MULTIDISCIPLINARY RESEARCH IN COMPUTING INFORMATION SYSTEMS

VOL 05 ISSUE 06 2025

P-ISSN: 3080-7182
E-ISSN: 3080-7190

https://mrcis.org

SOCIAL ENGINEERING ATTACKS: HUMAN FACTORS IN CYBER DEFENSE

Adeel Zahir [1], Hassan Mehmood [2]

Abstract. *Social engineering attacks exploit the psychological vulnerabilities of individuals rather than relying solely on technical weaknesses. In the evolving landscape of cybersecurity, human behavior remains one of the most significant factors determining organizational resilience. This paper analyzes the psychological manipulation techniques used by attackers, explores the reasons behind human susceptibility, and identifies mitigation strategies through education, awareness, and behavioral analysis. The study highlights the critical need for integrating human factor defense mechanisms into cyber protection frameworks, emphasizing employee training, adaptive awareness programs, and multi-layered authentication systems. It also discusses real-world case studies where social engineering led to severe data breaches, demonstrating the pressing need for human-centered cybersecurity approaches.*

Keywords: *Social Engineering, Cyber Defense, Human Factors, Phishing, Psychological Manipulation, Cybersecurity Awareness, Behavioral Analysis, Organizational Security.*

INTRODUCTION

In the modern digital age, cyber threats have evolved beyond technical vulnerabilities, targeting the weakest link in the security chain—the human mind. Social engineering attacks exploit human trust, curiosity, and authority bias to gain unauthorized access to confidential information. Unlike conventional cyberattacks that rely on malware or system vulnerabilities, social engineering focuses on manipulating individuals into compromising security protocols. These attacks are often executed through phishing emails, pretexting, baiting, and impersonation, making them difficult to detect through traditional security tools. In Pakistan, the rapid digital transformation across banking, government, and education sectors has increased exposure to such human-centered attacks. Despite the advancements in firewalls and encryption, the absence of cybersecurity awareness among users remains a persistent challenge. Therefore, understanding and mitigating human factors in cyber defense is essential for developing a holistic approach to cybersecurity management

[1] *Department of Computer Science, COMSATS University Islamabad, Pakistan.*

[2] *Department of Cybersecurity, University of Lahore, Pakistan.*

Understanding Social Engineering:

Social engineering represents one of the most sophisticated and psychologically driven forms of cyberattack, exploiting the innate human tendency to trust and respond emotionally. Rather than focusing on technical loopholes, attackers use manipulation, persuasion, and deception to trick individuals into revealing confidential information or performing actions that compromise security. These attacks often begin with information gathering, where attackers research their targets using social media, emails, or public databases to craft convincing narratives. The manipulation process typically appeals to emotions such as fear (e.g., threats of account suspension), urgency (e.g., limited-time offers or fake emergencies), curiosity (e.g., enticing links or files), or empathy (e.g., fake charity appeals). Social engineers exploit these psychological triggers to override rational judgment, prompting victims to disclose sensitive data or bypass security protocols. The success of such attacks relies heavily on social context and communication skills rather than advanced coding or hacking. As digital communication channels expand through emails, messaging apps, and social platforms, the scope and sophistication of social engineering continue to grow, making user awareness and behavioral defenses the cornerstone of effective cybersecurity.

Psychological Manipulation Techniques:

Attackers borrow proven persuasion tactics from behavioral psychology to steer victims' decisions without them noticing: for example, authority is simulated by spoofing an executive's email or using official-looking language so people comply out of perceived obligation (CEO fraud), while reciprocity works by offering a small favor or "free" resource—people feel obliged to return the favor by sharing information or clicking a link. Scarcity and urgency create a false limited window ("respond within 1 hour") that short-circuits deliberation, and social proof convinces targets by implying others have already approved the request (fake testimonials, forged colleague confirmations). Attackers also use liking (mirroring language, finding common ground) to build rapport quickly, commitment and consistency (start with a small yes, then escalate requests), priming and framing (wording a message to make a desired response feel normal), and cognitive overload (bombarding the target with details so they act reflexively). Combined with well-researched personal details from open sources, these techniques exploit automatic, emotionally driven shortcuts in human decision-making—making technically simple requests highly effective unless users are trained to pause, verify sources, and follow strict authentication procedures.

