P-ISSN: 2709-6254	Journal of Development and Social Sciences	Jan-March 2025, Vol. 6, No. 1
O-ISSN:2709-6262	https://doi.org/10.47205/jdss.2025(6-I)32	[364-374]

JDSS Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Social Engineering Attacks in Pakistan: Analyzing the Weakest Link in Cyber Security

[1]Shabana Kausar and [2]Ali Raza Laghari

1. Ph. D (Law) Scholar and Lecturer at Institute of Law University of Sindh Jamshoro, Sindh, Pakistan
2. Assistant Professor, Institute of Law University of Sindh Jamshoro, Sindh, Pakistan

***Corresponding Author:** adv.shabanakausar@gmail.com

ABSTRACT

This paper analyzes the prevalence, types, and root causes of social engineering attacks in Pakistan, emphasizing their implications. Researcher also proposed some possible solutions. In the era of rapid technological advancement, social engineering attacks have emerged as a significant cyber security challenge, particularly in countries like Pakistan undergoing swift digital transformation. Social engineering manipulates human vulnerabilities through techniques such as phishing, vishing, baiting, and pretexting, making individuals the focal point of exploitation rather than systems (NADRA. 2024). Researcher employed Doctrinal methodology and rely on research articles, books cases and online information available on websites. In Pakistan, the lack of cyber security awareness, digital illiteracy, weak organizational protocols, cultural tendencies toward trust, and an inconsistent legal framework have created a conducive environment for such attacks. The impacts are far-reaching, ranging from financial losses and data breaches to erosion of public trust and national security risks (FBR. 2021). Researcher suggest that to address this growing threat, the article recommends a multi-faceted approach, including cyber security awareness campaigns, digital literacy initiatives, strengthened organizational policies, technological solutions, and legal reforms. By fostering a culture of vigilance and resilience, Pakistan can mitigate these risks and safeguard its digital ecosystem.

KEYWORDS Cyber-Attacks, Vulnerable Security, Social Engineering Attacks, Digital, Technology, Weblinks Risk, Data Theft

Introduction

Whole world is facing new revolutionary Era of cyber influence including Pakistan. In the digital age, the growing dependance on technology has brought both opportunities and challenges. One of the most significant and highly effecting challenges is cybersecurity, where social engineering attacks have emerged as a critical concern. Social engineering, the art of manipulating individuals to divulge confidential information, exploits the human factor, often referred to as the weakest link in cybersecurity (NADRA. 2024). In Pakistan, a country experiencing rapid digitization, the prevalence of social engineering attacks has grown alarmingly, threatening businesses, governmental institutions, and individuals alike. This essay aims to analyze the dynamics of social engineering attacks in Pakistan, explore their underlying causes, assess their impacts, and suggest measures to mitigate this growing menace.

The Concept of Social Engineering: "Social engineering" influences emotional manipulation to exploit human vulnerabilities rather than technical weaknesses. Attackers use techniques such as phishing, baiting, pretexting, and tailgating to deceive victims into revealing sensitive data, such as passwords, financial information, or access credentials. Unlike traditional hacking, which targets systems, social engineering attacks focus on individuals, making them particularly challenging to counter (Jalal, Alon, & Paltrinieri, 2021).

- In Pakistan, the lack of widespread cybersecurity awareness and digital literacy exacerbates the problem. Many individuals and organizations fail to recognize the signs of a social engineering attack, making them easy targets for cybercriminals (FBR. 2021). This situation is further compounded by a cultural tendency toward trust, which attackers exploit to their advantage.
- **Prevalence and Types of Social Engineering Attacks in Pakistan:** Now a days during 2024 social engineering attacks in Pakistan have taken various forms, ranging from simple phishing scams to sophisticated schemes involving multiple layers of deception (FBR. 2021). Among the most common types are:

a. **Phishing Attacks (email and links phishing):** Phishing involves sending fraudulent emails or messages that appear to come from legitimate sources. In Pakistan, phishing scams often target bank customers, luring them into revealing their account details under the guise of security verification (Zaman, R., & Latif, A. 2023). With the rise of online banking, such attacks have become increasingly prevalent.

