GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

THE PSYCHOLOGY OF CYBER FRAUD: UNRAVELING THE TACTICS BEHIND MODERN-DAY SCAMS

Purnima Nagar

Assistant Professor, Department of Psychology, Daulat Ram College, Delhi University
Email id - nagarpurnima08@gmail.com

Abstract

In the backdrop of Digital India, where rising internet penetration has transformed financial transactions and communication, cyber fraud and online scams have emerged as widespread risks. Technology, both a friend and a foe, facilitates smooth digital exchanges and financial inclusion, but it also provides cybercriminals with advanced tools to exploit human weaknesses. The Victim-Perpetrator Interaction Model presented here offers a comprehensive understanding of cybercrime by analyzing the interactions among victim vulnerabilities, perpetrator tactics, and communication channels that enable deception. Unlike earlier research that examined either victim susceptibility or perpetrator psychology in isolation, this model integrates both perspectives to explain scam compliance. The study also highlights the role of psychological tricks, cognitive biases, and emotional manipulation in cybercrime. By addressing a gap in literature, this research enhances awareness of cyber threats. Future empirical testing of this model can improve scam detection techniques and develop more effective interventions to protect individuals from online deception.

Keywords: *Cybercrime, Psychological manipulation, Scam Compliance, Social Engineering*

"Technology is both a tool for helping humans and for destroying them. This is the paradox of our times which we were compelled to face."

— Frank Herbert (1969)

The 21st century, digital revolution and easy access to the internet has brought many breakthrough innovations. With such creative advancements facilitated by web 3.0 and "Digital India", we are also susceptible to modern day, ingenious cybercrimes. Everyday we hear new crimes that happen online or innovative ways to carry out online frauds that leave everyone appalled with creative storylines that can convince anyone.

Cybercrimes according to Halder and Jaishankar (2016) refer to "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)."

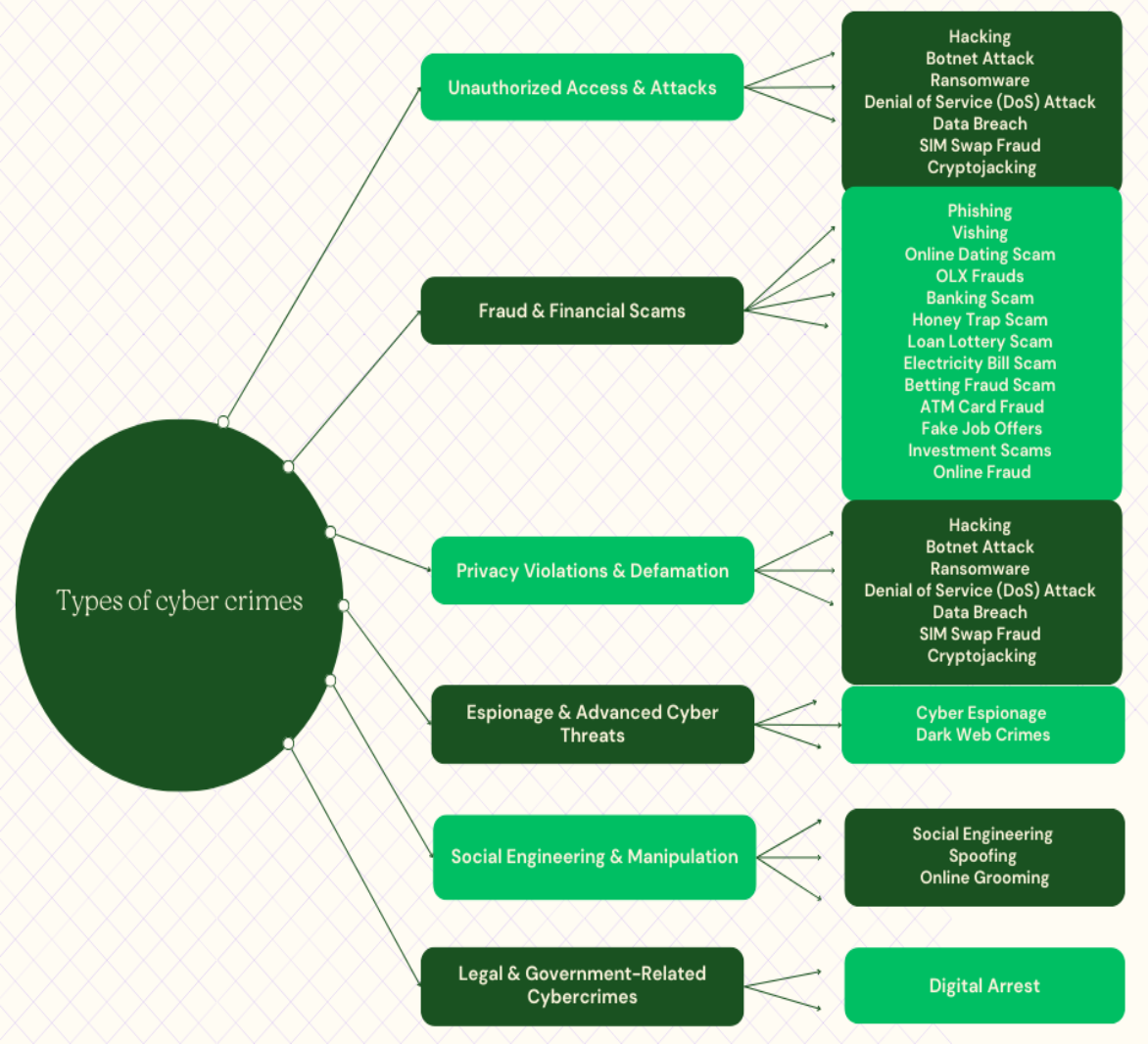
Additionally, according to Tripathy (2024), "Cybercrime refers to unlawful activities carried out through or targeting digital infrastructures, with information systems functioning as either the instrument or the victim of these offenses."