Common Forms of Social Engineering Attacks:

Human vulnerability in social engineering attacks stems primarily from cognitive biases and emotional responses that shape how individuals process information and make decisions. Attackers exploit these predictable human tendencies to create convincing deceptions that bypass rational thinking. For example, people often exhibit authority bias, automatically complying with perceived figures of power such as managers, law enforcement, or IT personnel. Similarly, urgency bias triggers impulsive actions under time pressure, leading victims to click on malicious links or share credentials without proper verification. Emotional manipulation—such as invoking fear of penalty, greed through rewards, or empathy via fabricated distress—further amplifies susceptibility. Another critical factor is overconfidence bias, where individuals believe they are too experienced to fall for scams, ironically making them more vulnerable. Social norms like trust, helpfulness, and politeness can also be exploited; people hesitate to question requests that appear legitimate or courteous. Moreover, fatigue, stress, and information overload reduce cognitive vigilance, increasing the success rate of attacks. Understanding these behavioral triggers and how

they interact with workplace culture and digital habits is vital for developing effective cybersecurity awareness programs that strengthen human defenses against manipulation.

Social Engineering Breaches:

the world vividly illustrate how human error can undermine even the most advanced cybersecurity infrastructures. One of the most notable examples is the 2011 RSA Security breach, where attackers used a simple phishing email with a malicious Excel attachment to compromise the company's SecurID authentication systems—ultimately affecting major clients, including U.S. defense contractors. Similarly, in 2013, the Target Corporation data breach resulted from a phishing attack on a third-party vendor, leading to the theft of over 40 million customer credit card records. In 2020, Twitter suffered a social engineering attack in which hackers manipulated employees over the phone to gain administrative access, allowing them to hijack high-profile accounts, including those of Elon Musk and Barack Obama, to promote cryptocurrency scams. Locally, Pakistani financial institutions have faced similar incidents; for instance, in 2018, several banks temporarily suspended international transactions after coordinated phishing and social engineering attempts compromised user data. These cases underscore a consistent theme: attackers did not exploit software vulnerabilities but rather the human tendency to trust and respond emotionally to perceived authority or urgency. The lessons learned from such breaches emphasize the urgent need for continuous cybersecurity awareness training, strict verification protocols, and psychological resilience programs to counteract human-centered attacks effectively.

Cybersecurity Awareness and Education:

Cybersecurity awareness and education are foundational elements in defending against social engineering attacks, as they directly address the human vulnerabilities that technology alone cannot eliminate. Effective awareness programs go beyond technical instruction—they are designed to influence behavior by leveraging psychological principles of learning, motivation, and habit formation. Training that incorporates real-world phishing simulations allows employees to experience attack scenarios safely, helping them recognize subtle signs of manipulation such as suspicious links, spoofed email addresses, and urgent language. Moreover, gamified learning modules—where users earn points, badges, or ranks for identifying threats—have proven highly effective in sustaining engagement and reinforcing knowledge retention. Tailoring educational content to different user roles within an organization ensures relevance; for instance, executives may need training on whaling attacks, while customer service teams require guidance on handling social-engineering-based inquiries. Continuous, adaptive training—rather than one-time workshops—is essential to keep up with evolving tactics. Additionally, incorporating behavioral feedback and positive reinforcement encourages proactive security behavior. In Pakistan and other developing nations, integrating cybersecurity awareness into academic curricula and workplace culture is particularly vital, as digital literacy gaps make users more susceptible to psychological manipulation. Ultimately, awareness and education empower individuals to act as the first line of defense, transforming potential targets into active defenders in the cybersecurity ecosystem

Organizational Policies and Human-Centric Defense:

Organizational policies play a pivotal role in building a resilient defense framework against social engineering attacks by embedding human awareness and behavioral control into every layer of cybersecurity strategy. A human-centric defense approach acknowledges that technology alone cannot prevent manipulation and that employees must be empowered through structured policies and clear procedures. Implementing the Zero-Trust Security Model ensures that no individual—whether inside or outside the organization—is automatically trusted, requiring continuous

authentication and verification of identity before granting access to sensitive resources. Furthermore, multi-factor authentication (MFA) significantly reduces the likelihood of unauthorized access by adding extra verification steps, even if credentials are compromised through phishing. Regular policy enforcement through security audits, role-based access controls, and least-privilege principles strengthens this structure. Organizations should also develop comprehensive incident response protocols, enabling swift identification, containment, and remediation of social engineering attempts before they escalate into full-scale breaches. Employee reporting mechanisms—such as anonymous threat reporting channels—encourage transparency and early detection. Beyond enforcement, cultivating a culture of accountability, where every member understands their role in maintaining security, is essential. Periodic policy reviews, executive leadership involvement, and collaboration between IT and HR departments ensure these measures remain adaptive to evolving threat landscapes. In essence, well-defined organizational policies that prioritize the human factor transform cybersecurity from a purely technical exercise into a collective responsibility across the enterprise.

