DOI: 10.71317/jgst.2.9(s2).2026.678
Journal of Global Social Transformation
Journal homepage: https://rjsaonline.org/index.php/JGST

Social Engineering and Cybercrime Victimization: Understanding The Hacking Misconception, Human Vulnerabilities, and Prevention Strategies in Cyber Landscape

Dr. Syed Muhammad Irfan[1], Dr. Naima Saeed[2], Syed Muhammad Abdullah Yousuf[3]
[1] Department of Criminology, University of Karachi.
Email: smirfan2025@gmail.com
[2] Chairperson, Department of Criminology, University of Karachi.
Email: naima.saeed7@gmail.com
[3] BSCS, Institute of Business Administration (IBA), Karachi.
Email: abdullahyousuf1234@gmail.com

ARTICLE INFO

Submission:
August 05, 2026
Revised:
August 20, 2026
Accepted:
September 09, 2026
Available Online:
September 24, 2026

Keywords:
social engineering, cybercrime, victimization, Routine Activity Theory, cyber security awareness, vulnerabilities, manipulation

Corresponding author:
Dr. Syed Muhammad Irfan
Email:
smirfan2025@gmail.com

ABSTRACT

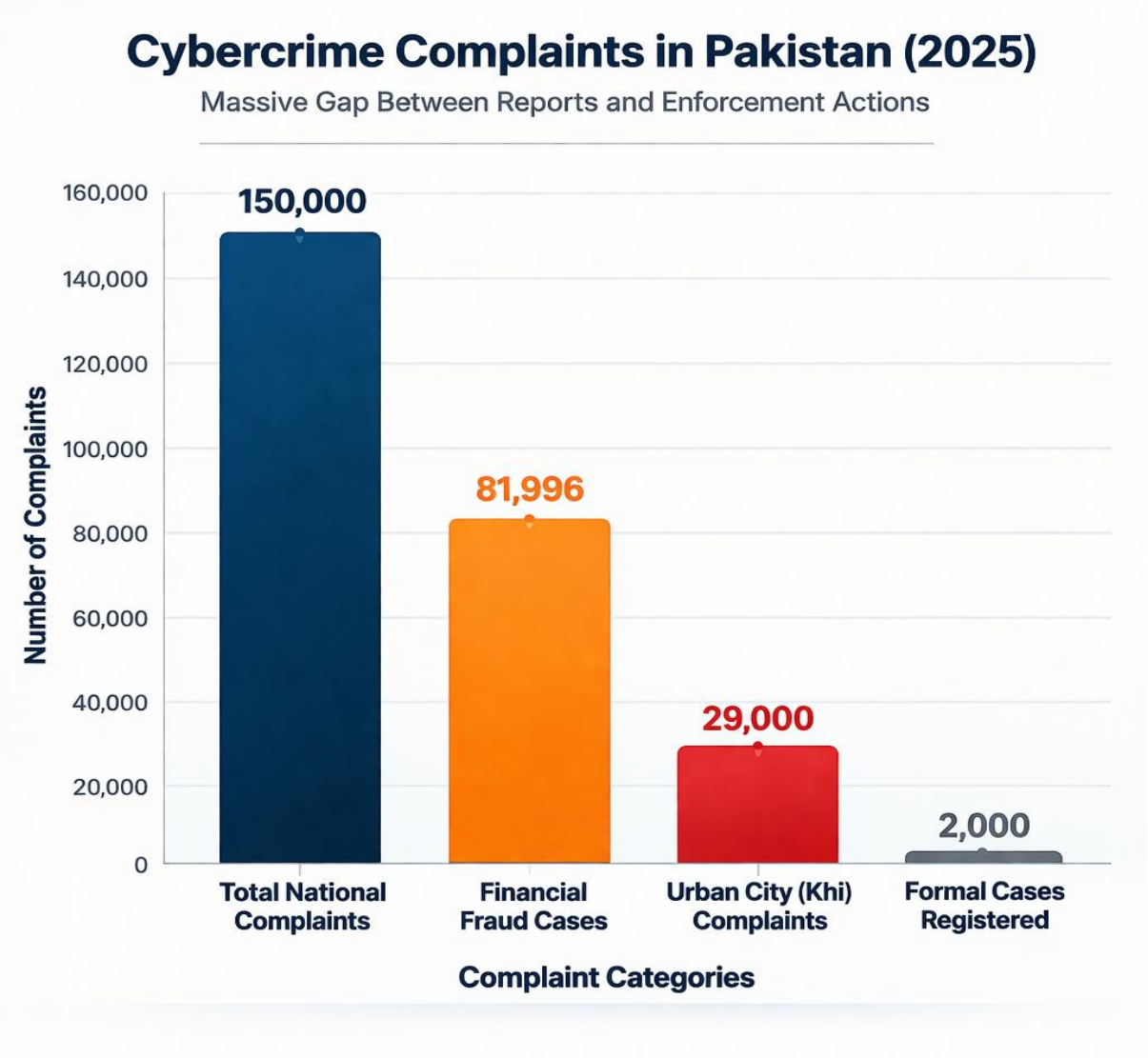
In this study, prevalence of social engineering scams and cybercrime victimization has been researched. This study is conducted in Pakistan, with particular focus on major cities, as major urban centers experience rapid digital transformations. A qualitative research design is used along with semi-structured interviews with 36 cybersecurity professionals to investigate the tactics used by cybercriminals. Interview includes the exploration of human vulnerabilities that enable fraud, and the role of cybercrime awareness in preventing victimization in digital platforms. The findings reveal that social engineering attacks are very common which particularly include banking verification scams, messaging account takeovers, and investment fraud. Social engineering is the most common forms of cyber attack in Pakistan. Another important aspect of this study reveals and identifies a widespread misconception among victims and other people, who frequently describe their experiences as "hacking." It is noted that in reality victims are involved voluntarily in disclosing their sensitive information through psychological manipulation by the cyber criminals. Routine Activity Theory is used as a theoretical framework. And cybercrime victimology framework is applied for conceptual understanding. This study reveals that motivated offenders, suitable targets, and absent guardianship are the major characteristics that prevail in digital environments. In conclusion by strengthening cybercrime and cybersecurity awareness, increasing digital literacy, and improving institutional response capacity are of paramount importance for reducing cybercrime victimization in Pakistan.