India has seen a sharp increase in the number of cyber crime cases in the last decade. The rapid digital adoption in India has been accompanied by corresponding cyber threats by individual hackers as well as sophisticated organized crime rings. In 2014, there were 9,622 cybercrime cases. This number witnessed a dramatic surge by the end of 2024 with the Indian Cyber Crime Coordination Centre (I4C) reporting over 12 Lakh cyber fraud complaints. Small cities have emerged as scam capitals and cyber crime hotspots. With an increase in the adoption of digital banking systems and cheap internet access, cyber crime has seen a 900% rise.

Modern day cyber crimes are idiosyncratic in nature. The various types can be briefly divided into 6 categories - Unauthorized access & attacks, fraud & financial scams, privacy violations & defamation, espionage & advanced cyber threats, social engineering & manipulation, legal & government related cybercrimes.

Figure 1
Types of cyber crimes

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.



Interestingly, all of these crimes make use of highly sophisticated psychological tactics, wherein the perpetrators exploit human vulnerabilities and lure the victims. It is imperative to understand the psychology behind these modern day cyber crimes so that there is an increased level of awareness as well as development of prevention programmes.

Existing literature focusing on the psychology of cybercrime predominantly sheds light on isolated aspects of the perpetrator-victim dynamic. A significant portion of research focuses on the personality traits of perpetrators (Osipyan, 2024) and victims (Van de Weijer & Leukfeldt 2017), exploring factors such as lack of empathy, sensation seeking, impulsivity or psychopathic tendencies (Seigfried-Spellar et al., 2017). Additionally, studies that examined psychological techniques used by the perpetrators - such as urgency creation, authority exploitation, and social engineering (Ferreira and Lenzini, 2015) are well documented. There exists a noticeable gap in research that offers a holistic understanding of how these tactics interact in real-world cyber fraud scenarios. Current studies analyze these factors in isolation rather than as part of an interconnected system that shapes scam compliance.