Technology Integration for Behavioral Analysis:

The future of human-centered cybersecurity lies in the seamless integration of advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), and behavioral analytics to anticipate and neutralize social engineering threats before they succeed. As attackers increasingly use AI to craft realistic phishing emails, deepfake voice calls, and impersonation messages, defense systems must evolve to recognize subtle behavioral deviations that signal malicious intent. AI-driven behavioral analysis tools monitor communication patterns, tone, response timing, and access behavior to establish a baseline of normal user activity. When anomalies occur—such as unusual login times, irregular message structures, or abnormal file access—these systems trigger alerts for further investigation. Moreover, Natural Language Processing (NLP) and emotion detection algorithms can analyze the psychological undertones of communications to detect coercion, deception, or manipulation attempts. In the future, cybersecurity frameworks will move beyond technical fortification to emphasize digital empathy, combining data analytics with insights from psychology and neuroscience to understand and defend against human-targeted attacks. Personalized risk profiles for employees, adaptive learning algorithms, and continuous monitoring will form the core of next-generation defense systems. As organizations in Pakistan and globally transition into hybrid work environments, integrating AI-driven behavioral analytics with human training will create dynamic, self-improving systems capable of identifying, predicting, and mitigating social engineering attacks with unprecedented precision and speed.

Future of Human-Centered Cybersecurity:

The future of human-centered cybersecurity is rapidly evolving as both defenders and attackers harness the power of artificial intelligence, automation, and psychological insight. In the coming years, cyber threats will become increasingly personalized through AI-generated phishing emails, deepfake audio and video impersonations, and automated social manipulation, making traditional detection tools insufficient. These sophisticated attacks will exploit not only technical weaknesses but also emotional and cognitive vulnerabilities, creating scenarios that appear almost indistinguishable from genuine interactions. To counter such threats, cybersecurity defense must adopt adaptive, psychologically informed frameworks that integrate technology with human behavioral science. This involves combining AI-driven threat detection, emotional intelligence analytics, and user behavior modeling to recognize subtle anomalies in communication and decision-making. Future systems will likely incorporate cognitive firewalls—mechanisms

designed to alert users when messages contain manipulative emotional triggers such as fear or urgency. Moreover, the emphasis will shift toward proactive defense strategies, where continuous behavioral monitoring and predictive analytics identify potential insider threats or manipulated users before breaches occur. Education and ethical AI governance will also play a central role, ensuring that human judgment remains the cornerstone of digital decision-making. Ultimately, the cybersecurity of the future will depend not just on smarter machines, but on smarter, more psychologically resilient humans working in harmony with intelligent, adaptive systems.

Role of Culture and Organizational Behavior in Security Compliance:

Culture and organizational behavior play a profound role in shaping employees' attitudes and responses toward cybersecurity practices. In many workplaces, particularly within hierarchical or collectivist cultures such as those found in South Asia, employees often prioritize obedience and respect for authority over critical questioning. This cultural dynamic can create an environment where individuals hesitate to challenge or verify suspicious requests from superiors, inadvertently increasing vulnerability to social engineering attacks. Additionally, workplace communication styles—whether formal, indirect, or highly deferential—affect how quickly and accurately employees report anomalies. A rigid top-down management structure may discourage open dialogue or fear of blame, leading to delayed incident reporting or concealment of mistakes. On the other hand, organizations with transparent, trust-based cultures that encourage information sharing tend to exhibit higher cybersecurity resilience. Moreover, cultural perceptions of privacy and technology adoption influence compliance with security policies; for instance, employees who perceive cybersecurity rules as intrusive or unnecessary are less likely to follow them diligently. Therefore, building a security-aware organizational culture involves more than issuing policies—it requires promoting psychological safety, empowering employees to question authority when something seems suspicious, and incorporating cultural sensitivity into awareness training. By aligning cybersecurity initiatives with local cultural values and workplace behaviors, organizations can foster compliance, vigilance, and collective responsibility across all levels of their workforce**.**

