Scientific and Social Research, 2025, Volume 7, Issue 7
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Why Would People Fall Victim to Scams? Psychological Manipulation Behind Telecom and Online Scams

Zhenwang Xie*

Tourism College of Zhejiang, Hangzhou 311231, Zhejiang, China

**Author to whom correspondence should be addressed.*

Abstract: Telecom and online scams pose a global challenge. Despite intensified crackdowns worldwide, emerging technologies like AI have spawned novel tactics that threaten public safety. Grounded in multidisciplinary theoretical frameworks, this study analyzes victims' susceptibility profiles across cognitive, behavioral, emotional, needs-based, and personality dimensions, demonstrating that vulnerability transcends specific demographics. The paper deconstructs how scammers exploit universal human weaknesses through stage-based psychological manipulation tactics. Finally, the study proposes public self-protection strategies: enhancing cognitive awareness (knowledge reserves), strengthening needs management, and building psychological resilience (inner fortitude) to identify and resist scams, thereby mitigating losses.

Keywords: Telecom and online scams; Psychological susceptibility profiles; Psychological manipulation; Countermeasures

Online publication: August 12, 2025

1. Introduction

Telecom and online scams have evolved into a global challenge, inflicting annual losses exceeding $3 trillion USD worldwide. While intensified crackdowns by governments—notably the dismantling of scam syndicates in Southeast Asia, particularly those operating in Myanmar's Shan State and Myawaddy—have effectively curbed the escalation of such crimes, telecom fraud persists at alarming levels. Criminals now leverage AI and blockchain technologies to innovate tactics, deploying sophisticated schemes like deepfake voice and video manipulation that prove exceptionally difficult to detect. More alarmingly, these crimes have converged with violent offenses, as evidenced by high-profile cases including the murder of a Chinese pharmaceutical executive following kidnapping in the Philippines and the abduction of actor Wang Xing. These developments pose severe threats to citizens' lives and property security across nations.

Through multi-agency governance involving governmental, judicial, financial, and cyber-regulatory bodies alongside industry stakeholders, significant progress has been achieved in combating telecom scams. However, systemic breakdowns in early warning mechanisms and regulatory disorder persist [1]. Paradoxically, despite saturation-level public anti-scam campaigns, substantial numbers of victims continue to fall for seemingly transparent schemes. This raises critical questions: Do these victims share common susceptibility traits—creating an “ideal victim profile” characterized by inexperience, financial distress, greed, vanity, or credulity? Yet empirical evidence reveals victims include accomplished academics, renowned entrepreneurs, and public figures possessing abundant life experience, professional success, and demonstrable prudence—directly contradicting stereotypical victim archetypes. This suggests telecom scams are neither exclusive to specific demographics nor random opportunism, but rather precision-targeted operations exploiting universal human vulnerabilities. Consequently, does this imply every individual constitutes a potential victim?

Addressing these questions holds dual significance: academically, it advances scholarly understanding of telecom scam dynamics; practically, it resolves systemic gaps in prevention mechanisms by centering on victim psychology, thereby enhancing governance efficacy. This study systematically categorizes victims’ psychological profiles and deciphers the underlying psychological manipulation apparatus, investigating whether heterogeneous susceptibility traits heighten vulnerability to specific scam types. Building upon this analysis, we propose actionable countermeasures to strengthen societal resilience.

2. Psychological susceptibility profiles of telecom scam victims

2.1. Theoretical underpinnings of susceptibility profiles

One perspective posits that victims exhibit heterogeneous traits, heightening their susceptibility to telecom scams. Theoretical underpinnings include Lifestyle Exposure Theory, Routine Activity Theory, Victim Precipitation Theory, Vulnerability Theory, and Self-Control Theory [2].

Lifestyle Exposure Theory posits that high-risk lifestyles and behaviors increase individuals’ susceptibility to telecom scams. For instance, oversharing sensitive information—such as contact details and personal interests—on social media heightens targeting risks by scammers.

Routine Activity Theory identifies three prerequisites for crime: motivated offenders, suitable targets, and absence of capable guardians. Victims with inadequate social experience, poor cybersecurity awareness, and risk complacency often embody these “suitable targets.”