Therefore, to bridge this gap, this paper proposes a comprehensive model that explains the interaction between perpetrators of cybercrimes and their victims, focusing on the psychological mechanisms that drive scam compliance. The model integrates three components: the perpetrator's manipulation tactics, victim vulnerabilities, and the communication channels through which scams are executed. This paper offers a structured framework that explains how perpetrators exploit emotional triggers and cognitive biases to influence victims' decision-making.

REVIEW OF LITERATURE

Tripathy (2024) carried out a comprehensive survey on cybercrimes in India over the last decade and his analysis of reported fraud cases across different categories from 2014 to 2024 revealed a substantial increase in financial fraud, phishing attacks, identity theft, online harassment and ransomware incidents. He also shed light

on the shifting landscape of cybercrime, which has wider societal ramifications ranging from emotional distress to financial losses for victims.

Cheque fraud and wire fraud which were identified as "traditional financial scams" have now transitioned to the cyber space wherein perpetrators now leverage anonymity, automation and global connectivity to lure victims (Kapure, 2025). Cybercriminals now infiltrate financial systems with sophisticated attacks as they have switched from physical to digital transactions.

The primary tools used by cybercriminals to steal financial assets and sensitive data with minimal risk include social engineering tactics, malware attacks, and phishing scams. Additionally, one of the most lucrative forms of cybercrime is ransomware, which has increased multifold in recent years. In such attacks, fraudsters demand cryptocurrency payments in exchange for unlocking encrypted files. (Kapure, 2025)

The shifting nature of online crimes can be understood from a psychological lens wherein these perpetrators make use of various tactics to deceive victims such as principles of persuasion like authority, reciprocity, commitment and scarcity. Bundala (2024) highlighted how psychological tricks often supersede technical tricks to lure victims. Psychological tactics such as emotional manipulation, trust through love and divinity, involvement of trusted religious leaders, urgency, and direct solicitation of personal information often precede technical methods, such as downloads or phishing links.

With respect to frauds and scams, three taxonomies are often referred to in literature: Cialdini's principles of influence, Gragg's psychological triggers, and Stajano et al. principles of scams. Ferreira and Lenzini (2015) compared these three theories above and proposed five core principles called 'Principles of persuasion in social engineering (PPSE). Ferreira and Lenzini's principles take into consideration persuasion, scam/deception and the psychology of social engineering. These five principles include *Authority* (AUTH), *Social Proof* (SP), *Liking, Similarity & Deception* (LSD), *Commitment, Reciprocation & Consistency* (CRC), and *Distraction* (DIS). In simple terms, victims tend to follow authority figures without questioning, imitate the behavior of the majority, and are influenced by those they perceive as similar to or likable. Once they commit to a decision, they are likely to stick to it to maintain consistency and feel obligated to reciprocate favors. Lastly, distractions cause individuals to overlook important cues while focusing on the immediate gratification of their needs.

Furthermore, cognitive biases such as optimism bias, cognitive overload, and loss aversion, along with emotional triggers like desperation and greed, play a significant role in victimization by perpetrators. Montanez et. al. (2020) highlighted that cognitive workload, stress, and attack effort increase one's vulnerability to social engineering cyberattacks. Additionally, cognitive biases, such as the authority effect, trust effect, and confirmation bias, significantly influence decision-making in cyber fraud. These biases shape individuals' choices and actions, highlighting the interplay between cognitive mechanisms and the socio-cultural environment in cyber fraud practices (Vasilkova, 2024). It is also important to note that victims' psychological states (stress and exhaustion) make them more susceptible to cybercrime. These psychological states often lead to cognitive errors and decision making biases.

