Hassan Narejo¹, Dr Abdul Basit Solangi², Shakeela Ali Ahtasham Narejo³, Dr. Taha Shabbir⁴

¹ Advocate High Courts, LLM Scholar, Shadeed Zulifqar Ali Bhutto University of Law, Clifton Karachi, Pakistan,

Email: narejo.ahtasham@gmail.com

² Assistant Professor, Pakistan Studies, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Pakistan,

Email: abdulbasit@sbbusba.edu.pk

³ Advocate High Courts, BA LLB (Hon) & LLM, Pakistan, Email: Shakeelaali.narejo@gmail.com

⁴ Associate Professor, Hamdard University, Karachi, Pakistan

ABSTRACT

This study investigates public awareness regarding artificial intelligence (AI), social engineering, and cybersecurity threats among the educated population of Karachi, Pakistan. A quantitative, survey-based methodology was employed, collecting 152 responses from the general public through structured questionnaires distributed via both print and online (Google Forms) channels. The sample predominantly comprised young adults (81.6% aged 18–34), with the majority holding at least a bachelor's degree (67.8%) and reporting daily internet use (94.7%). Despite this high educational attainment and digital connectivity, the findings reveal significant awareness gaps: only 49% reported strong familiarity with AI, over half (52.3%) were unaware of deepfake technology, 50.3% had never heard of social engineering in a cybersecurity context and 40% were unaware of any Pakistani laws addressing cybercrimes. Notably, 70% had never received any training on cybersecurity or AI-related risks. Bivariate Pearson correlation analysis revealed statistically significant positive relationships between familiarity with specific AI threats and the perceived vulnerability of the public to AI-driven cyberattacks ($r = 0.399$ for deepfake concern, $p < 0.001$). These results underscore a paradox of widespread AI adoption coexisting with critically low threat awareness, highlighting an urgent need for structured public education campaigns and policy interventions in Pakistan.

Keywords: Artificial Intelligence; Cybersecurity; Social Engineering; Deepfake; Public Awareness; Pakistan; PECA 2016



© 2026 The Authors, Published by [Center of Innovation in Interdisciplinary Research \(CIIR\)](#).
This is an Open Access Article under the Creative Common Attribution Non-Commercial 4.0

Article History: Received: 15-07-2026 Accepted: 20-08-2026 Published: 04-09-2026

Corresponding Author's Email: narejo.ahtasham@gmail.com

Introduction

The rapid advancement of artificial intelligence (AI) and machine learning (ML) technologies has fundamentally transformed human interaction with digital systems. From chatbots and virtual assistants to predictive algorithms and autonomous vehicles, AI applications have become embedded in everyday life at an unprecedented scale. The emergence of large language models such as ChatGPT in late 2022 further accelerated public engagement with AI tools, triggering a global conversation about both the promise and the peril of these technologies (Kamruzzaman, Thakur, & Mahbub, 2024). However, this rapid adoption has introduced an equally rapid expansion of the cyber threat landscape, as malicious actors increasingly leverage AI to enhance the sophistication and scale of cyberattacks.

In the domain of cybersecurity, AI has proven to be a double-edged sword. On the defensive side, AI-powered systems enhance intrusion detection, automate threat hunting, and enable behavioral analytics to identify anomalies in network traffic (Bécue, Praça, & Gama, 2021). On the offensive side, cybercriminals have weaponized AI to create adaptive malware, generate highly convincing phishing campaigns, and produce deepfake audio and video content that can impersonate real individuals with alarming accuracy (Guembe et al., 2022). Social engineering attacks, which exploit human psychological vulnerabilities rather than technical weaknesses, have become particularly potent when augmented by AI. These attacks, ranging from AI-crafted spear-phishing emails to deepfake voice impersonation, represent a growing category of threats that traditional cybersecurity measures alone cannot address (Narejo, A. H., Solangi, A. B., Ali, S., & Shabbir, T. 2026).