b. **Vishing (Voice Phishing):** Voice phishing, or vishing, uses phone calls to deceive victims. Scammers often pose as representatives from financial institutions or government agencies. For instance, victims might receive calls claiming they have unpaid taxes or that their bank account has been compromised, prompting them to share sensitive information (Zaman & Latif, 2023).

c. **Baiting:** Baiting exploits human curiosity or greed by offering something enticing, such as free software or gifts, to lure victims into downloading malware or providing personal information. USB-based baiting schemes are common in offices and educational institutions (Zaman & Latif, 2023).

d. **Pretexting:** In pretexting, attackers create a fabricated scenario to gain the victim's trust. For example, attackers might impersonate IT support staff and request login credentials to "fix" a nonexistent issue. This method has been reported in corporate and public sector environments (Zaman & Latif, 2023).

Literature Review

Government of Pakistan making Laws time to time to combat cyber-attacks and trying to bring criminals in Court of Law and punish them for their crime but a big hindrance in this way is that this crime has no boundaries and territorial jurisdiction because any one who is physically present anywhere i.e. India or Afghanistan can commit crime in Pakistan, therefore international cooperation to combat the situation is necessary and need of time. Pakistan did not have extradition treaties with too many countries and it provides an easy shelter to cyber criminals (Jalal, Alon, & Paltrinieri, 2021). Pakistan Government also made following Laws to address these issues:

Prevention of Electronic Crimes Act (PECA) 2016

Scope: PECA 2016 is the primary law for addressing cybercrimes in Pakistan. It outlines offenses, investigation procedures, and penalties for cyber-related crimes.

Key Features

- **Cybercrimes Defined:** Includes hacking, unauthorized access, cyberstalking, online harassment, spoofing, and identity theft.

- **Penalties:** Prescribes fines and imprisonment based on the severity of the offense (e.g., up to 7 years for unauthorized access to critical infrastructure).
- **Child Exploitation:** Severe punishments for creating, sharing, or distributing child pornography.
- **Hate Speech and Defamation:** Criminalizes online hate speech and defamation, with specific penalties.
- **Cyberterrorism:** Harsh penalties for using cyberspace for terrorism or threatening critical infrastructure.
- **Data Protection:** Limited provisions for securing personal and organizational data (NADRA. 2024).

Pakistan Telecommunication (Re-organization) Act, 1996

Purpose: Focuses on regulating telecommunication services and addressing illegal interception of communications. It was made to

- **Prohibits Unauthorized Access:** Outlines punishments for unlawful access to telecommunications networks.
- **Interception and Surveillance:** Provides guidelines for lawful interception of communication by authorized entities.

Electronic Transactions Ordinance (ETO), 2002: Facilitates electronic transactions and e-commerce by providing legal recognition to electronic communications and documents.

Purpose: Grants electronic signatures and records the same legal validity as traditional paper-based documents. Encourages businesses to adopt secure electronic systems to protect data integrity and confidentiality.

Data Protection Bill (Draft): Although not yet enacted, this draft bill seeks to regulate the processing, storage, and protection of personal data in Pakistan.

Purpose: Requires organizations to protect personal data and prohibits unauthorized processing. Mandates notification of data breaches to individuals and the regulator. To set conditions for transferring data outside Pakistan.

National Cyber Security Policy 2021: It is a strategic document outlining Pakistan's vision for enhancing national cybersecurity.

Purpose: Emphasizes the development of technical skills and cybersecurity awareness. It Establishes a National Computer Emergency Response Team (CERT) to respond to cyber incidents. It was made to focuses on securing critical systems like energy, finance, and defense. It also Encourages partnerships to strengthen cybersecurity resilience.