METHOD

This article adopts an analytical and descriptive approach to examine the psychological tactics underlying cyber fraud. By synthesizing research from criminology and psychology, it constructs a conceptual framework that holistically explains how perpetrators manipulate victims into scam compliance. Using databases including PsycINFO, Scopus, and Google Scholar, a systematic literature search was conducted. Studies from 2000 to 2025 that looked at behavioral patterns, communication tactics, or psychological mechanisms in online fraud were included. Following careful review of literature, three main themes emerged: communication channels (such as phishing emails, fake websites, and social media), victim vulnerabilities (such as impulsivity, loneliness, and low digital literacy), and perpetrator tactics (such as emotional manipulation, persuasion techniques). Their interaction shapes the victim's situational and psychological condition, which in turn affects how likely they are to comply with the fraud. The model provides a nuanced understanding of how communication dynamics and personal psychological characteristics combine to enable online fraud.

RESULTS

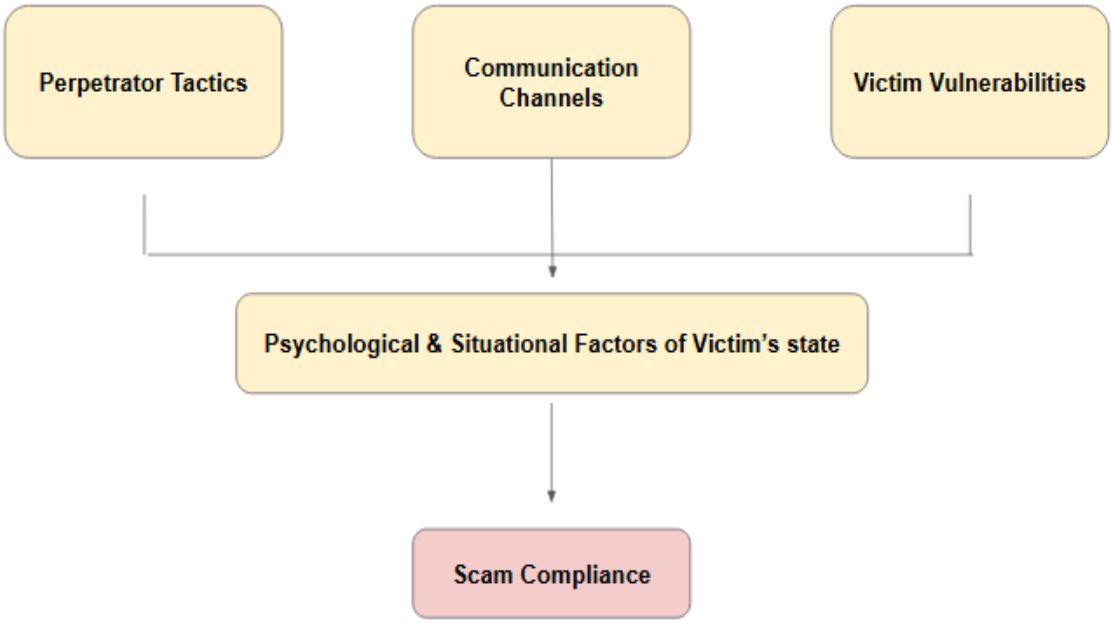
Through a comprehensive review of existing literature to address gaps in research, this paper introduces the **Victim-Perpetrator Interaction Model**. This model offers a holistic explanation of the relationship between perpetrators and victims, emphasizing the crucial role of communication channels in the deception process. It also highlights the manipulation strategies used by perpetrators against the backdrop of existing psychological vulnerabilities of the victims.

The model posits that the perpetrator's persuasion tactics shape the communication style, which in turn influences the victim's cognitive state, ultimately leading to scam compliance.

Figure 2

Victim-Perpetrator Interaction Model

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.



The perpetrators of cybercrimes make use of psychological tactics as well as persuasion techniques to lure the victims. These techniques can be broadly divided into six types i.e., *compliance and commitment*, *cognitive trickery*, *emotional manipulation*, *scarcity and urgency*, *deceptive legitimacy*, *politeness and formality*.