Introduction

The exponential growth of internet accessibility, mobile banking, and digital payment systems has enormously transformed economic and social interactions in Pakistan. It is extremely important and offers benefits in efficiency, connectivity, and financial inclusion. There are more than 140 million internet users nationwide. Digital platforms and social media have become integral to daily life. It is enabling millions of citizens to conduct financial transactions, communicate through social media, and participate in e-commerce (Profit by Pakistan Today, 2026). However, this digital transformation has expanded the vulnerability of users and attack surface for cybercriminals. They are creating new opportunities regularly for exploitation which not only threaten individual financial security and trust in digital infrastructure. In major metropolitan cities, online scams and digital fraud have increased dramatically in recent years. Theses cybercrimes are posing serious financial and psychological risks to victims while undermining confidence in Pakistan's growing digital economy (Profit by Pakistan Today, 2025).

Although cybercrime victims frequently characterize their experiences as hacking while a large number of these cybercrimes are not executed through sophisticated technical hacking skills. Cybercriminals use social engineering attacks which are the techniques that exploit human psychology to manipulate individuals into voluntarily revealing confidential information. These include sharing one-time passwords (OTPs), or transferring money to criminals through deceit (NCCIA, 2025). Hacking is a systematic process where technical vulnerabilities in computer systems or software are being exploited. Through social engineering cyber criminals attack the targets who are the most vulnerable segment in any security system, which is humans and their decision-making capability. Cyber criminals draft convincing messages and emails, impersonate as trusted organization or person and use urgency, greed, fear or sympathy to deceive and bypass technological security controls. It is very important to understand the difference between technological cyberattacks and psychological manipulation. Without clear understanding, effective prevention measures and improving cybersecurity awareness among people are not possible.

The exponential increase in cybercrimes is alarming and becoming more challenging for authorities to manage and mitigate. According to official data presented in National Assembly of Pakistan, cybercrime incidents have increased by 35% in 2025. Authorities received 150,000 cybercrime complaints nationwide, as it should be noted that actual incidents may be huge in numbers due to widespread underreporting (Urdupoint, 2026). There are more than 81,000 cases reported for financial frauds alone, as it the largest category of reported cybercrime in Pakistan (Profit by Pakistan Today, 2026). In a testimony by National Cyber Crime Investigation Agency (NCCIA) to parliament committee, it was stated that the financial impact is quite alarming as the estimated value of losses due to this financial fraud is Rs 3 billion (Daily Pakistan English News, 2025).



Metropolitan city, Karachi has become the major center for this cybercrime epidemic. It is the commercial and industrial hub of the country. There were approximately 29,000 cybercrime complaints registered in the city, which is the one-fifth of the total national cybercrime complains (Profit by Pakistan Today, 2025). The frequently reported cybercrime in Karachi includes social media accounts takeovers, banking frauds, and online marketplace scams. The major reasons for this density of cybercrime increase in Karachi are widespread adoption of smart phones, digital banking, and lack of security awareness which cyber criminals seek to exploit. It is worth noting that social engineering tactics were used in most of these cybercrimes.

Cybercrime threats in Pakistan extend beyond the officially reported complaints statistics. Different surveys have revealed that more than half of the consumers nationwide have experienced some form of digital fraud. In surveys 20% reported that they have been targeted multiple times by cybercriminals. It indicates that victimization is increasingly likely for internet users (MM News, 2024). The survey's findings suggest that online activities have multiple threats and risks for its users. especially social engineering tactics which are quite sophisticated and not easy for them to identify.

Background of Study

There are more than 140 million internet users in Pakistan (Profit by Pakistan Today, 2026). The exponential growth and adoption of internet, mobile banking, e-commerce transactions, etc. have significantly transformed the economic and social transformation. Although it has brought advantages in efficiency, connectivity and financial inclusion, this cyber transformation has increased the cyberattack surface for cyber criminals as well. It has given new opportunities for cyber risks and exploitation which are threatful for both financial security of individuals and their trust in digital infrastructure.

Misconceptions About "Hacking" in Online Fraud

There is a critical misconception regarding hacking and cybercrime persist among public which hinders effective prevention strategies.

The Conceptual Confusion Between Hacking and Social Engineering

A misconception among victims of online fraud is the belief that their accounts have been "hacked." Individuals commonly use the term "hacking" to describe any unauthorized financial transaction, social media account takeover, or digital fraud incident in their daily language (Furnell, 2021). However, cybersecurity research draws a clear and critical distinction between hacking and social engineering. Hacking refers to the technological exploitation of vulnerabilities in computer systems, networks, or software to gain unauthorized access by cyber criminals (Yar & Steinmetz, 2019). Whereas most of the cyber scams are carried out through social engineering tactics by cyber criminals to victims where they are psychologically manipulated to voluntarily provide their sensitive information like passwords, one time password (OTPs), or account verification details (Hadnagy, 2018).