The Investigation for Fair Trial Act, 2013: Allows law enforcement agencies to collect evidence through surveillance and interception in cybercrime cases.

Purpose: It provides legal backing for monitoring online communication for national security purposes. It requires court approval for surveillance operations.

Banking Laws and Guidelines: The State Bank of Pakistan (SBP) issues various regulations for cybersecurity in the financial sector:

- **Cybersecurity Framework for Banks (2017):** Requires banks to implement robust cybersecurity measures, including risk assessments and incident response plans.

- **Outsourcing Guidelines:** Emphasizes securing outsourced services, particularly IT functions.

Problems in implementation: Researcher noted that lack of awareness and training among stakeholders. Due to inadequate enforcement mechanisms and infrastructure facing challenges in Implementation (Zubair, K. 2021). In Pakistan due to very limited public awareness of rights and reporting mechanisms very little cases comes on record. These laws and policies are critical in addressing the growing cybersecurity challenges in Pakistan, though further refinement and enforcement are necessary to ensure their effectiveness.

Cases of Data Breaches Involving Pakistan:

- In 2024 Russian state-sponsored hackers infiltrated a Pakistani Advanced Persistent Threat (APT) group, leveraging their espionage campaigns to extract information from government and military targets in Afghanistan and India (Zulfikar, N. 2023).
- The Pakistani APT group "Transparent Tribe" expanded its operations to include cross-platform malware, targeting entities in India and Afghanistan (Zulfikar, N. 2023).
- Pakistani hackers deployed the DISGOMOJI malware in phishing attacks against Indian government officials, exploiting vulnerabilities to gain unauthorized access (Zulfikar, N. (2023).
- Cybercriminals targeted Pakistani individuals with tax-related phishing emails containing malicious MSC files, leading to the installation of obfuscated backdoors (Zulfikar, N. 2023).
- A significant data breach exposed the personal information of approximately 115 million Pakistani mobile users, raising concerns about data security practices (Zulfikar, N. 2023).
- Phishing emails impersonating Pakistani Armed Forces were used in targeted attacks against the country's critical information infrastructure (Zulfikar, N. 2023).
- The official websites of Pakistan's Ministry of Foreign Affairs and the Army were compromised by hackers, disrupting services and raising security concerns (Zulfikar, N. 2023).
- Sensitive personal data of approximately 2.7 million Pakistanis was compromised from the National Database and Registration Authority (NADRA), notably from offices in Multan, Karachi, and Peshawar (FBR. 2021).

International Breaches

- Marriott faced a series of data breaches affecting over 344 million customers, exposing sensitive information like passport details and payment cards (Marriott International Data Breach 2018-2020).
- An adult streaming website, Cam4, suffered a data breach exposing more than 10 billion data records, making it one of the largest breaches in history (Cam4 Data Breach 2020).
- Yahoo experienced a data breach affecting all 3 billion of its user accounts, exposing names, email addresses, and hashed passwords (Yahoo Data Breach (2013).

- LinkedIn suffered a data breach where 165 million email and password combinations were stolen and later sold online (LinkedIn Data Breach 2012).
- Alibaba's shopping platform, Taobao, was scraped by an affiliate marketer who collected over 1.1 billion pieces of user data over eight months (Alibaba Data Breach (2019).
- India's national ID database, Aadhaar, experienced a breach where the personal information of over 1.1 billion citizens was exposed (Aadhaar Data Breach 2018)
- A massive database named RockYou2024 was compiled, containing nearly 10 billion leaked passwords, posing significant risks for credential stuffing attacks (RockYou2024 Password Leak 2024).
- Retailer Hot Topic was hacked by the group Dark X, resulting in the theft of data belonging to 350 million customers, which was then sold on underground forums (Hot Topic Data Breach (2024).
- Australian banking apps, including those of major banks, were targeted in a sophisticated malware attack aimed at Android users, leading to significant security concerns (Australian Banks Targeted by Global Cyber Robbery (2024).
- The WHO faced a cyberattack where hackers leaked login credentials of staff members during the COVID-19 pandemic, highlighting vulnerabilities in global health organizations (World Health Organization Cyber Attack (2020).
- Adobe Systems suffered a breach where hackers obtained access to user information and source code, affecting approximately 150 million customers (Adobe Data Breach (2013).
- The online marketplace LivingSocial experienced a security breach exposing names, email addresses, and password data for up to 50 million users (Living Social Data Breach 2013).