Pakistan, the world's fifth most populous country, presents a uniquely vulnerable case study. The country has experienced exponential growth in internet connectivity, yet it lacks widespread public awareness of AI-related cybersecurity threats. The existing legal framework, primarily the Prevention of Electronic Crimes Act (PECA) 2016 and the Electronic Transactions Ordinance 2002, provides a statutory basis for combating cybercrimes. However, the effectiveness of these laws depends critically on the awareness and engagement of both the public and the legal profession. In a society where social media is a primary news source and where emotional susceptibility to misinformation is high, the risks posed by deepfakes and AI-powered social engineering are not merely theoretical; they represent a clear and present danger to social cohesion and democratic integrity.

This paper, derived from the LLM thesis of Ahtashamul Hassan Narejo at Shaheed Zulfiqar Ali Bhutto University of Law (Karachi), presents the findings from a survey of the general public in Karachi. It aims to answer the following research questions: (1) To what extent are educated internet users in Karachi familiar with AI, social engineering, and deepfake technology? (2) What is the level of public awareness regarding Pakistan's cybersecurity laws? (3) Is there a statistically significant relationship between awareness of specific AI threats and the perceived vulnerability of the public to AI-driven cyberattacks?

Literature Review

AI and the Evolving Cyber Threat Landscape

Artificial intelligence, broadly defined as the application of technology to automate tasks that normally require human intelligence (Surden, 2019), has evolved from a niche research discipline to a pervasive force in modern society. The subset of AI most relevant to cybersecurity is machine learning (ML), which employs statistical models to identify meaningful patterns in large datasets and generate intelligent-looking outputs without explicit programming (Touretzky, Gardner-McCune, & Seehorn, 2023). The proliferation of ML applications from recommendation engines and natural language processing to computer vision and autonomous systems—has created both new tools for cybersecurity defense and new vectors for attack.

On the threat side, AI has enabled a new generation of cyberattacks. AI-powered phishing uses machine learning to mimic writing styles and personalize content, making attacks significantly more convincing (Waizel, 2024). AI-enhanced malware employs polymorphic code that constantly mutates to evade signature-based detection systems. AI-driven ransomware leverages intelligent algorithms to identify and encrypt the most valuable data on a network. Perhaps most alarmingly, deepfake technology uses deep learning neural networks to synthesize realistic audio and video of real individuals, enabling sophisticated impersonation for financial fraud, political disinformation, and reputational damage (Westerlund, 2019; Sharma & Kaur, 2022). The convergence of these AI-augmented threats with the psychological manipulation techniques of social engineering creates a particularly dangerous cocktail.

Social Engineering: The Human Vulnerability

Social engineering, in the cybersecurity context, refers to the use of deception to induce individuals to divulge private information or provide unauthorized access to systems (Hatfield, 2018). Unlike technical exploits, social engineering attacks target the most persistent vulnerability in any security system: the human element. Hatfield (2018) traces the conceptual lineage of social engineering from political technocracy to its modern cybersecurity application, identifying three core elements—epistemic asymmetry, technocratic superiority, and teleological replacement—that characterize all forms of social engineering.

The scale of the problem is substantial. Industry surveys indicate that social engineering was the most common cyber threat for organizations from 2016 to 2018 (Rawal, Eberhardt, & Lee, 2016). In 2018, 85% of organizations reported experiencing social engineering attacks, at an average annual cost exceeding \$1.4 million per organization. The integration of AI into social engineering tactics has only amplified these figures, as AI enables attackers to automate reconnaissance, personalize attacks at scale, and generate convincing pretexts using deepfake technology.

Pakistan's Legal Framework for Cybercrimes

Pakistan's legislative response to cybercrimes has evolved incrementally. The Electronic Transactions Ordinance (ETO) 2002 established the legal foundation for electronic records and digital signatures. The more comprehensive Prevention of Electronic Crimes Act (PECA) 2016 addresses a broad spectrum of offenses, including unauthorized access to data (Sections 3–5), offenses against critical infrastructure (Sections 6–8), electronic forgery and fraud (Sections 13–14), identity theft (Section 16), privacy violations (Section 20), cyberstalking (Section 24), and spamming (Section 25). PECA 2016 provides substantive legal tools for prosecuting AI-related cybercrimes, yet the effectiveness of any legal framework is contingent on both public awareness and professional enforcement capacity.