Why Distinction Matters for Prevention

When cybercriminals use social engineering tactics and impersonate as a legitimate bank representative, they convince the victim to provide their OTP or bank details. The criminals simply use their actual authentication credentials to access victim's bank account (Nobles, 2022). It should be noted that the system has not been compromised technically, instead the victim has been manipulated into granting access to sensitive bank account. This difference is not simply semantic but has greater significance and implications for preventive measures. If the victims keep believing that they are "hacked", it may make them feel powerless as not everyone can understand and escape technological cyberattacks. It is necessary to make victims understand that their own awareness and behavioral choices can keep them safe from these attacks, as they were manipulated (Button & Cross, 2017). This significant understanding can shift the efforts of authorities from purely technological solutions to comprehensive cyber literacy programs that address the social engineering and human vulnerabilities (Williams et al., 2017).

The Role of Social Engineering

In this study it is revealed that a significant number of cybercrimes are not executed through sophisticated technological skills, instead cyber criminals relied on social engineering tactics. While victims of these cybercrimes reported their sufferings as hacking.

Understanding Social Engineering as a Cybercrime Method

Social engineering is a methodology where cyber criminals exploit and manipulate human psychology rather than using the technical vulnerabilities of computer systems, networks or software to access sensitive information or financial resources (Hadnagy, 2018).

Cybercriminals unlike traditional hacking, use social engineering tactics for manipulating human cognition, emotions, and behavioral patterns to bypass the most advanced cyber security controls (Mitnick & Simon, 2002). This basic difference makes social engineering attacks more harmful in a way that is gradual and not easily noticed. It specifically targets the human factor which is considered as the weakest link in cyber security domain (Nobles, 2022). Cybersecurity professionals globally emphasize that organizations even with most advanced technological security tools are vulnerable to cyberattacks if the users are not trained regarding social engineering attacks. They can be manipulated by cyber criminals to provide sensitive credentials or authentication codes through social engineering (Button & Cross, 2017).

It is notable that authorities in Pakistan have warned regarding complications and difficulties in prevention against social engineering attacks due to inherent human tendencies for trust and compliance, while technical vulnerabilities can be patched or updated when discovered (ProPakistani, 2023).

Psychological Foundations and Attack Stages

Social engineering attacks are very effective due to its systematic exploitation of human psychological traits and cognitive biases. Cyber criminals usually employ processes like

a) **Information gathering**
In this stage cyber criminals collect the personal information of targeted persons from social media platforms, open sources databases, or previously breached information (Wang et al., 2021). It enables cybercriminals to draft and craft convincing messages or mails tailored to specific individuals.

b) **Establish trust**
Cyber criminals impersonate as legal authorities like representatives from a bank, any government official, or employee from any telecommunication company which makes individuals more willing to comply with their commands naturally (Algarni et al., 2017)

c) **Create urgency or fear**
In this process cyber criminals warn the individuals that if they will not take the immediate action necessitated by criminals, they may face account suspension, monetary loss or legal consequences (Williams et al., 2017). This urgency pressure overrides the rational decision-making of victims and causes them to comply with tricky requests they would otherwise question.

Research Problem and Rationale

There is a critical misconception regarding hacking and cybercrime persisting among public which hinders effective prevention strategies. This misunderstanding has serious consequences as it directs the attention of authorities towards technological cybersecurity controls while human factor remains vulnerable. There is very limited scientific research in Pakistan which examines the human and criminological aspects of cybercrimes. As most research focuses on technological cybersecurity challenges and controls instead of victimization patterns (Ahmed & Khan, 2024).

Research Questions

This study is investigating the following research questions:

- **RQ1:** What types of social engineering scams and online fraud tactics are most commonly used against individuals and organizations in Pakistan?
- **RQ2:** What human vulnerabilities and behavioral factors contribute to cybercrime victimization in social engineering attacks?

- **RQ3:** How does cybersecurity awareness influence the likelihood of individuals becoming victims of online scams and fraud?

Significance of the Study

This study is an attempt to contribute to academic literature on cybercrimes by introducing criminological theories. The findings in the study are evidence based and important insights for policy makers, law enforcements agencies and financial institutions to develop and introduce easy and effective cybercrimes prevention methodologies and mass humanistic awareness campaigns.

Literature Review

The social engineering attacks by cybercriminals to obtain sensitive information or financial gain are increasing exponentially all around the globe (Hadnagy, 2018). The significant increase of smartphones, digital banking applications, and social media platforms have introduced new opportunities for cybercriminals to exploit. Cybercrime like online scams and frauds are the fastest-growing cybercrime affecting not only individuals but organizations as well.

Researcher Christopher Hadnagy elucidates social engineering as one of the most effective cyberattack techniques used by cybercriminals because it bypasses technical cybersecurity controls by targeting the humans are important element of information systems. Kevin Mitnick argues that humans are found to be the weakest link in cybersecurity systems that is why cybercriminals often rely on manipulation and impersonation to obtain sensitive information such as passwords, banking details, or authentication codes (Mitnick & Simon, 2002).

Common forms of social engineering attacks include:

- **Phishing emails**: these are the fraudulent messages used to trick recipients into disclosing sensitive information.
- **Vishing (voice phishing)**: Cyber criminals use phone calls impersonating as legitimate organizations.
- **Smishing (SMS phishing)**: These are the fraudulent text messages containing urgent requests to share sensitive information.
- **Impersonation scams**: cyber criminals pretend to be trusted individuals or authorities who can ask for sensitive information.
- **Romance scams**: it is the exploitation of romantic and emotional relationships for financial gain.

In these cybercrimes, cybercriminals rely on psychological manipulation and persuasion instead of hacking. It makes these cybercrimes particularly difficult to prevent through technological cybersecurity controls alone (Krombholz et al., 2015).