Table 1

Perpetrator Factors

Psychological Tactic	**Specific Techniques**	**Analysis**
Compliance & Commitment	• Small steps • 'Foot in the door' technique • Reciprocity • Gradual Escalation • Sunk Cost Fallacy • Forced Choice Strategy	Before moving on to more significant requests, offenders first establish compliance with little, ostensibly innocuous requests. Because they feel they have no other option (forced choice method) or because of past commitments (sunk cost fallacy), victims feel pressured to continue.
Cognitive trickery	• Information overload • Illusions of control • Misleading Statistics • Confusing Jargon	In order to cause cognitive fatigue, scammers bombard victims with too much or inaccurate information. By creating the illusion of credibility through the use of technical jargon or fabricated figures, they increase the likelihood that victims will cooperate without question.
Emotional manipulation	• Use of emotional triggers • Use of attraction/excitement • Guilt-Tripping • Fear Appeals • Creating a Sense of Exclusivity	Fraudsters exploit emotions such as love, fear or greed to cloud rational judgment. By instilling hope for a future relationship, romance scammers foster strong emotional attachments; other scammers employ fear techniques, such as threats of legal action, to coerce cooperation.
Scarcity & Urgency	• Limited time offers • Making victim believe its a unique opportunity • Fake Urgency Notifications • Countdown Timers • Fake High Demand	Victims are persuaded they must take rapid action or risk missing a unique opportunity, which forces them to make snap judgments. Countdown timers and claims of high demand are two strategies that take advantage of FOMO and cause victims to behave impulsively.

	• Fear of Missing Out (FOMO)	
Deceptive Legitimacy	• Authority symbols • Personal approach • Social Engineering • Fake Testimonials • Mimicking Official Documents • Deepfake Technology	Cybercriminals increase their perceived legitimacy by impersonating trusted figures (e.g., banks, officials) or using testimonials and forged documents. Deception is made even more convincing with technology like deepfake.
Politeness & Formality	• Establishing rapport • Capitalization of trust • Professional Language • Mimicking Customer Support • Personalized Messages	Scammers build trust through formality and politeness, making their requests seem legitimate. They enhance credibility and lower skepticism by using personalized greetings or mimicing official customer support.

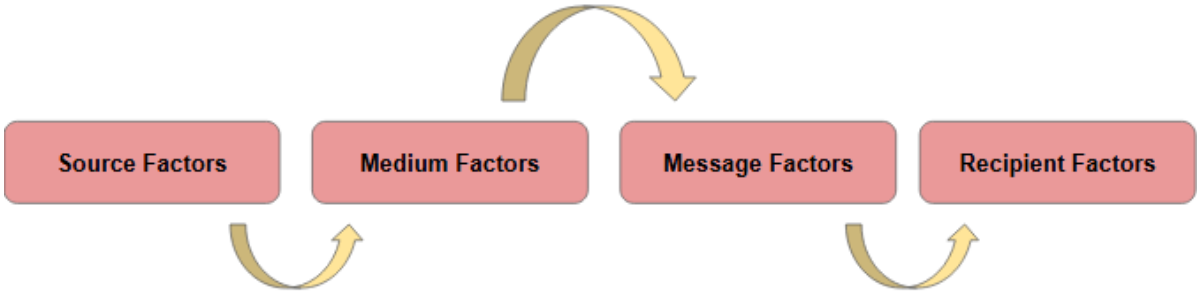
As seen by numerous contemporary scams, cybercriminals employ a variety of psychological strategies to trick and influence victims. The **Digital Arrest Scam** is a well-known example, in which criminals use video calls enhanced with deepfake technology to pose as law enforcement officers. Victims are coerced into obeying by the threat of legal repercussions after seeing what looks to be a real officer in uniform, frequently holding official-looking identification documents. By imitating authority figures, this fraud takes advantage of **deceptive legitimacy**, and **compliance and commitment** strategies compel victims to blindly follow directions. In similar fashion, **banking scams** exploit victims by impersonating bank employees who convincingly provide personal information, including account numbers, in order to gain confidence. After claiming that the victim's account has been compromised, scammers demand that they take quick action, forcing them to share OTPs or move funds to a "secure" account. This tactic uses **scarcity and urgency** to create a false sense of crisis and **cognitive manipulation** to create an illusion of control. **Romance fraud** is another common scam in which scammers create strong emotional bonds with their victims online and use their desire for a relationship and feelings of attraction to control them. Using **emotional manipulation** techniques like guilt-tripping and fear appeals, victims are later forced into giving money because they think they have discovered a reliable companion. Lastly, **investment scams** use false urgency, exaggerated data, and fabricated testimonials to pressure victims into making rash financial decisions by promising large financial returns. These frauds profit on **deceptive legitimacy** (false success stories, social engineering) and **scarcity and urgency** (limited-time offers, FOMO). The success of these manipulation techniques in contemporary digital fraud schemes is demonstrated by the way hackers consistently take advantage of human psychology to boost scam compliance in all of these scenarios.