Victim Precipitation and Vulnerability Theories elucidate why certain individuals face disproportionate targeting. Specific socioeconomic, psychological, and behavioral traits—including economic precarity or cognitive biases—amplify victimization likelihood.

2.2. Empirical evidence on psychological susceptibility profiles

Empirical studies lend robust support to this perspective, validating the existence of distinct susceptibility profiles among telecom scam victims. For instance, research on recurrent victimization among the elderly reveals that prior scam experiences fail to significantly alter behavioral patterns or lifestyles, thus validating the “heterogeneous susceptibility” mechanism. From psychological vantage points, researchers have dissected victims’ characteristic desire-driven needs, emotional vulnerabilities, and decision-making traits. These investigations—targeting cohorts like university students and seniors—have mapped vulnerability indicators and devised specialized assessment instruments [3–4].

Concretely, these victims consistently exhibit marked characteristics across five dimensions: cognitive, behavioral, emotional, needs-based, and personality facets [5].

2.3. Psychological susceptibility profiles of scam victims

2.3.1. Cognitive susceptibility markers

Schema limitations: Victims demonstrate superficial information processing, uncritically accepting fraudulent claims and forming erroneous judgments.

Heightened suggestibility: Susceptible to psychological control through persuasive scripts, fostering unwarranted trust.

Knowledge/Awareness deficits: Inadequate anti-scam literacy; insufficient; cybersecurity consciousness; excessive curiosity exploitation.

2.3.2. Behavioral susceptibility markers

Pathological credulity: Over-trust during relationship-building phases, enabling entrapment.

Speculative escalation: Initial "test investments" progressing to catastrophic losses under criminal inducement.

Decision impulsivity: Action without deliberation or consequence analysis.

Loss-chasing paradox: Pursuing recovery through further engagement despite scam recognition (sunk cost fallacy manifestation).

Help-seeking avoidance: Withholding reports due to shame/fear, missing critical intervention windows (<10 min optimal timeframe).

2.3.3. Emotional susceptibility triggers

Pathological dependency: Victims develop excessive reliance on scammers post-bonding, exhibiting unquestioning compliance.

Manipulated euphoria: False empathy and fictitious gains reporting induce pleasure, critically lowering vigilance.

Engineered panic: Irrational responses to fabricated emergencies, disabling rational cognition.

Exploited anxiety: Urgency-driven acceptance of criminal "solutions" without verification.

Shame-driven isolation: Post-victimization withdrawal due to social stigma, entrenching helplessness.

2.4. Needs-based exploitation vectors

How criminals leverage universal human needs for criminal targeting is shown in **Table 1**.

Table 1. Leveraging universal human needs for criminal targeting

Core need	Exploitation mechanism	Primary targets	Scam archetypes
Physiological	Sexual gratification exploitation	Adolescents/Young adults	Sextortion, "Escort" fraud
Economic	False empowerment illusions	Financially strained	Fake jobs, Investment traps
Security	Authority trust exploitation	Crisis-experiencing	Impersonation scams (e.g., "Police" scams)
Social Belonging	Emotional vacancy targeting	Loneliness-suffering	Romance scams, Friendship fraud
Esteem	Fictitious community bonding	Socially isolated	Cult-like recruitment scams
Self-Actualization	Achievement desire weaponization	Career-ambitious	"Get-rich-quick" scams

2.5. Personality-based susceptibility markers

Empirical evidence confirms low self-control as a critical predictor of scam vulnerability [6]. Individuals exhibiting this trait demonstrate:

Impulsivity: Action without deliberation

Risk-seeking propensity: Heightened reward sensitivity

Immediate gratification preference: Temporal discounting anomalies

Future insensitivity: Defective long-term planning

Empathy deficits: Impaired perspective-taking

Additional vulnerability markers include: Agency Deficits; Volitional Weakness; Naivety Spectrum; Avoidance Coping; Toxic Optimism.