Common Types of Cybercrime

There are several types of cybercrime which rely heavily on social engineering tactics:

a) Banking and OTP Fraud

It involves cybercriminals posing as bank legal representatives. Victims usually receive phone calls or messages in which cyber criminals claim that their bank account has been compromised or requires verification. They persuade the victim to share credentials or OTPs, which allow criminals unauthorized access to the victim's account (NCCIA, 2025).

b) **WhatsApp and Social Media Account Hacking**

Cyber criminals gain control of messaging accounts and contact of victim's friends and family and request them for urgent financial help. As individuals perceive that request appear to come from a trusted person, victims usually transfer the requested amount without any further verification (Profit by Pakistan Today, 2025).

c) Investment and Cryptocurrency

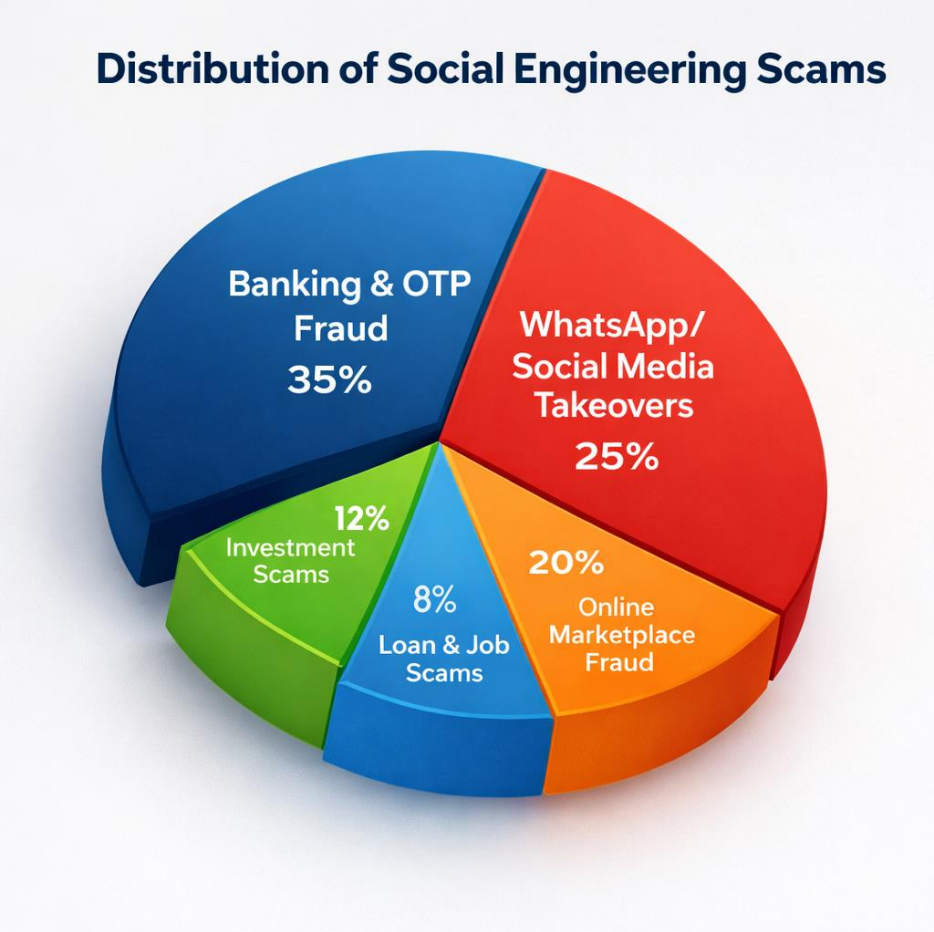
Cyber criminals create fake cryptocurrency or foreign exchange trading platforms where they promise high returns. A major fraud network operating from Karachi reportedly ran a $60 million crypto and forex scam which demonstrates the substantial scale of these illegal operations (Profit by Pakistan Today, 2025).

d) Online Shopping and Marketplace Fraud

Cyber criminals create fake online stores and advertise expensive products at very low prices and request advance payments from interested victims through digital wallets or bank transfers. After receiving payments, they disappear without delivering the product.

e) Loan App and Task-Based Job

In this cybercrime victims usually receive small payments initially to build trust. Then they are persuaded to deposit large amounts for higher rewards, once the amount is deposited cybercriminals disappear.



Theoretical Framework

A theoretical framework is the foundational structure of this research study to support the research problem.

Introduction to the Theoretical Framework

This research study is grounded in an integrated theoretical framework that combines Routine Activity Theory and Cybercrime Victimology. These are used to explain the occurrence of social engineering tactics and factors that increase individuals' vulnerability to cybercrime. These theoretical perspectives provide a comprehensive foundation for understanding how motivated offenders, suitable targets, and situational opportunities converge in cyber environments to facilitate cybercrime (Cohen & Felson, 1979).

Routine Activity Theory

(Cohen & Felson, 1979), propose that crime occurs when three essential elements, a motivated offender, a suitable target, and the absence of capable guardianship are present. It was initially presented to explain physical crimes. This theory has been widely

applied to cybercrime research as cyber environments create unprecedented opportunities for these three elements (Yar & Steinmetz, 2019).

Motivated Offenders in Cyber Environments

It is evident that advances in communication technologies have enabled cybercriminals to operate across borders using advanced tools such as fraudulent call centers for phishing campaigns and automated messaging systems (Nobles, 2022). In Pakistan, some cybercrime networks operate nationally while few collaborate with international cybercriminal groups, as demonstrated by the $60 million crypto and forex fraud exposed in Karachi where foreign nationals were involved (Profit by Pakistan Today, 2025).

Suitable Targets in the Digital Landscape

According to Routine Activity Theory, cyber criminals select targets who are vulnerable or easily accessible. The targets include individuals who frequently use online banking services, conduct digital transactions, share personal information on social media platforms, or possess limited cybersecurity awareness (Reyns, 2013). Over 140 million internet users in Pakistan are creating huge opportunities for victimization through social engineering (Shah et al., 2024).