Pakistan has low literacy rate and increasing use of smart phones and internet along with Socializing fever on websites. It makes easy for criminal mind peoples to commit fraud and deceive innocent and illiterate peoples; this increasing problem needs special steps to be taken to address it. Therefore, Researcher decided to learn and find some solutions.

Root Causes of Social Engineering Vulnerabilities in Pakistan

Several factors contribute to the prevalence of social engineering attacks in Pakistan. These include:

- **Low Cybersecurity Awareness** A significant portion of the population remains unaware of cybersecurity best practices. Many individuals do not verify the authenticity of emails, calls, or websites, making them vulnerable to manipulation.

- **Digital Illiteracy** Despite rapid technological advancements, digital literacy levels in Pakistan remain low. This gap leaves individuals and small businesses unprepared to identify and counter cyber threats.

- **Weak Organizational Policies** Many organizations lack robust cybersecurity protocols. Employees often receive little to no training on recognizing social engineering tactics, leaving them susceptible to attacks.

- **Cultural Factors**: Pakistan's collectivist culture often emphasizes trust and cooperation, which attackers exploit. People are more likely to comply with requests that appear to come from authority figures or familiar entities.

- **Inadequate Legal Framework**: While Pakistan has laws addressing cybercrime, enforcement remains inconsistent. This creates an environment where attackers feel emboldened to operate with minimal fear of repercussions.

Impacts of Social Engineering Attacks

The consequences of social engineering attacks in Pakistan are far-reaching, affecting individuals, businesses, and the nation's overall cybersecurity posture.

- **Financial Losses**: Victims of social engineering often suffer significant financial losses. Phishing scams targeting bank customers and small businesses have led to substantial monetary theft.
- **Data Breaches**: Organizations targeted by social engineering attacks risk exposing sensitive data. This can lead to reputational damage, legal liabilities, and operational disruptions.
- **Erosion of Trust:** Frequent social engineering incidents erode public trust in digital platforms, hindering the adoption of online services and slowing digital transformation efforts.

National Security Risks: Researcher noted that social engineering attacks targeting governmental institutions can have severe implications for national security. Breaches in critical sectors, such as defense or energy, could have catastrophic consequences (Tahir, F., & Iqbal, H. 2019).

Countermeasures and Recommendations: Researcher suggest that to combat the growing threat of social engineering attacks, a multi-pronged approach is essential. The following measures can help mitigate risks in Pakistan:

- **Cybersecurity Awareness Campaigns:** Government should initiate public and private cooperation to launch nationwide campaigns to educate individuals about social engineering tactics. Such initiatives should focus on recognizing phishing attempts, verifying sources, and safeguarding personal information.
- **Digital Literacy Programs:** By incorporating digital literacy into national educational curriculums can help bridge the knowledge gap. Workshops and training sessions targeting specific demographics, such as students and small business owners, can be particularly effective.
- **Strengthening Organizational Policies**: Researcher also recommend that organizations should implement comprehensive cybersecurity policies, including regular training for employees on identifying and reporting social engineering attempts. Simulated phishing exercises can also help reinforce vigilance (Tahir, F., & Iqbal, H. 2019).
- **Technology-Based Solutions:** By leveraging technologies such as multi-factor authentication (MFA), spam filters, and endpoint security can reduce exposure to social engineering attacks. Encouraging the use of encrypted communication channels adds an additional layer of protection.
- **Legal and Regulatory Frameworks:** there is a need of strengthening Pakistan's cybercrime laws and ensuring their enforcement can deter attackers. Collaboration with international cybersecurity organizations can also enhance threat intelligence and response capabilities.
- **Cultural Shift:** By promoting a culture of skepticism and critical thinking can empower individuals to question unsolicited requests and identify potential scams. Encouraging open communication within organizations can also facilitate early detection of suspicious activities.