Impact of Remote Work and Digital Communication Channels:

The shift toward remote and hybrid work environments has fundamentally transformed the cybersecurity landscape, creating new vulnerabilities that attackers are quick to exploit. When employees operate outside the controlled boundaries of corporate networks, they often rely on personal devices, home Wi-Fi connections, and unsecured cloud platforms, all of which expand the attack surface for cybercriminals. Phishing, impersonation, and business email compromise (BEC) attacks have surged as remote workers communicate primarily through digital channels like email, WhatsApp, Slack, and Microsoft Teams. The informal nature of these platforms—combined with the absence of face-to-face verification—makes it easier for attackers to pose as trusted colleagues or superiors. Furthermore, the sense of isolation and urgency often experienced by remote employees can lead to impulsive decision-making, such as clicking malicious links or sharing credentials. Attackers also exploit time zone differences, sending messages during off-hours when IT support is unavailable, increasing the likelihood of human error. Remote work has also blurred the line between professional and personal digital spaces, with employees multitasking across personal accounts and work platforms—creating potential crossover points for compromise. To counter these challenges, organizations must enforce robust endpoint protection, VPN access, and two-factor authentication, while also conducting continuous awareness training tailored to remote communication habits. Building a security-first culture in remote work requires fostering vigilance, ensuring secure collaboration tools, and promoting digital hygiene as an integral part of everyday operations.

Regulatory Frameworks and Compliance in Cybersecurity Awareness:

Regulatory frameworks and international compliance standards play a critical role in shaping how organizations approach cybersecurity awareness and human-factor resilience. Standards such as **ISO/IEC 27001**, **NIST Cybersecurity Framework**, and **GDPR (General Data Protection Regulation)** explicitly recognize human error as a major risk factor and mandate employee training as part of organizational security governance. These frameworks emphasize that technological controls alone are insufficient without ensuring that personnel understand and adhere to secure practices. Under ISO/IEC 27001, for example, information security awareness programs must be documented, regularly updated, and tailored to employees' roles and access levels. Similarly, GDPR places legal obligations on organizations to protect personal data, which includes preventing breaches caused by social engineering or negligent behavior. Non-compliance not only exposes organizations to reputational damage but also to heavy financial penalties under laws such as the **EU's GDPR** or **Pakistan's Personal Data Protection Bill (PDPB)**, which is under development. Moreover, emerging global standards—such as the **Cybersecurity Maturity Model Certification (CMMC)** in the U.S.—further stress the integration of awareness into operational culture. Therefore, organizations must align their cybersecurity training programs with these regulations, ensuring that employees are not only informed but also accountable for maintaining data protection principles. Establishing a **compliance-driven awareness ecosystem** reinforces both legal responsibility and ethical digital conduct, bridging the gap between regulatory policy and practical human behavior in cybersecurity.

The Economics of Social Engineering Attacks :

The economics of social engineering attacks reveal why these tactics remain among the most cost-effective and profitable strategies for cybercriminals. Unlike technical attacks that require specialized tools, expensive malware development, or deep system knowledge, social engineering relies primarily on psychological manipulation—making it both inexpensive and highly scalable. A single phishing campaign can be launched at virtually no cost using automated email generators, fake websites, or social media impersonation, yet it can yield massive financial gains if even a small fraction of targets respond. According to cybersecurity research, the return on investment (ROI) for social engineering can exceed that of ransomware or data breaches because attackers exploit human trust rather than technical systems. Moreover, the accessibility of the dark web has lowered entry barriers, enabling less-skilled attackers to purchase phishing kits, deepfake software, and stolen credentials cheaply. For organizations, this creates a dangerous imbalance—while the cost to attackers remains minimal, the financial and reputational losses for victims can be enormous, ranging from data theft and fraud to regulatory fines and loss of customer trust. Understanding this cost-benefit disparity highlights the necessity of investing in proactive defenses such as employee training, behavior-based monitoring, and awareness-driven policies. Preventive measures, although requiring upfront investment, are far less expensive than the costs of breach recovery, legal liabilities, and long-term brand damage resulting from successful social engineering attacks.