Absence of Capable Guardianship

It refers to mechanisms that prevent cybercrime which include technological tools, law enforcement activities, and user awareness (Button & Cross, 2017). When these preventive and protective mechanisms are weak or absent, cybercriminals can successfully exploit victims through social engineering techniques. In Pakistan, limited guardianship significantly increases the risk of cybercrime.

Cybercrime Victimology

Cybercrime victimology complements the Routine Activity Theory by analyzing the behavioral, psychological, and situational factors that make certain individuals more vulnerable to cybercrime (Cross, 2018). This perspective signifies the focus from the mere presence of suitable targets to understanding the characteristics that increase susceptibility to social engineering attacks of individuals.

Digital Literacy and Awareness

Awareness and digital literacy play an important role in determining vulnerability to cybercrime. Individuals who lack knowledge about cyber security practices may un deliberately expose themselves to cybercrime by sharing sensitive information. They usually fail to recognize warning signs as well (Sheng et al., 2010). Many cybercrime victims are unaware that one-time passwords (OTPs) should never be shared with anyone whether asked by banks representatives or government institutions. It is revealed in this study that users frequently share sensitive personal information such as phone numbers and addresses on social media platforms which create opportunities for cybercriminals (Ahmed & Khan, 2024). It is important to understand that limited awareness among people is a critical vulnerability that cyber criminals systematically exploit through social engineering attacks.

Psychological and Behavioral Factors

Social engineering attacks are lethal and effective due to exploitation of emotional triggers and cognition which influence the individual's decision making. It is evident through research that humans are prone to respond to messages that create urgency or fear (Williams et al., 2017). Individuals usually get pressurized into sharing their confidential credentials when a message from cyber criminals impersonated as a bank representative claiming that their bank account will be suspended unless immediate action is not taken. Research reveals that urgency and authoritative messages increase susceptibility to cybercrime and people over age of 25 show greater vulnerability (Shah et al., 2024).

Information Sharing Behavior and Digital Footprint

Personal information sharing on digital platforms and social media by individuals increases the risk of being exploited by cyber criminals. Cyber criminals gather personal details like phone numbers, email addresses, job details and daily routine, and use this information to draft a customized convincing social engineering attack which is difficult to avoid (Reyns, 2013). It is important to educate people regarding the sharing of information on social media. Research revealed that internet users sometime share sensitive information without knowing that their information might be exploited by cybercriminals (Ahmed & Khan, 2024).

Integration of Theoretical Perspectives

In explaining cybercrime, Routine Activity Theory and Cybercrime Victimology complement each other comprehensively. Routine Activity Theory elaborates the situational factors that allow cybercrime like presence of motivated offenders, suitable targets, and absent guardianship in cyber spaces. Cybercrime Victimology explains the behavioral characteristics that make individuals vulnerable to cybercrime victimization that include limited digital knowledge, susceptibility to psychological manipulation, and risky online information sharing practices (Cross, 2018).

In this integrated framework:

- Social engineering techniques represent the actions of motivated offenders seeking to exploit human vulnerabilities
- Human psychological and behavioral characteristics represent the factors that make individuals suitable targets
- Cybersecurity awareness and institutional safeguards function as forms of capable guardianship that can disrupt the convergence of offenders and targets

Conceptual Framework

A structured representation of the key concepts, variables, and their presumed relationships within this study

Conceptual Model for Cybercrime Victimization

This research proposes a conceptual framework explaining cybercrime victimization. The model suggests that social engineering techniques influence human vulnerabilities, which ultimately lead to cybercrime victimization. However, cybersecurity awareness and digital literacy play a moderating role that can reduce the likelihood of cybercrime victimization.

The conceptual model includes four key constructs:

Construct Type	Variable	Description
Independent Variable	Social Engineering Techniques	Psychological manipulation used by cybercriminals
Mediating Variable	Human Vulnerabilities	Behavioral and psychological factors that increase Vulnerabilities
Dependent Variable	Cybercrime Victimization	Financial loss, identity theft, or account takeover
Moderating Variable	Cybersecurity Awareness	Knowledge and practices that protect against cybercrime

Hypothesis Development

H1: Social Engineering and Human Vulnerability

Social engineering tactics mostly rely on psychological manipulation to influence victims' decision making. Cybercriminals exploit emotions such as fear, urgency, and trust to convince victims to reveal sensitive information (Hadnagy, 2018; Mitnick & Simon, 2002). Therefore:

H1: Social engineering techniques significantly increase human vulnerability to cybercrime.

H2: Human Vulnerability and Cybercrime Victimization

Human vulnerabilities play an important role in cybercrime victimization. Individuals without awareness about cyber threats are more likely to fall victim to social engineering attacks (Sheng et al., 2010). Therefore:

H2: Human vulnerabilities significantly increase the likelihood of cybercrime victimization.

H3: Cybersecurity Awareness as a Protective Factor

Cybersecurity awareness is an important preventive measure that can mitigate the risk of cybercrime victimization. Many research studies indicated that cybersecurity training and awareness programs significantly reduce social engineering success rates (Krombholz et al., 2015). Therefore:

H3: Cybersecurity awareness negatively moderates the relationship between human vulnerability and cybercrime victimization.

Research Methodology

This section explains the systematic plan for how the study was conducted.

Research Design

In this study qualitative research design is used to understand and explore social engineering attacks and cybercrime victimization patterns. Qualitative research design allows researchers to gain deeper insights into the experiences and perceptions of cybersecurity professionals and IT experts (Braun & Clarke, 2006). Due to the exploratory nature of the research questions this methodology is significant as it gathers rich and detailed information about complex social phenomena.