Material and Methods

Researcher employed doctrinal method of research for present article. Researcher relied on secondary sources of data because general public is not even aware about recent technicalities and vulnerability of cyber security problems.

Results and Discussion

Researchers analysis revealed that social engineering attacks in Pakistan are pervasive and multifaceted, leveraging both human and systemic vulnerabilities. Key findings include:

Prevalence of Attacks: Now a days social engineering attacks, including phishing, vishing, baiting, and pretexting, are widespread. These methods exploit the lack of cybersecurity awareness, digital literacy, and weak organizational policies (Tahir, F., & Iqbal, H. 2019).

Root Causes: Researcher identified following root causes of these increasing crime in Pakistan:

- That a significant portion of the population is unaware of basic cybersecurity practices, making them vulnerable.
- That limited understanding of digital technologies amplifies susceptibility to attacks.
- That trust-oriented cultural norms are frequently exploited by attackers.
- That inconsistent enforcement and a lack of international cooperation hinder effective response to cybercrimes (FBR. 2021).
- That these methods dominate due to their simplicity and effectiveness in extracting sensitive information.
- That less common but equally impactful, targeting corporate and public sectors.
- That due to these attacks people face direct monetary theft from individuals and businesses (FBR. 2021).
- That compromise of sensitive organizational and personal information.
- That public mistrust in digital platforms and online services.
- That there is a significant threats to critical infrastructure and governmental operations.

Discussion

Researcher underscore that there the critical need for a comprehensive approach to mitigate social engineering attacks in Pakistan. Despite significant technological advancements, the human factor remains the weakest link in the cybersecurity chain. Addressing this challenge requires a multi-pronged strategy:

- Nationwide cybersecurity awareness campaigns are essential to educate the public on recognizing and avoiding common attack techniques.
- Incorporating digital literacy into school curriculums can create a foundational understanding of secure digital practices.
- That regular training sessions for employees to recognize social engineering tactics can significantly reduce vulnerabilities.
- That simulated phishing exercises can prepare staff for real-world scenarios and reinforce vigilance.
- That by Implementing multi-factor authentication (MFA), spam filters, and robust endpoint security measures can mitigate exposure to attacks.

- Leveraging advanced tools like artificial intelligence (AI) for threat detection and behavioral analytics can enhance incident prevention and response capabilities.

Legal and Regulatory Reforms:

- Strengthening existing cybercrime laws, such as the Prevention of Electronic Crimes Act (PECA) 2016, and ensuring their enforcement is critical.
- Collaborating with international cybersecurity organizations and establishing extradition treaties can improve response to transnational cybercrimes.
- Researcher observed by promoting a culture of skepticism and critical thinking can empower individuals to question unsolicited requests and detect potential scams.
- Researcher also underline that encouraging open communication within organizations can facilitate the early identification of threats.

Implications for Policy and Practice: Researcher in present study highlighted the urgent need for a coordinated effort by stakeholders, including the government, private sector, and civil society, to address social engineering attacks. Researcher recomend combining technological solutions, educational initiatives, and robust policies, Pakistan can strengthen its cybersecurity posture and reduce the risks posed by these pervasive threats (Jalal, Alon, & Paltrinieri, 2021).