Methodology

Research Design

This study adopted a quantitative, non-doctrinal (empirical) research design employing a survey-based approach. The objective was to assess the real-world cognizance of the general public regarding AI, social engineering, and cybersecurity threats, which required the collection of primary data rather than solely analyzing legal texts.

Sampling and Data Collection

The target population was the general public of Karachi, with an emphasis on educated internet users. A total of 152 valid responses were collected through a structured questionnaire distributed via both printed forms and Google Forms. The questionnaire comprised 21 items covering demographics (age, gender, education, occupation), internet usage patterns, familiarity with AI and its applications, awareness of social engineering and deepfake technology, perceived vulnerability to AI-driven cyberattacks, awareness of cybersecurity laws, prior cybersecurity training, and perceived importance of AI-related public education.

Data Analysis

Descriptive statistics (frequencies and percentages) were used to characterize the sample and summarize responses. Bivariate Pearson correlation analysis was performed to test the relationships between key awareness variables and perceived vulnerability. Scale reliability was assessed using Cronbach's Alpha.

Hypothesis

Null Hypothesis (H_0): There is no significant correlation between the level of education of the general public and their cognizance of potential dangers associated with AI for social engineering and cybersecurity.

Alternative Hypothesis (H_1): There is a significant positive correlation between the level of education of the general public and their cognizance of potential dangers associated with AI for social engineering and cybersecurity.

Results

Demographic Profile

The sample was predominantly young and educated. The largest age cohort was 25–34 years (44.1%), followed by 18–24 years (37.5%), 35–44 years (13.8%), with only 4.6% aged 45 or above. Gender distribution was heavily male (79.5% male, 20.5% female). The majority of respondents held a bachelor's degree (67.8%), with a further 26.3% holding a master's degree. In terms of occupation, 42.4% were employed, 29.1% were students, 17.2% were self-employed, and 11.3% were unemployed. Nearly all respondents (94.7%) reported daily internet use.

AI Familiarity and Usage

Approximately 49% of respondents described themselves as “very familiar” with AI, while 37.7% were “somewhat familiar,” 10.6% were “not very familiar,” and 2.6% were “not at all familiar.” This indicates that roughly half of this educated sample lacked strong familiarity with AI—a concerning finding given their educational attainment and digital connectivity. Paradoxically, approximately 85% reported using at least one AI application (chatbots, virtual assistants, predictive text, language translation apps, or social media algorithms), while 74.8% acknowledged that AI has a significant impact on daily life.

Awareness of AI-Driven Threats

Awareness of the specific threats investigated was markedly low. Only 49.7% of respondents had heard of the term “social engineering” in a cybersecurity context. When asked about familiarity with social engineering attacks such as phishing, pretexting, and baiting, only 24.3% reported being “very familiar,”

while 18.9% were “not at all familiar.” Most alarmingly, 52.3% of respondents were unaware of the term “deepfake.” Only 48.3% believed the general public to be “somewhat vulnerable” to AI-driven cyberattacks, with 17% perceiving the public as “very vulnerable.”

Table 1: Summary of AI Threat Awareness Among General Public (N = 152)

Variables			
Familiarity with AI (Very Familiar)	49.0%	13.2%	37.7%
Use of AI Applications	85.0%	15.0%	—
Heard of Social Engineering	49.7%	50.3%	—
Familiar with SE Attacks (Very)	24.3%	18.9%	56.8%
Aware of Deepfake Technology	47.7%	52.3%	—
Aware of Cybersecurity Laws	36.2%	39.5%	24.3%
Received Cybersecurity Training	30.0%	70.0%	—

Legal Awareness and Education

Awareness of Pakistan’s cybersecurity legislation was notably low. Approximately 40% of respondents were unaware of any laws or regulations addressing cybercrimes and AI-related threats in Pakistan, with a further 24.3% responding “maybe.” Critically, 70% of respondents reported having never received any training or education on cybersecurity or the risks associated with AI. However, when asked about the importance of public education on AI and its potential risks, 78% deemed it “very important” and a further 14.7% deemed it “somewhat important”—representing a near-universal demand for educational intervention.