On one hand, researchers leverage these susceptibility profiles to develop risk prevention models aimed at identifying, intervening in, and preventing telecom and online scams [7–8]. On the other hand, excessive focus on susceptibility traits reinforces stereotypes, stigmatizes victims, and diminishes public vigilance ("I'm too smart to fall for this"). The public tends to partially attribute blame to victims' behaviors or characteristics rather than wholly condemning the criminal acts themselves. This explains why victimization persists despite widespread awareness campaigns. Simultaneously, victims' fear of secondary harm reduces help-seeking willingness, emboldening perpetrators and objectively facilitating their evasion of legal consequences.

3. Psychological manipulation mechanisms in telecom and online scams

An alternative perspective posits that telecom scams predominantly exploit universal human vulnerabilities rather than individual-specific traits. Victims' responses reflect fundamental psychological patterns—empathy, sunk cost fallacy, cognitive dissonance, confirmation bias, and emotional reactivity—common to all humans. Criminals weaponize these innate weaknesses through coercive narratives and technological tools to achieve psychological domination.

The psychological manipulation process typically unfolds across three phases:

3.1. Initial phase

3.1.1. Relationship building

Perpetrators initiate contact through passive or active approaches. Passively, they broadcast messages (SMS, emails, links) to mass audiences, disseminating fake job offers, task scams, escort fraud solicitations, or refund notices. These exploit curiosity to induce targeted demand, leveraging confirmation bias to entice victims into voluntary engagement. Actively, in romance-investment scams, AI deepfake schemes, or investment frauds, perpetrators launch precision strikes after thorough victim profiling, manipulating specific vulnerabilities to trap victims incrementally.

Regardless of approach, once initial contact is established, they deploy social engineering techniques—active listening, feigned empathy, strategic understanding, cold reading, and calculated self-disclosure—to build trust by mirroring victims' preferences.

3.1.2. Situation fabrication

Following initial trust establishment, perpetrators orchestrate deceptive scenarios to feign authenticity. Through direct and indirect psychological priming, they induce voluntary victim entrapment [9]. Subsequently, under pretexts of confidentiality, privacy, or security, they engineer victims' self-isolation, creating information vacuums that foster cognitive dissonance. Amidst fabricated verisimilitude, they exploit confirmation bias while leveraging authority effects and social desirability bias to covertly steer victims toward "self-determined" compliance. This systematic operant conditioning progressively reinforces victims' conviction until full belief in the fabricated reality is achieved.

3.2. Mid-phase

3.2.1. Emotional intensification

Upon victims' full compliance, perpetrators activate the exploitation phase. They fabricate exigencies or crises to instill acute anxiety, fear, rage, shame, or frustration through urgency impositions, threats, humiliation, or loss amplification. These engineered negative emotions prime specific behavioral responses, conditioning victims for irrational decision-making under duress.

3.2.2. Behavioral activation

Drawing on General Strain Theory (Agnew, 1992), individuals under tension or stress compulsively seek relief. Perpetrators exploit this urgency through monetary priming effects, presenting constrained choices to create an illusion of autonomy via double-bind inducement. This activates victims' irrational payment behaviors, ultimately incurring financial damages.

3.3. Terminal phase

3.3.1. Foot-in-the-door escalation

Following victims' initial losses, perpetrators capitalize on sunk cost fallacy and confirmation bias, offering post-hoc rationalizations to fuel the gambler's fallacy mentality. This induces further financial commitments, progressively escalating exploitation.

3.3.2. Perpetrator disengagement

Upon financial depletion, perpetrators typically enact abrupt disengagement—blocking and deleting victims—while vanishing without a trace. In more egregious cases, they inflict humiliation and derision, amplifying social stigma to suppress victims' reporting likelihood through shame-based deterrence.

Table 2 provides a concise overview of stage-specific psychological manipulation tactics.