Interestingly, scammers are also capitalizing on the **fear of being scammed** to exploit potential targets. As public awareness about various cybercrimes increases, many people have become more cautious and alert. Paradoxically, scammers are using this heightened awareness against them. In scams like the **digital arrest scam**, they instill panic by falsely claiming that the victim's identity has already been stolen or that they are involved in some illegal activity. By convincing the individual that they have already fallen victim to fraud, scammers coerce them into compliance—often under the guise of helping them resolve the issue. They **turn a protective instinct into a vulnerability** by exploiting the fear of fraud.

The **communication channel** is the **second essential element** and the center of this model. Perpetrators successfully deceive their victims by using extremely complex and convincing communication. Thus, a more thorough analysis of these channels is essential to comprehending how this manipulation takes place and how victims are swayed.

Figure 3
Communication Channel

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.



The **source of communication**—the perpetrator—leverages *signs of authority* and status symbols to establish compliance. They build credibility by displaying familiarity with personal facts like the victim's name or bank account information, and they take advantage of reputation by posing as reliable people, such as a police officer or bank representative. The victim is compelled to participate because of the sense of accountability or curiosity this familiarity fosters. Furthermore, the perpetrator uses consistency in their communication to reinforce persuasion, and *trust signals* function as indicators of legitimacy.

Medium factors focus on the *method of communication* and *interaction style*. To reach their victims, scammers employ social media, phone calls, emails, and phony websites. Their direct and professional communication style frequently instills a sense of urgency while also overwhelming the victim with too much information, which hinders their ability to make logical decisions.

Message factors relate to the *content* and *tone* of the communication. In order to lure victims, perpetrators design communications that mostly rely on emotional appeals, scarcity cues, and perceived rewards. In order to reduce doubt and promote prompt cooperation, the tone is usually urgent, courteous, official, or authoritative.

The chance of scam compliance is ultimately determined by **recipient factors**. It is important to consider the *victim's cognitive state* because scams work best when the victim is distracted, has poor awareness, or is easily manipulated. Furthermore, the victim is more likely to be persuaded if they have trust in the source, which raises the likelihood that they will fall for the scam.

This model's **last section** looks at **victim vulnerabilities**, which are influenced by the communication channel mentioned above as well as the perpetrator's strategies. These elements include *situational variables* as well as *psychological characteristics* that eventually raise the probability of scam compliance.

Table 2
Victim Vulnerabilities

Victim Factors	Subtypes	Analysis
Psychological Traits & vulnerabilities		
Emotional triggers	• Greed • Desperation • Companionship • Fear • Guilt • Hope for a better future	Perpetrators exploit emotions such as hope (e.g., lottery scams), guilt (e.g., fake charity scams), and fear (e.g., threats of arrest or account closure) to manipulate victims.
Cognitive errors	• Cognitive overload • Optimism bias • Overconfidence • Attentional blindness	Overwhelming information is difficult for victims to handle, which can result in mental shortcuts, misplaced confidence, or a failure to recognize warning signs.
Decision making biases	• Loss aversion • Errors in judgment • Commitment bias • Sunk cost fallacy	Due to previous investments (money, time, and emotional commitment), victims may persist in falling for scams, making them difficult to leave even when anything seems fishy.
Situational Influences		

State of Mind	• Stress • Distraction • Exhaustion • Loneliness • Urgency	Victims who are under time constraint or experiencing elevated emotions are more prone to act on impulse without checking facts.
Window of Tolerance	• Impact of emotional state on decision-making • Trust disposition	A victim's natural inclination to trust brands, authority figures or official-looking messages makes them more vulnerable to deception.