Correlation Analysis

Bivariate Pearson correlation analysis was conducted on four key awareness variables. The results revealed several statistically significant relationships:

Table 2: Pearson Correlation Matrix for Public Awareness Variables (N = 154)

Variables				
PAA6 (AI Familiarity)	1.000	.202*	.106	.243**
PAA10 (SE Attack Familiarity)	.202*	1.000	.154	.353**
PAA13 (Deepfake Concern)	.106	.154	1.000	.399**
PAA14 (Perceived Vulnerability)	.243**	.353**	.399**	1.000

* $p < 0.05$; ** $p < 0.01$ (2-tailed)

The strongest correlation was between concern about deepfake technology (PAA13) and perceived vulnerability to AI-driven cyberattacks (PAA14), at $r = 0.399$, $p < 0.001$. Familiarity with social engineering attacks (PAA10) also showed a strong positive correlation with perceived vulnerability ($r = 0.353$, $p < 0.001$). A weaker but significant correlation existed between general AI familiarity (PAA6) and perceived vulnerability ($r = 0.243$, $p < 0.01$). The reliability analysis yielded a Cronbach’s Alpha of 0.562, which, while below the conventional threshold of 0.700, is interpretable in the context of an exploratory study measuring distinct facets of awareness rather than a single unified construct.

Discussion

The Paradox of Use Without Awareness

The most striking finding of this study is the paradox between AI adoption and AI literacy. While 85% of respondents use AI applications and 94.7% are daily internet users, only 49% claim strong familiarity with AI as a concept, and the majority are unaware of foundational threat categories such as social engineering and deepfakes. This suggests a pattern of unconscious adoption—a condition where individuals interact extensively with AI-powered systems without possessing the conceptual vocabulary or threat awareness to navigate the risks these systems create. In the Pakistani context, where social media serves as a primary information source and where emotional susceptibility to sensationalist content is well-documented, this awareness deficit represents a systemic vulnerability that extends far beyond individual risk.

The Correlation Between Knowledge and Risk Perception

The correlation analysis offers an important insight: greater familiarity with specific AI threats is significantly associated with a heightened perception of vulnerability. The finding that deepfake concern ($r = 0.399$) is the strongest predictor of perceived vulnerability aligns with the literature on the unique psychological impact of manipulated audio-visual content, which exploits the inherent human tendency to trust visual evidence (Westerlund, 2019). This positive feedback loop—where knowledge drives concern, which in turn drives demand for education—suggests that targeted awareness campaigns focusing on concrete, relatable threat demonstrations (such as deepfake examples) may be the most effective entry point for public education.

The Education and Training Deficit

The finding that 70% of respondents have never received cybersecurity or AI-risk training, combined with the near-universal demand for such education (92%), represents both a failure and an opportunity. It is a failure of current educational and workplace training systems, which have not adapted to the realities of an AI-saturated digital environment. It is an opportunity in that the demand for education is clear and overwhelming, providing a strong mandate for intervention by government agencies, educational institutions, and civil society organizations.

Legal Awareness Gap

The finding that 40% of the general public is unaware of any cybercrime laws underscores a critical disconnect between legislative intent and public reach. Pakistan's PECA 2016 provides a comprehensive, if imperfect, legal framework for addressing AI-related cybercrimes. However, laws cannot serve their protective function if the very population they are designed to protect is unaware of their existence. This awareness gap means that victims of AI-driven cybercrimes may not know their rights, may not report offenses, and may not seek legal recourse—perpetuating a cycle of impunity for cybercriminals.

Limitations

Several limitations must be acknowledged. The sample was geographically limited to Karachi and skewed toward young, educated, employed males, which limits generalizability to the broader Pakistani population. The relatively low Cronbach's Alpha (0.562) indicates that the survey instrument measures

distinct facets of awareness rather than a single cohesive construct. The reliance on self-reported familiarity may also be subject to social desirability bias.

Conclusion and Recommendations

This study reveals a critical and paradoxical situation: Karachi's educated; digitally connected population is extensively using AI technologies while remaining substantially unaware of the cybersecurity threats these technologies enable. Over half are unaware of deepfakes, the majority have not heard of social engineering, 40% do not know about cybercrime laws, and 70% have received no relevant training. The correlation analysis confirms that those who are more aware of specific threats perceive greater public vulnerability, suggesting that education itself is a powerful tool for building societal resilience.