Conclusion

Researcher in conclusion, while the human element and also weak programing is identified and highlighted as the weakest link in cybersecurity, it can be transformed into the strongest defense with proper awareness, training, and vigilance. Building a secure digital ecosystem requires not only technological advancements but also a cultural and institutional shift towards proactive cybersecurity practices (Tahir, F., & Iqbal, H. 2019). Social engineering attacks represent a formidable challenge in Pakistan's evolving cybersecurity landscape. By exploiting human vulnerabilities, these attacks have the potential to cause significant financial, operational, and reputational harm. Addressing this issue requires a concerted effort from individuals, organizations, and the government. Through awareness, education, technological advancements, and robust policies, Pakistan can fortify its defenses against social engineering threats and build a more secure digital environment. While the human factor is often seen as the weakest link in cybersecurity, it can also become the strongest line of defense with the right knowledge and practices.

Recommendations

Researcher pleased to recommend following steps to be taken to secure internet use in beloved country Pakistan:

- Require multiple forms of verification (e.g., passwords and biometrics) to access systems will be helpful.
- Ensure all software and systems are up-to-date to address known vulnerabilities and attacks.
- Deploy these tools to monitor and block unauthorized access to networks.
- Apply strong encryption for sensitive data, both in transit and at rest.
- Limit access by verifying every user and device attempting to connect to a network.
- Educating employees on recognizing phishing attempts, secure password practices, and safe browsing habits will improve efficiency.
- By encouraging employees to report potential security breaches without fear of reprisal is also a key to protection.

- Conduct regular penetration tests and phishing simulations to evaluate preparedness.
- Create a Software based Cybersecurity Framework: Adopt standards such as NIST, ISO 27001, or CIS to guide security policies.
- Periodically evaluate and address vulnerabilities within the organization.
- Incident Response Plan: Establish a clear protocol for detecting, responding to, and recovering from security breaches.
- Artificial Intelligence (AI) for Threat Detection: Leverage AI to identify unusual patterns and potential threats in real time.
- Endpoint Detection and Response (EDR): Monitor devices connected to the network for suspicious activities.
- Behavioral Analytics: Use analytics to detect deviations from normal user behavior that could indicate an attack.
- Participate in Cybersecurity Information Sharing Communities: Collaborate with industry peers to share threat intelligence.
- Work with Law Enforcement: Establish relationships with local and international cybersecurity authorities to respond to incidents swiftly.
- Assess Third-Party Vendors: Conduct regular security audits of vendors and partners to ensure they meet cybersecurity standards.
- Implement Secure Development Practices: Enforce secure coding and testing practices for software and system development.
- Use Virtual Private Networks (VPNs): Ensure secure connections for remote workers.
- Secure Remote Access Tools: Adopt tools with robust security features for accessing organizational resources.
- Monitor Remote Devices: Require endpoint protection for devices used outside the office.
- Obtain insurance coverage to mitigate financial losses in the event of a significant cybersecurity incident.
- Real-Time Monitoring: Use Security Information and Event Management (SIEM) tools for continuous oversight.
- Incident Reviews: After an attack, analyze the incident to learn and strengthen defenses.
- Proactive Threat Hunting: Regularly search for indicators of compromise within the network.

References and Biblography:

Ali, H. (2020). Phishing trends in Pakistan: An evaluation. *Cyber Journal of South Asia*, volume:6(2), 45-58.

Anwar, T., & Zaidi, N. (2021). The impact of digital illiteracy on cybersecurity in developing nations. *International Journal of Digital Literacy*, volume:5(1), 32-49.

Bashir, M., & Rehman, Z. (2022). Cybercrime laws in Pakistan: Effectiveness and enforcement challenges. *Legal Review of Cybersecurity*, 18(1), 67-89.