Integrating Behavioral Science with Cybersecurity Training:

Integrating behavioral science with cybersecurity training represents a progressive and human-centric approach to strengthening digital resilience. Traditional security awareness programs often focus on technical procedures and compliance, overlooking the psychological mechanisms that drive human behavior. By applying insights from behavioral science—such as cognitive psychology, neuroscience, and behavioral economics—organizations can design training that aligns with how people actually perceive risk, make decisions, and respond under pressure. For example, understanding cognitive biases like optimism bias (believing "it won't happen to me") or confirmation bias (trusting only familiar sources) enables trainers to address these misconceptions directly. Behavioral science also highlights the role of emotional triggers—fear, curiosity, and social belonging—in decision-making, allowing for simulations that mimic real-world manipulation attempts. Additionally, techniques such as nudging and habit formation can subtly influence employees toward safer digital behaviors, such as verifying links or reporting suspicious emails without hesitation. Personalized and adaptive training programs, informed by behavioral data and feedback, can reinforce security habits through repetition and reward systems. Over time, this integration fosters a security-aware mindset rather than rote compliance, making individuals more resistant to manipulation. In essence, merging behavioral science with cybersecurity education transforms awareness from passive learning into an active, psychologically grounded defense mechanism against social engineering attacks.

Ethical Challenges in Behavioral Monitoring and AI Defense Systems:

The use of AI-based behavioral monitoring and defense systems introduces complex ethical challenges that extend beyond technical considerations. While these systems are effective in detecting anomalies and preventing social engineering attacks, they often rely on continuous observation of employee communications, behaviors, and digital footprints—raising serious privacy and consent concerns. The boundary between legitimate security monitoring and intrusive surveillance becomes blurred when organizations collect data on keystrokes, email tone, or online activity without transparent disclosure. Such practices can erode employee trust, create feelings of constant surveillance, and potentially violate data protection laws like the General Data Protection Regulation (GDPR) or Pakistan's Personal Data Protection Bill (PDPB). Additionally, the algorithms used in behavioral analytics may unintentionally introduce bias or discrimination, leading to unfair profiling or false positives that target specific individuals. Ethical implementation therefore requires transparency, accountability, and proportionality—ensuring that monitoring practices are necessary, clearly communicated, and limited to legitimate security objectives. Organizations should establish clear governance frameworks defining how behavioral data is collected, processed, and stored, as well as obtain informed consent from employees. Regular audits, anonymization of personal data, and the inclusion of human oversight can help mitigate ethical risks. Ultimately, balancing security with respect for individual privacy is essential for maintaining trust and ensuring that AI-driven cybersecurity remains aligned with ethical and legal standards.

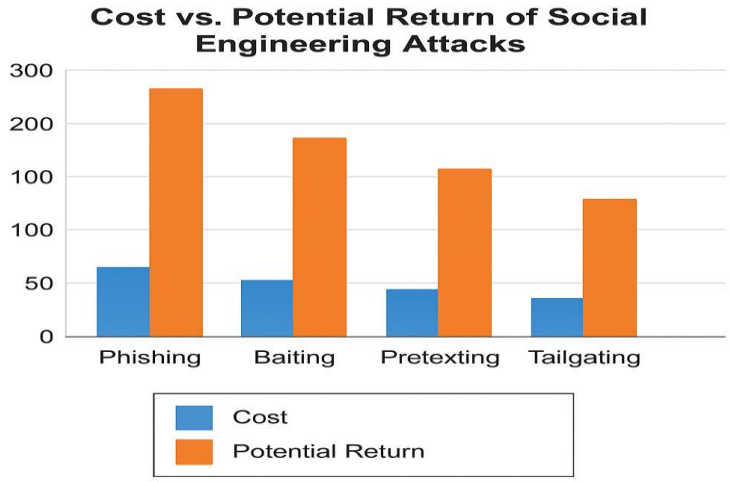
Global Collaboration and Information Sharing:

Global collaboration and information sharing have become essential components of modern cybersecurity defense, especially in combating rapidly evolving social engineering attacks. Since these attacks often transcend national and organizational boundaries, no single entity can effectively address them in isolation. Establishing global cyber-intelligence networks allows governments, private companies, and research institutions to share data on new threat patterns, phishing campaigns, and manipulation tactics in real time. Platforms such as the Computer