Modern-day cybercrimes heavily rely on victim vulnerabilities, as offenders use psychological characteristics and contextual factors to control their victims.

Ponzi schemes and investment frauds, for example, exploit victims' **greed and hope for financial gain** by offering irrationally high returns in an attempt to persuade them to make huge investments. **Fear and urgency** are frequently employed in digital arrest scams, in which con artists pose as law enforcement officers and threaten victims with legal repercussions if they do not comply right away. Additionally, a major contributing element to banking scams is **cognitive overload**, where con artists overwhelm victims with complex financial jargon and formal-sounding processes, impairing their ability to critically evaluate information. Another contemporary cybercrime i.e., online romance scams exhibit **commitment bias** and the **sunk cost fallacy**, wherein victims keep sending money to scammers because they feel they have already emotionally committed too much to withdraw. In similar fashion, victims of phishing scams frequently respond hurriedly to emails or messages claiming their bank account has been seized without checking the sender's legitimacy because they are **stressed or exhausted**. Cybercriminals use fictitious dating profiles or social media friendships to pursue people, giving them a false sense of companionship before taking advantage of them financially. Examples from the real world demonstrate how situational and psychological vulnerabilities greatly raise the probability of scam compliance.

As a result, the **Victim-Perpetrator Interaction Model** provides a structured perspective on how cybercriminals use communication techniques and psychological vulnerabilities to control victims. The model emphasizes the underlying mechanisms that result in scam compliance by demonstrating the interaction between victim susceptibilities, the communication medium, and perpetrator techniques. It highlights how crucial it is to identify these deceptive patterns, not just for individuals but also for institutions and legislators looking to improve fraud prevention measures.

DISCUSSION

The **Victim-Perpetrator Interaction Model** offers a methodical way to comprehend the communication and psychological processes that underlie cybercrime. The model reveals important elements that influence scam compliance by highlighting the interaction between victim vulnerabilities, communication routes, and perpetrator methods. This has important ramifications for victim support, fraud prevention, and cybersecurity initiatives. These findings can be used by law enforcement and financial institutions to improve scam detection methods, pinpoint high-risk individuals, and customize interventions to thwart fraudulent schemes. Additionally, educational programs can be created to increase public knowledge of the psychological strategies employed by cybercriminals, giving potential victims the cognitive abilities they need to spot and resist manipulation. The model's insights can also be used to improve technology-based solutions, such as behavioral analysis tools and AI-driven fraud detection algorithms, to spot deceptive trends and reduce risks instantly.

This model expands and develops upon the psychological ideas of social engineering, trust, and persuasion that are currently in use. Frameworks like **social engineering models** and **Cialdini's Principles of Influence** describe how people might be convinced to agree with false requests, but they frequently concentrate on specific strategies alone. However, by combining these strategies with victim vulnerabilities and communication channels, the **Victim-Perpetrator Interaction Model** offers a more thorough perspective. Furthermore, this model provides a comprehensive knowledge of cyber fraud mechanisms by capturing the dynamic interaction between victim vulnerability and perpetrator intent, which are the two main topics of traditional fraud models. The model provides a more sophisticated framework for examining and thwarting online frauds by bridging this gap and advancing current psychological and criminological studies. Future studies could empirically test its elements, improving methods for shielding people from online fraud.