Bergeron, A., Décary-Hétu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy, 83*, 102870. https://doi.org/10.1016/j.drugpo.2020.102870

Bergeron, A., Décary-Hétu, D., Giommoni, L., & Villeneuve-Dubuc, M. P. (2022). The success rate of online illicit drug transactions during a global pandemic. *International Journal of Drug Policy, 99*, 103452. https://doi.org/10.1016/j.drugpo.2021.103452

CISO Magazine. (2021). Pakistan's Army and Foreign Ministry websites hacked. Retrieved from https://www.cisomag.com

Dark Reading. (2024). Transparent Tribe APT aims for cross-platform impact. Retrieved from https://www.darkreading.com

FBR. (2021). Advisory No. 60: Cyberattacks on Pakistan's critical information structure. Retrieved from https://download1.fbr.gov.pk

Groshkova, T., Stoian, T., Cunningham, A., Griffiths, P., Singleton, N., & Sedefov, R. (2020). Will the current COVID-19 pandemic impact on long-term cannabis buying practices? *Journal of Addiction Medicine*. Advance online publication. https://doi.org/10.1097/ADM.0000000000000724

Hacker News. (2024). Hackers use DISGOMOJI malware to target Indian government. Retrieved from https://www.thehackernews.com

Jalal, R. N. U. D., Alon, I., & Paltrinieri, A. (2021). A bibliometric review of cryptocurrencies as a financial asset. *Technology Analysis & Strategic Management.* Advance online publication

Kausar, S. (2024). Analytical study of social engineering attacks in Pakistan. *Institute of Law University of Sindh Journal*, 7(2), 123-142.

Khan, A. M. (2020). The role of trust in social engineering attacks: Evidence from Pakistan. *Journal of Security Studies*, 10(4), 56-73.

Khan, Z. (2021). Strengthening cybersecurity frameworks in South Asia. *Asian Security Journal*, 12(3), 34-56.

Marriott. (2024). FTC orders data security improvements for Marriott hotels. Retrieved from https://www.theverge.com

NADRA. (2024). Personal data breach in NADRA: Analysis of vulnerabilities. *Journal of Data Protection in Pakistan*, 9(2), 45-67.

NIST. (2023). Cybersecurity framework 2.0. Retrieved from https://www.nist.gov

State Bank of Pakistan. (2017). Cybersecurity framework for financial institutions. Retrieved from https://www.sbp.org.pk

Statista. (2020). Global data breaches and their impact. https://www.statista.com

Sun, T. (2024). The largest password leak: Implications for global cybersecurity. Retrieved from https://www.thesun.ie

Tahir, F., & Iqbal, H. (2019). Social engineering vulnerabilities: Lessons from Pakistan. *Cyber Policy Review*, 6(3), 34-47.

The Australian. (2024). Global cyber heist targets Australian banks. https://www.theaustralian.com.au

The Verge. (2024). Data breach highlights security flaws in hospitality. https://www.theverge.com

UNESCO. (2021). Enhancing digital literacy in developing nations. https://www.unesco.org

Wikipedia. (2020). Cybersecurity in developing countries. https://en.wikipedia.org

Wikipedia. (2024). NADRA data breach: Lessons learned. https://en.wikipedia.org

Wired. (2024). Dark X hackers target retailer Hot Topic. https://www.wired.com

Yasin, M. (2022). Zero trust architecture: A case for Pakistan. *Journal of Modern IT Security*, 5(3), 78-93.

Zaman, R., & Latif, A. (2023). Evaluating cybersecurity awareness campaigns in Pakistan. *Journal of Public Awareness and Security*, 7(1), 15-29.

Zia, U. (2019). Cybersecurity challenges for SMEs in Pakistan. *Small Business Journal of Cyber Risks*, 8(2), 12-23.

Zubair, K. (2021). Bridging the gap in digital literacy. *Journal of Digital Transformation*, 9(1), 22-41.

Zubair, M. (2022). Cyber laws and enforcement in Pakistan: A critical review. *Legal Perspectives on Cyber Issues*, 11(4), 78-90.

Zulfikar, N. (2023). Tackling phishing scams: A strategic approach for Pakistan. *Cyber Defense Review*, 13(3), 31-49.