Emergency Response Teams (CERTs), INTERPOL Cybercrime Directorate, and regional collaborations like APCERT or EUROPOL's EC3 demonstrate the power of cross-border cooperation in early threat detection and coordinated response. Shared databases and incident repositories help organizations identify trends, benchmark vulnerabilities, and develop region-specific awareness programs that account for cultural and linguistic variations in social engineering techniques. Moreover, international collaboration encourages the development of standardized policies, ethical guidelines, and technical protocols for managing cyber threats. For developing countries such as Pakistan, participation in global intelligence networks can significantly enhance preparedness, providing access to early warnings, shared resources, and expert insights. Ultimately, fostering a culture of open communication, mutual trust, and knowledge exchange among nations and industries strengthens the global cybersecurity ecosystem—transforming collective intelligence into a proactive shield against social engineering and other human-centric cyber threats.

Ahmad (2025) provides a detailed analysis of eight major Pakistani State-Owned Enterprises (SOEs), including PIA, Pakistan Steel Mills, and Pakistan Railways, over the period 2019–2024. Using both quantitative and qualitative methods such as thematic content analysis, cross-case comparison, and theoretical mapping, the study reveals chronic losses, heavy subsidy dependence, and low operational efficiency. PIA and Pakistan Steel Mills alone consume over 92% of total subsidies, reflecting structural inefficiencies and political interference. Ahmad emphasizes that urgent reforms, including privatization, public-private partnerships, and professionalized governance, are essential to restore public trust, enhance accountability, and promote sustainable public sector management in Pakistan.

Ahmad (2025) examines human–AI collaboration in professional knowledge work, focusing on productivity, error patterns, and ethical risks. Participants were assigned to human-only, AI-assisted, and optional AI-only task groups performing writing, summarization, decision-support, and problem-solving activities. Findings indicate that AI assistance accelerates task completion by 32–39%, especially benefiting novices in structured tasks, but increases errors by 15–25% in complex tasks. Ahmad identifies trust calibration, verification behaviors, cognitive load, and ethical awareness as critical factors affecting AI effectiveness. The study highlights the importance of human oversight, training, and ethical risk mitigation to balance efficiency with accuracy in AI-assisted workflows.



Summary

The study concludes that social engineering remains a critical challenge in the cybersecurity landscape due to the persistent role of human error. The success of such attacks depends largely on the manipulation of trust and authority, indicating the psychological nature of the threat. The integration of human-centered defense mechanisms, including behavioral monitoring, adaptive education, and advanced authentication systems, is essential. In Pakistan and globally, cybersecurity awareness must be institutionalized as part of corporate culture. Organizations that invest in human-centric defense mechanisms, continuous education, and psychological resilience training can significantly reduce the likelihood of breaches. The intersection of psychology and technology represents the next frontier in combating social engineering attacks effectively.

References

Mitnick, K., & Simon, W. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

Albladi, S. M., & Weir, G. R. S. (2018). Human factors in social engineering attacks: A systematic literature review. Computers & Security, 73, 101-122.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662-674.

Parsons, K., et al. (2017). Determining employee awareness using phishing simulation. Computers & Security, 68, 45-59.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), 983–988.

Mouton, F., et al. (2016). Social engineering attack framework. Computers & Security, 59, 109–122.

Wright, R. T., et al. (2014). Research note: Social influence and information security behaviors. Journal of Information Systems, 28(1), 1–15.

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. Journal of Information Security and Applications, 27, 123–135.

Halevi, T., et al. (2013). Cognitive biases and phishing susceptibility. Human Factors, 55(6), 1153–1168.

Anwar, M., et al. (2017). Security behavior of smartphone users. Computers & Security, 68, 75–90.

Zand, F., et al. (2020). Understanding human error in information security: A human factors approach. Information & Computer Security, 28(3), 363–382.

Ahmad, N. R. (2025). *Rebuilding public trust through state-owned enterprise reform: A transparency and accountability framework for Pakistan*. Punjab Sahulat Bazaars Authority (PSBA), Lahore, Pakistan. https://doi.org/10.24088/IJBEA-2025-103004

Ahmad, N. R. (2025). *Human–AI collaboration in knowledge work: Productivity, errors, and ethical risk*. https://doi.org/10.52152/6q2p9250