Data Collection

Data were collected through semi-structured interviews with cybersecurity professionals working in organizations across Pakistan. Semi-structured interviews were selected because they provide flexibility to explore emergent themes while maintaining focus on the research questions (Braun & Clarke, 2006).

A total of 36 interviews were conducted with IT managers, Cybersecurity specialists, Information security officers, Network administrators, Risk management professionals

Sampling Strategy

In this research study purposive sampling method is used to select participants with relevant expertise in cybersecurity and IT management. Participants for interview were selected from organizations operating in sectors such as banking, telecommunications, government agencies, and private enterprises.

Data Analysis

The interviews data were analyzed using thematic analysis, following the methodology proposed by (Braun & Clarke, 2006). For familiarization with the data reading and re-reading interview transcripts were done to become immersed in the content. Initial codes were generated from meaningful data segments. Themes were identified and checked against coded extracts and the entire dataset. Finally, themes were analyzed in relation to research questions and theoretical framework.

Ethical Considerations

In this research study ethical guidelines were followed, and participants were informed about the purpose of the study. Their consent was obtained before conducting interviews.

Confidentiality and Anonymity

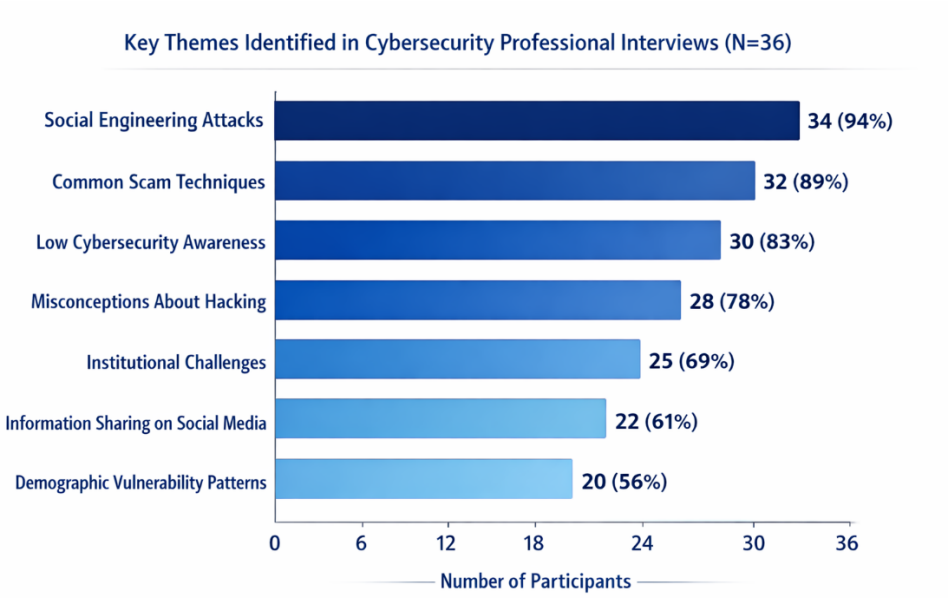
Confidentiality and anonymity of participants maintained by removing identifying information from the research data.

Data Analysis and Findings

This section provides the core evidence of this research study.

Introduction

The purpose of the data analysis is to identify patterns related to social engineering attacks, cybercrime victimization, and cybersecurity awareness. The analysis was conducted using thematic analysis, following the framework developed by (Braun & Clarke, 2006).



Theme 1: Increasing Prevalence of Social Engineering Attacks

The most frequently discussed theme was the increasing prevalence of social engineering attacks targeting individuals and organizations. Participants in the interview indicated that cybercriminals increasingly use psychological manipulation rather than advance technological hacking techniques. This finding is consistent with previous research indicating that social engineering attacks exploit human vulnerabilities rather than system weaknesses (Hadnagy, 2018). These findings align with the argument by (Mitnick & Simon, 2002) that humans represent the weakest link in cybersecurity systems.

Theme 2: Common Social Engineering Tactics

Participants identified several social engineering tactics commonly used by cybercriminals in that include:

- **Impersonation of Bank Representatives:** Cybercriminals pose as a bank official and claim that accounts require verification or have been compromised. Victims are asked to share account details, PINs, or OTP codes.
- **Creating Urgency and Fear:** cyber criminals create scenarios where victims believe immediate action is necessary to prevent financial loss or legal consequences. This urgency call overrides their rational decision-making.
- **Authority Exploitation:** Impersonation of government officials, police officers, or regulatory authorities are used to demand payment or personal information.
- **Emotional Manipulation: cyber criminals ex**ploit personal relationships by taking over messaging accounts and sending urgent requests for financial assistance to friends and family members.

Theme 3: Misconceptions About Hacking

An important theme that was identified during the analysis was the widespread misconception that online fraud always involves hacking. Participants explained that cybercrime victims frequently claim their accounts were hacked when unauthorized transactions occur. However, investigation often reveals that victims voluntarily provided sensitive information to scammers.

This misunderstanding among victims has important implications for cybersecurity awareness. If individuals believe that cybercrime occurs due to sophisticated hacking techniques, they may underestimate the role of their own behavior in occurrence of cybercrime (Krombholz et al., 2015).

Theme 4: Limited Cybersecurity Awareness

Another major theme identified during the interviews was the lack of cybersecurity awareness among internet users. Interview participants revealed that many internet users are unfamiliar with basic security practices such as:

- Protecting passwords and never sharing them
- Avoiding suspicious links in messages and emails
- Verifying unknown communications through official channels
- Understanding that OTPs should never be shared with anyone
- Recognizing common social engineering indicators

It is evident that insufficient digital literacy increases vulnerability to social engineering attacks. Previous studies have similarly found that limited cybersecurity awareness is strongly associated with social engineering attacks (Sheng et al., 2010).