LIMITATIONS OF THE MODEL

The lack of empirical testing of this model is a major drawback. Past research and case studies have suggested the relationships between perpetrator tactics, communication channels, and victim vulnerabilities; however,

experimental studies, victim surveys, or law enforcement data are required to validate these relationships in the real world and determine their predictive accuracy and practicality.

Additionally, the model makes the assumption that every instance of cyber fraud follows a predetermined procedure, although in practice, scams can differ greatly depending on the situation, cultural norms, and technology developments. Given the dynamic nature of cybercrime and the fact that offenders are always changing their strategies, the model might require ongoing improvement in order to be applicable. Furthermore, the existing approach may not adequately account for the diversity introduced by individual differences in victim susceptibility, such as personality factors, prior experiences, and digital literacy. Notwithstanding these drawbacks, this model is a valuable place to start for future studies and can direct empirical inquiries meant to strengthen victim resilience and fraud prevention tactics.

CONCLUSION

This study introduces the Victim-Perpetrator Interaction Model as a thorough framework for comprehending how scams operate and emphasizes the psychological dynamics that underlie cyber fraud. The model offers an organized method for examining cybercriminal methods and their psychological effects on victims by combining perpetrator tactics, communication channels, and victim vulnerabilities. It emphasizes how cognitive biases, emotional manipulation, and persuasion strategies all contribute to scam compliance. Although the model provides insightful information, in order to improve its applicability, future research should concentrate on empirical validation through case studies, victim surveys, and experimental studies. Furthermore, investigating the ways in which various demographics, cultural settings, and changing technology environments impact scam susceptibility can improve our comprehension of cyber fraud. Reducing the risks presented by cybercriminals still requires stepping up efforts to prevent fraud through policy changes, awareness campaigns, and technological safeguards.

REFERENCES

[1] Bundala, N. (2024). Understanding cybercrime modus operandi: Techniques, psychological tricks, and countermeasures. *Asian Journal of Research in Computer Science, 17(12), 234–251*. https://doi.org/10.9734/ajrcos/2024/v17i12541

[2] Ferreira, A., & Lenzini, G. (2015). An analysis of social engineering principles in effective phishing. In *Proceedings of the 2015 IEEE Security and Trust for Applications (STAST)*. https://doi.org/10.1109/STAST.2015.10

[3] Halder, D., & Jaishankar, K. (2016). *Cyber crimes against women in India*. SAGE Publications India.

[4] Lemay, A., & Leblanc, S. (2018). Cognitive biases in cyber decision-making. *Journal of Cyber Security Technology, 2*(1), 1–15. https://doi.org/10.1080/23742917.2017.1413732

[5] Montanez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology, 11, 1755.* https://doi.org/10.3389/fpsyg.2020.01755

[6] Osipyan, Natalia. (2024). On the Issue of Taking into Account the Psychological Characteristics of a Cybercriminal's Personality for the Purposes of Preventive Activities. *Victimology. 11. 425-433.* https://doi.org/10.47475/2411-0590-2024-11-3-425-433.

[7] Sani, K., & Kapure, A. (2025). Data privacy in the age of FinTech: Navigating regulatory frameworks and compliance challenges. https://doi.org/10.13140/RG.2.2.33541.87528

[8] Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice, 51, 67–73.* https://doi.org/10.1016/j.jcrimjus.2017.06.003

[9] Tripathy, Sudhanshu. (2024). A comprehensive survey of cybercrimes in India over the last decade. *International Journal of Science and Research Archive.* 13. 2360-2374. https://doi.org/10.30574/ijsra.2024.13.1.1919.

[10] Van de Weijer, Steve & Leukfeldt, Eric. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking. 20.* https://doi.org/10.1089/cyber.2017.0028.

[11] Vasilkova, V. (2024). Cognitive biases in cyber fraud practices: The heuristic potential of M. Norton's theory. *Zhurnal Sotsiologii i Sotsialnoy Antropologii (The Journal of Sociology and Social Anthropology)*. https://doi.org/10.31119/jssa.2024.27.4.7