Table 2. Overview of stage-specific psychological manipulation tactics

Phase	Stage	Core manipulation tactics
Initial	Relationship Building	Mass broadcasting scam lures (SMS/email/links); Precision victim profiling; Trust grooming via feigned empathy & cold reading
	Scenario Fabrication	Psychological priming; Forced self-isolation; Information control; Authority effect exploitation
Mid	Emotional Activation	Fabricated emergencies; Urgency imposition; Loss amplification; Humiliation/threat deployment
	Behavioral Triggering	Monetary priming; Constrained choices; Double-bind inducement; False autonomy illusion
Terminal	Foot-in-the-Door	Sunk cost fallacy exploitation; Post-hoc rationalization; Gambler's fallacy activation
	Disengagement	Immediate blocking/disappearing; Victim shaming/humiliation; Stigma-based reporting suppression

4. Countermeasures

4.1. Expand knowledge reserves, enhance scam detection capabilities

Leverage institutional anti-scam networks (schools, communities, workplaces) to strengthen public awareness through multi-channel campaigns—disseminating brochures, short videos, and official social media content. These initiatives elevate cybersecurity literacy, enhance information protection consciousness, deconstruct scam typologies, and unveil psychological manipulation mechanisms to empower early scam detection.

4.2. Fortify needs management, combat customized grooming

"Embrace desire-moderation to avoid becoming a criminal-ready target." Cognizantly regulate economic, material, and emotional needs through legitimate fulfillment channels. Cultivate robust social bonds for crisis support, while maintaining hypervigilance against stranger grooming tactics to neutralize customized scams.

4.3. Bolster psychological resilience, resist manipulation tactics

Fortify emotional stability and elevate self-esteem/confidence levels. Cultivate independent thinking and critical reasoning capacities to detect manipulation tactics preemptively. When confronting fabricated emergencies, maintain composure through multi-source verification and help-seeking—resisting coercive control under duress.

5. Future prospects

Telecom and online scams constitute not merely criminal issues but complex societal challenges. On one hand, researchers must intensify analysis of victim characteristics, researching susceptibility variations across diverse demographics and groups, identifying critical vulnerability markers, developing reliable assessment tools, and constructing precision prevention models for early identification of at-risk populations and targeted awareness campaigns. On the other hand, moving beyond the "ideal victim" paradigm, we must expose psychological manipulation mechanisms exploiting universal human vulnerabilities and enhance public capacity to detect coercive tactics—essential for effective scam prevention. Consequently, future research must prioritize empirical analysis and experimental studies to decode the underlying principles of psychological manipulation.

Funding

This research was supported by: Zhejiang Provincial Department of Education Special Project on Ideological and Political Education (Grant No. Y202250385); Ministry of Education Humanities and Social Sciences Research Special Task Project (Grant No. 23JDSZ3155)

Disclosure statement

The author declares no conflict of interest.

References

[1] Zhuang H, Ma ZH, 2025, Failure and Optimization of Telecom and Online Fraud Intelligence Warning. Journal of Intelligence, 44(2): 116–123.

[2] Zhang H, Jiang Y, 2023, Victimization Causes and Countermeasures of Telecom Fraud from Criminological Perspectives. Journal of Bohai University (Philosophy and Social Science Edition), 45(3): 38–41.

[3] Xia YW, 2025, Patterns and Causes of Repeated Fraud Victimization among Elderly Population: An Empirical Analysis Based on Over 10000 Samples. Journal of Shandong University (Philosophy and Social Sciences Edition), 2025(2): 76–90.

[4] He Q, Shen JR, 2020, Fraud Vulnerability of the Elderly: Concept, Theories, and Measurements. Chinese Journal of Applied Psychology, 26(3): 208–218.

[5] Tian L, Qian H, 2023, Psychological Susceptibility Profiles and Countermeasure Pathways of Undergraduate Victims in Telecom Scam Incidents. West Academic Journal, 2023(11): 131–134.

[6] Wang J, Qian XY, 2021, A Meta-Analysis on the Relation Between Self-Control and Fraud Vulnerability. Proceedings of the 23rd National Conference of Psychology: Abstracts (Volume II), 705–706.

[7] Whitty TM, 2019, Predicting Susceptibility to Cyber-fraud Victimhood. Journal of Financial Crime, 26(1): 277–292.

[8] Cross C, Kelly M, 2016, The Problem of "White Noise": Examining Current Prevention Approaches to Online Fraud. Journal of Financial Crime, 23(4): 806–818.

[9] Zhang WS, Xie ZW, 2024, Re-exploring the Definition of Hypnosis: A Kind of Profound Influence Characterized by Trance. Psychology Monthly, 19(9): 221–224 + 228.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.