Theme 5: Demographic and Behavioral Vulnerability Patterns

Interview participants identified certain demographic groups and behavioral patterns associated with higher vulnerability to social engineering attacks:

- **Older Adults:** Individuals with limited digital literacy and less experience with online platforms were perceived as more vulnerable to manipulation.
- **Frequent Online Shoppers:** Individuals who regularly conduct online transactions may become desensitized to security warnings or more likely to encounter fraudulent sellers.
- **Active Social Media Users:** Individuals who share extensive personal information online provide attackers with reconnaissance material for crafting convincing impersonation attacks.
- **Highly Trusting Individuals:** People who naturally trust others or have difficulty saying no to authority figures were seen as more susceptible.

Theme 6: Information Sharing on Social Media

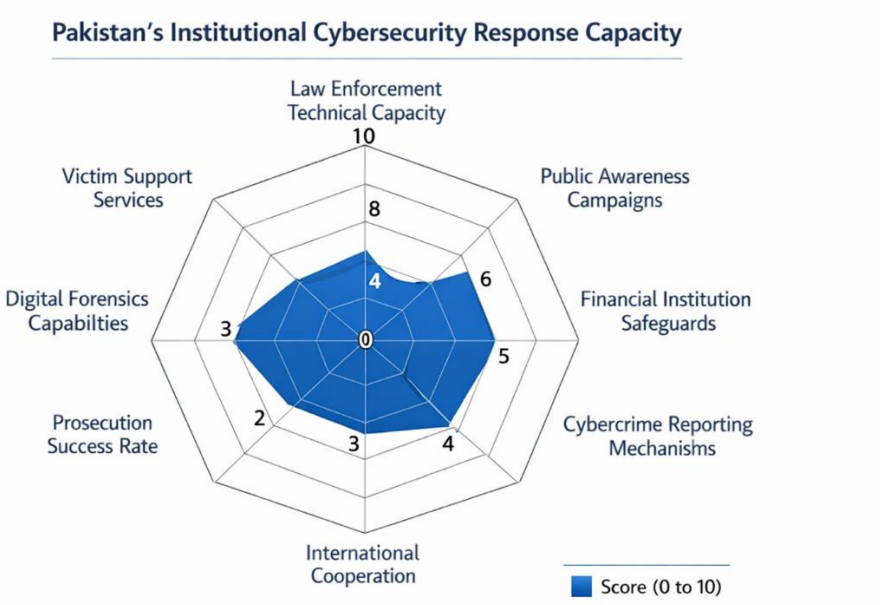
Participants expressed concern about the extent to which individuals share personal information on social media platforms. Information such as phone numbers, email addresses, workplace details, daily routines, and family relationships can be collected by attackers and used to craft convincing impersonation attacks. Such exposure increases the likelihood that individuals may be targeted by cybercriminals (Ahmed & Khan, 2024).

Theme 7: Weak Institutional Response

Participants highlighted several challenges faced by organizations and law enforcement agencies when responding to cybercrime:

- **Limited Cybersecurity Expertise:** Many organizations lack trained cybersecurity professionals who can identify and respond to threats effectively.
- **Lack of Digital Forensic Resources:** Law enforcement agencies often lack the technical tools and expertise required to investigate cybercrime cases thoroughly.
- **Jurisdictional Issues:** Cross-border cybercrime creates legal complexities that hinder investigation and prosecution of international criminal networks.
- **Underreporting of Cyber Incidents:** Many victims do not report incidents due to shame, lack of awareness, or belief that reporting will not lead to resolution.
- **Slow Response Times:** Even when incidents are reported, investigation and resolution processes are often slow, allowing criminals to continue operating.

These findings are consistent with research suggesting that many cybercrime cases remain unresolved due to technical and legal complexities (Wall, 2007).



Theme 8: Organizational Challenges in Cybersecurity

Participants from organizational settings identified additional challenges specific to workplace environments:

- **Employee Training Gaps:** Many organizations provide inadequate cybersecurity training to employees, leaving them vulnerable to business email compromise and other targeted attacks.
- **Bring Your Own Device (BYOD) Risks:** Personal devices used for work purposes may lack adequate security controls, creating vulnerabilities.
- **Third-Party Risks:** Vendors and partners with access to organizational systems may have weaker security practices.
- **Budget Constraints:** Many organizations, particularly smaller ones, lack resources to invest in robust cybersecurity measures.
- **Balancing Security and Usability:** Strict security measures may face resistance from employees who prioritize convenience.

Conclusion and Recommendations

These concluding segments tie together the entire study by finalizing arguments and identifying the next logical steps for research or policy.

Summary of Findings

This research study examined the social engineering attacks and cybercrime victimization in Pakistan, as major urban centers are experiencing rapid digital transformation. Qualitative research design is used for this research study. Semi-structured interviews with 36 cybersecurity professionals were conducted to get comprehensive insights into the tactics used by cybercriminals, the human vulnerabilities, and the role of cybersecurity awareness in preventing cybercrime victimization.

The findings reveal that social engineering attacks like banking verification fraud, messaging account takeovers, investment fraud, and online marketplace scams are the most common forms of cybercrime in Pakistan. Cybercriminals exploit the psychological vulnerabilities of individuals' that include trust in authority, response to urgency, fear of loss, and manipulation of emotions.

It is also significantly noted in the study regarding the widespread misconception among victims who frequently describe their experiences as "hacking" while in reality, they are involved in voluntary disclosure of sensitive information through psychological manipulation. This misunderstanding among victims and authorities has significant implications for cybercrime prevention, as it directs attention toward technological solutions while neglecting the behavioral factors that enable most of the cybercrime.