Based on these findings, the following recommendations are offered: First, the government of Pakistan should launch large-scale public awareness campaigns on AI-related cybersecurity threats, leveraging the same digital platforms—social media, messaging apps—through which threats are most commonly delivered. Second, cybersecurity literacy modules should be integrated into the national educational curriculum from secondary level onward. Third, the Pakistan Bar Council and provincial bar associations should mandate continuing legal education programs on AI and cybersecurity for practicing lawyers. Fourth, employers should be incentivized to provide regular cybersecurity training. Fifth, the government should establish accessible online portals and helplines for reporting cybercrimes and seeking guidance. These interventions are not merely desirable; in an age where AI-powered threats are rapidly outpacing public awareness, they are essential for national security and social stability.

References

1. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, 54(5), 3849–3886.
2. Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. *Journal of Artificial Intelligence General Science (JAIGS)*, 3(1), 143–154.
3. Cloud Security Alliance. (2024). State of AI and security survey report. <https://cloudsecurityalliance.org/artifacts/state-of-ai-and-security-survey-report>
4. Dsouza, K. J., Mukherjee, A., & Bhat, M. S. (2024). Deepfakes in social engineering attacks. *International Journal of Innovative Science and Research Technology*, 9(9), 1948–1957.
5. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence*, 36(1), 2037254.
6. Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102–113.
7. Narejo, A. H., Solangi, A. B., Ali, S., & Shabbir, T. (2026). The enforcement gap: Assessing legal professionals' knowledge of AI-related cyber threats and Pakistan's cybersecurity legislation. *Journal for Social Science Archives*, 4(1), 2231–2238. <https://doi.org/10.59075/jssa.v4i1.654>
8. Iqbal, M., Talpur, S. R., Manzoor, A., Abid, M. M., Shaikh, N. A., & Abbasi, S. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the challenges in Pakistan. *Siazga Research Journal*, 2(4), 273–282. <https://doi.org/10.58341/srj.v2i4.35>
9. ISC2. (2024). 2024 ISC2 Cybersecurity Workforce Study. <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>
10. Kamruzzaman, A. S., Thakur, K., & Mahbub, S. (2024). AI Tools Building Cybercrime & Defenses. *Proceedings of the 2024 International Conference on ACDSA*.
11. Nadella, G. S., & Gonaygunta, H. (2024). Enhancing cybersecurity with artificial intelligence:

- Predictive techniques and challenges in the age of IoT. *International Journal of Science and Engineering Applications*, 13(04), 30–33.
12. Nguyen, D., & Hekman, E. (2024). AI and cybersecurity: A risk society perspective. *Frontiers in Computer Science*, 6, 1462250. <https://doi.org/10.3389/fcomp.2024.1462250>
 13. Nibigira, N., Havyarimana, V., & Xiao, Z. (2024). Artificial intelligence adoption for cybersecurity in Africa. *Journal of Information Security*, 15(2), 134–147. <https://doi.org/10.4236/jis.2024.152009>
 14. Rawal, B. S., Eberhardt, G., & Lee, J. (2016). Cybersecurity snapshot: Google, Twitter, and other online databases. *Journal of Advanced Computer Science & Technology*, 5(1), 14–22.
 15. Salman, A., & Shamsi, J. A. (2023). Analytical survey of deepfake detection and psychological factors in digital media manipulation. *Issues in Information Systems*, 25(2), 96–112.
 16. Sharma, M., & Kaur, M. (2022). A review of Deepfake technology: An emerging AI threat. *Soft Computing for Security Applications: Proceedings of ICSCS 2021*, 605–619.
 17. Sidoti, O., & Vogels, E. A. (2023). Most Americans haven't heard of deepfakes; those who have are skeptical of what they see online. Pew Research Center. <https://www.pewresearch.org/short-reads/2023/02/15/>
 18. Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, 35(4).
 19. Touretzky, D., Gardner-McCune, C., & Seehorn, D. (2023). Machine learning and the five big ideas in AI. *International Journal of Artificial Intelligence in Education*, 33(2), 233–266.
 20. Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. *Proceedings of TRUST Conference*.
 21. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11).