By applying Routine Activity Theory (Cohen & Felson, 1979) and cybercrime victimology frameworks, the study shows that cybercrime occurs in the presence of motivated offenders, suitable targets, and absent guardianship in cyber environments. That is why the rapid digital expansion in Pakistan has created conditions where these factors increasingly explain the dramatic rise in cybercrime complaints.

Practical Recommendations

Based on the research findings, the following recommendations are proposed:

For Individuals:

- It is important to understand never share passwords, OTPs, or sensitive financial information with anyone, regardless of how legitimate a request may appear.
- Always verify suspicious communications independently through official channels using contact information from official sources
- It is alarming when someone asks for unsolicited information, demanding urgent action, unexpected transfer requests, and offering high returns.
- It is highly risky behaviour to share personal information on social media platforms so think before you share.
- It is advisable to use multi-factor authentication (MFA) for all financial and important accounts.

For Financial Institutions:

- It is a dire need of time to implement robust multi-factor authentication for all transactions.
- It is important to effectively deploy fraud detection systems that monitor transaction patterns and identify suspicious activities.
- Every organization needs to conduct regular customer education campaigns about social engineering tactics.
- Keep clearly communicating that organizational representatives never request for OTPs or passwords from users.
- There must be a rapid response system for fraud incidents.

For Law Enforcement Agencies:

- Government should develop specialized cyber investigation capabilities, including digital forensics expertise with proper scientific available technologies.
- They need to establish international cooperation frameworks for pursuing cross-border cybercriminal networks.
- As cybercrimes are dynamic and emerging it is necessary to provide specialized training for prosecutors and judges on cybercrime matters.
- Authorities should create easy and accessible cybercrime reporting mechanisms that encourage victims to report cybercrime.

For Policymakers:

- It is a dire need of time to integrate cybersecurity education into school and university curricula.
- Funds should be allocated for public awareness campaigns targeting diverse populations.

- There is a huge gap in research regarding cybercrime and academia needs support from policy makers to keep investigating cybercrime trends and prevention effectiveness.
- There must be a mechanism to facilitate public-private partnerships for cybersecurity enhancement in the country.

Limitations and Future Research

This study has limitations that suggest directions for future research.

This study focused on perspectives of cybersecurity professionals rather than victims themselves. Research directly examining victim experiences could provide additional insights.

It is important that future research should evaluate the effectiveness of specific cybersecurity awareness programs in Pakistan.

It is important to conduct longitudinal studies to examine the cybercrime pattern's evolution as digital adoption continues and effectiveness of preventive measures accordingly.

References

1. Ahmed, S., & Khan, M. (2024). Information sharing behavior and privacy risks in Pakistani online communities. *arXiv preprint*. https://arxiv.org/abs/2509.08782
2. Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems, 26*(6).
3. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2).
4. Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.
5. Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.). Pearson Education.
6. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4).
7. Cross, C. (2018). Victims' motivations for reporting to the 'truecaller' anti-scam initiative. *Journal of Criminological Research, Policy and Practice, 4*(1).
8. Daily Pakistan English News. (2025, September 3). *Online fraud in Pakistan reaches Rs3 billion, NCCIA tells lawmakers*. https://en.dailypakistan.com.pk/03-Sep-2025/online-fraud-in-pakistan-reaches-rs3-billion-nccia-tells-lawmakers
9. Furnell, S. (2021). Categorising cybercrime and cybercriminals: The problem and how it has changed. *Journal of Information Warfare, 20*(4).
10. Furnell, S., & Moore, L. (2014). Security literacy: Identifying the gaps. *Computer Fraud & Security, 2014*(10).
11. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
12. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications,* https://doi.org/10.1016/j.jisa.2014.09.005
13. Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.
14. MM News. (2024). *One in two Pakistanis faced online frauds in 2024, survey reveals*. https://mmnews.tv/one-in-two-pakistanis-faced-online-frauds-in-2024-survey-reveals/
15. National Cyber Crime Investigation Agency. (2025). *Cybercrime trends in Pakistan: Annual report 2025*. Government of Pakistan.
16. Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. In *Research Anthology on Artificial Intelligence Applications in Security*. IGI Global.

17. Profit by Pakistan Today. (2025). *NCCIA busts $60 million crypto and forex scam, arrests 15 foreign nationals in Karachi*. https://profit.pakistantoday.com.pk/2025/12/26/nccia-busts-60-million-crypto-and-forex-scam-arrests-15-foreign-nationals-in-karachi/

18. Profit by Pakistan Today. (2025b). *Cybercrime agency registers over 50,000 complaints, 690 arrested in four months*. https://profit.pakistantoday.com.pk/2025/07/25/cyber-crime-agency-registers-over-50000-complaints-690-arrested-in-four-months/

19. Profit by Pakistan Today. (2026). *NCCIA received over 150,000 complaints last year, including 81,000 linked to financial fraud, NA told*. https://profit.pakistantoday.com.pk/2026/01/17/nccia-received-over-150000-complaints-last-year-including-81000-linked-to-financial-fraud-na-told/

20. ProPakistani. (2023). *There is no solution for banking finance frauds in Pakistan: NTISB*. https://propakistani.pk/2023/09/04/there-is-no-solution-for-banking-finance-frauds-in-pakistan-ntisb/

21. Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2).

22. Shah, A., Hussain, S., & Ahmed, Z. (2024). Phishing susceptibility in Pakistan: Demographic and behavioral factors. *arXiv preprint*. https://arxiv.org/abs/2510.09249

23. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

24. UrduPoint. (2026). *Over 150,000 cybercrime complaints reported in Pakistan in 2025*. https://www.urdupoint.com/en/pakistan/over-150000-cybercrime-complaints-reported-i-2119756.html

25. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

26. Wang, Z., Sun, L., & Zhu, H. (2021). Defining social engineering in cybersecurity. *IEEE Access, 9*.

27. Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72*.

28. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications