Original paper

УДК 159:004:343.9

Preventing social engineering crimes: Vietnam's experience with the "5-NOs" rule and its alignment with modern behavioral psychology

Ninh Van Ngo
People's Security Academy,
Ministry of Public Security
(Hanoi, Vietnam)
ninhngo.pnsyc@gmail.com
ORCID: 0009-0002-3314-0002

Abstract

Introduction. The article examines Vietnam's "5-NOs" rule as a behavioral cybercrime prevention model against social engineering crimes. Drawing on case study analysis and theoretical cross-examination, the study analyzes how social engineering exploits cognitive vulnerability, emotional pressure, trust, urgency, and authority to manipulate victims' decision-making. In the context of industrialized scam centers, transnational cyber fraud, and AI-enhanced deception, the article argues that effective prevention requires not only technical cybersecurity measures but also the strengthening of human cognitive protection capacity. Based on an analysis of the psychological underpinnings of cybercrime, it has been shown that social engineering exploits cognitive vulnerabilities, emotional pressure, a psychological predisposition to trust, and factors such as urgency and the speaker's authority to manipulate the victim's decision-making process. **Methods:** general scientific methods of information processing (analysis, synthesis, specification) and discipline-specific methodology (case studies) are used to generalize and specify our understanding of behavioral strategies for countering cybercrimes committed through social engineering. **Results.** The findings suggest that Vietnam's "5-NOs" rule functions as a practical "Human Firewall" mechanism by translating critical thinking into simple behavioral refusal principles: no fear, no greed, no disclosure, no access, and no transfer. The article contributes to cybercrime prevention literature by positioning the Vietnamese experience as a community-based cognitive prevention model that may offer useful policy implications for countries facing similar social engineering threats.

Keywords

social engineering, Human Firewall, behavioral decision-making, "5-NOs" rule, cybercrime prevention, behavioral psychology, cognitive management, social prevention ecosystem

For citation: Ngo, N. V. (2026). Preventing social engineering crimes: Vietnam's experience with the "5-NOs" rule and its alignment with modern behavioral psychology. *Russian Journal of Deviant Behavior,* 6 (2), 288–298.

Оригинальная статья

Правило пяти «нет»: профилактика киберпреступлений, совершаемых методом социальной инженерии, в свете современной поведенческой психологии Республики Вьетнам

Нин Ван Нго
Академия общественной безопасности Министерства общественной безопасности Социалистической Республики Вьетнам
(Ханой, Вьетнам)
ninhngo.pnsyc@gmail.com
ORCID: 0009-0002-3314-0002

Аннотация

Введение. В статье рассматривается Правило пяти «нет», представляющее собой поведенческую модель профилактики киберпреступлений, используемую в Республике Вьетнам в целях предупреждения преступных посягательств с использованием методов социальной инженерии. Оценивая рост индустриализованных центров телефонного мошенничества, транснационального кибермошенничества и обмана с использованием искусственного интеллекта, автор отмечает, что эффективная профилактика требует не только применения технических мер кибербезопасности, но и укрепления когнитивных способностей для защиты от киберпреступников. На основе анализа представлений о психологических предпосылках киберпреступлений показано, что социальная инженерия использует когнитивную уязвимость, эмоциональное давление, психологическую установку на доверие, факторы срочности и авторитета говорящего для манипулирования процессом принятия решений жертвой. **Методы:** общенаучные методы обработки информации (анализ, синтез, конкретизация) и частнонаучная методология (анализ случаев (case study) применяются для обобщения и конкретизации представлений о поведенческих стратегиях противодействия киберпреступлениям, совершаемым методом социальной инженерии. **Результаты.** Полученные данные показывают, что Правило пяти «нет», разработанное на основе теоретических представлений о поведении жертвы кибермошенников, функционирует как механизм «межсетевого экрана» (Human Firewall), переводя принципы критического мышления в простые поведенческие правила отказа: не поддавайся страху, не поддавайся жадности, не разглашай, не предоставляй доступ, не переводи. Статья расширяет представления о психологической профилактике киберпреступлений, демонстрируя вьетнамский опыт как модель когнитивной профилактики киберпреступлений для стран, население которых подвергается аналогичным угрозам.

Ключевые слова

социальная инженерия, человеческий межсетевой экран, принятие решений, Правило пяти «нет», профилактика киберпреступлений, поведенческая психология, когнитивный менеджмент

Для цитирования: Нго, Н. В. (2026). Правило пяти «нет»: профилактика киберпреступлений, совершаемых методом социальной инженерии, в свете современной поведенческой психологии Республики Вьетнам. *Российский девиантологический журнал,* 6 (2), 288–298.

Introduction

In the era of global digital transformation, cybercrime has shifted from purely technical attacks to sophisticated forms that directly manipulate human cognition. According to Hadnagy (2018), Social Engineering is not merely a fraudulent act but a science of intentional influence aimed at neutralizing the most complex security systems through psychological manipulation.

This phenomenon has reached industrial proportions in Southeast Asia with the emergence of cross-border "scam centers" linked to cyber fraud, trafficking in persons, money laundering, underground banking, and transnational organized crime networks in East and Southeast Asia (UNODC, 2023, 2024). According to UNODC (2024), estimated annual revenues generated by these criminal operations range from USD 18 billion to USD 37 billion. The phenomenon reflects a form of "double victimization," in which trafficked or coerced individuals are forced to participate in online fraud operations while online citizens become victims of large-scale asset misappropriation.

The massive scale of this criminal network was further demonstrated by INTERPOL's Operation First Light 2024, a global crackdown targeting phishing, investment fraud, fake online shopping, romance scams, and impersonation scams across multiple jurisdictions. The operation resulted in nearly 4,000 arrests and the seizure of approximately USD 257 million in illicit assets[1].

Recent developments in generative artificial intelligence and deepfake technologies have further intensified the sophistication of social engineering attacks. AI-generated voice cloning, synthetic video impersonation, and automated conversational systems now enable cybercriminals to simulate trusted identities with unprecedented realism. As a result, psychological manipulation no longer depends solely on human persuasion skills but is increasingly amplified by AI-driven deception capable of accelerating emotional trust, panic, and impulsive decision-making. This observation is consistent with recent research showing that generative artificial intelligence can significantly amplify social engineering by enabling realistic content creation, advanced personalization, and automated attack infrastructure (Schmitt & Flechais, 2024).

In Vietnam, this challenge has become increasingly urgent, with economic losses caused by cyber-enabled fraud between 2020 and 2025 estimated at nearly VND 40 trillion[2]. The success of these crimes stems from exploiting cultural collectivism to paralyze critical thinking - a phenomenon consistent with behavioral decision-making theories, where emotional pressure weakens rational judgment and increases impulsive compliance (Kahneman, 2011).

Against this backdrop, this article focuses on decoding the psychological mechanisms behind the operation of scam centers, thereby sharing Vietnam's practical experience in building the "Human Firewall" model. The core of this model is the 5-NOs rule implemented by the Vietnam People's Public Security forces - an exemplary prevention strategy that combines cognitive education and law enforcement to ensure sustainable cyberspace protection.

Theoretical Framework and Literature Review

Social Engineering as a Behavioral Form of Cybercrime

Recent studies indicate that cybercrime has evolved from purely technical attacks into psychologically oriented forms of manipulation targeting human cognition and behavior. According to Hadnagy (2018), Social Engineering refers to the deliberate exploitation of psychological vulnerabilities such as trust, fear, urgency, authority, and emotional dependence in order to manipulate victims into

[1] INTERPOL. (2024, June 27). *USD 257 million seized in global police crackdown against online scams*. https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams

[2] Vietnam Government Electronic Newspaper. (2025, December 29). *Cybercrime causes nearly VND 40 trillion in losses during the 2020–2025 period* [In Vietnamese]. https://baochinhphu.vn/toi-pham-mang-gay-thiet-hai-gan-40000-ty-dong-giai-doan-2020-2025-102251229175200352.htm

compliance. Unlike traditional hacking methods that target technological systems, Social Engineering primarily attacks human decision-making processes.

Contemporary criminological research increasingly emphasizes the behavioral dimension of cybercrime. Wall (2007) argued that contemporary cybercrime increasingly exploits social interaction and human vulnerabilities embedded within digital communication systems. Similarly, Yar (2013) emphasized that modern online offending increasingly relies on symbolic persuasion and emotional influence rather than purely on technical expertise.

Within this framework, Social Engineering can be understood as a form of behavioral cybercrime in which offenders intentionally manipulate cognitive processes in order to bypass rational behavioral regulation and exploit emotional instability.

Behavioral Decision-Making and Cognitive Manipulation

The psychological effectiveness of Social Engineering can be explained through behavioral decision-making theories. According to Kahneman (2011), human cognition operates through two interconnected systems: intuitive-emotional processing (System 1) and analytical-rational processing (System 2). Under conditions of emotional pressure, urgency, fear, or excitement, individuals tend to rely on rapid emotional reactions rather than logical evaluation.

More recent cybersecurity research further supports this cognitive explanation by showing that heuristic processing and cognitive biases play a central role in users' susceptibility to social engineering attacks (Greavu-Şerban et al., 2025) found that social engineering vulnerability is closely associated with psychological shortcuts and biased decision-making, particularly when users are exposed to uncertainty, urgency, authority cues, or emotionally loaded messages. This reinforces the argument that Social Engineering operates not only through deception, but also through the deliberate exploitation of cognitive vulnerabilities in human decision-making.

Behavioral decision-making theories suggest that emotional pressure, urgency, and cognitive overload significantly weaken rational behavioral regulation and increase impulsive decision-making (Kahneman, 2011). In cybercrime contexts, offenders intentionally create psychological instability in order to reduce critical thinking and increase victim compliance.

Recent cyberpsychology studies also suggest that digital environments accelerate trust formation through anonymity, emotional projection, and identity flexibility. According to Whitty (2013), these characteristics enable offenders to rapidly construct false legitimacy and emotional dependence during online interactions. Consequently, Social Engineering functions not merely as deception, but as a process of behavioral destabilization aimed at temporarily suppressing rational cognitive control.

Persuasion Theory and Emotional Triggers

Research on persuasion theory further explains the effectiveness of online fraud schemes. Cialdini (2009) identified several major principles of persuasion, including authority, scarcity, reciprocity, social proof, commitment, and liking. Contemporary online fraud operations frequently operationalize these principles through impersonation tactics, romance scams, fake investment opportunities, and emergency scenarios designed to manipulate emotional responses.

Such emotional triggers significantly reduce the victim's capacity for rational judgment. In this sense, Social Engineering succeeds because emotional arousal temporarily overwhelms critical cognitive evaluation mechanisms. This process is particularly effective in online environments characterized by information overload, anonymity, and rapid communication.

Human Firewall and Preventive Criminology

The growing recognition that humans constitute the primary vulnerability in cybersecurity has contributed to the development of the "Human Firewall" concept. Unlike traditional cybersecurity

approaches focused primarily on technical protection, the Human Firewall model emphasizes cognitive awareness, behavioral resilience, and critical thinking as central mechanisms of cyber defense (Siegel, 1980, Thaler & Sunstein, 2009).

This approach is closely connected to the theory of Critical Thinking proposed by Harvey Siegel, which emphasizes rational evaluation and independent judgment as essential components of decision-making (Siegel, 1980). In addition, the behavioral intervention framework developed by Richard Thaler and Cass Sunstein through "Nudge Theory" suggests that simple and repeated behavioral guidance can shape safer decision-making patterns without requiring complex technical expertise (Thaler & Sunstein, 2009).

Within this context, Vietnam's "5-NOs" strategy may be interpreted as a behavioral prevention model designed to strengthen rational decision-making under psychological pressure and enhance community-based cyber prevention capacity. Protection Motivation Theory (PMT) further reinforces this perspective by explaining how individuals adopt protective behaviors when confronted with perceived threats (Rogers, 1975). According to PMT, protective action depends on two cognitive processes: threat appraisal (perceived severity and vulnerability) and coping appraisal (belief in one's ability to respond effectively). From this perspective, the "5-NOs" strategy functions not only as a behavioral guideline but also as a coping mechanism designed to enhance public self-efficacy and resistance against psychologically manipulative cyber threats.

Research Gap and Theoretical Contribution

Although previous studies have extensively examined online fraud and Social Engineering, several important gaps remain. First, limited research has analyzed Social Engineering through the lens of behavioral decision-making and cognitive destabilization. Second, empirical studies on Southeast Asian prevention models remain relatively underdeveloped, particularly regarding community-based cognitive prevention strategies.

However, recent Vietnam-focused empirical research has begun to provide important evidence on users' awareness of online scams. Pham et al. (2024), through an empirical survey of Vietnamese users, found that scam recognition varies across user groups and that prior victimization and information technology-related experience may influence users' ability to identify fraudulent scenarios. This finding suggests that anti-scam prevention in Vietnam should not be understood merely as a matter of information dissemination, but as a behavioral and cognitive problem involving perception, experience, and decision-making capacity.

Therefore, this study contributes to the literature by integrating criminological psychology with cybercrime prevention, applying behavioral decision-making theory to online fraud analysis, and examining Vietnam's "5-NOs" model as a practical Human Firewall strategy within the broader framework of preventive criminology.

Building upon this theoretical foundation, it becomes evident that the efficacy of cybercrime prevention depends not only on technical barriers but also on the strategic reinforcement of human cognitive defenses. While the concepts of behavioral decision-making and the Human Firewall provide a robust conceptual lens, their practical application requires rigorous empirical validation within specific socio-cultural contexts. Therefore, the following section outlines the methodological framework used to dissect the '5-NOs' strategy in Vietnam. By employing a case study approach, this research moves from abstract behavioral principles to a concrete analysis of how these psychological triggers are operationalized in real-world scams and how the Vietnamese prevention model functions as a psychological pause mechanism against such threats.

Methods

This study employs Case Study Analysis combined with empirical content analysis to examine the psychological mechanisms of Social Engineering techniques. Due to the anonymous and transnational nature of cybercrime and the inherent difficulties in gaining direct access to criminal organizations, the case study method allows the author to conduct an in-depth analysis of micro-behavioral mechanisms and the psychological transformations of victims - details that broad quantitative methods often fail to extract.

The research process was standardized through three logical stages to ensure objectivity and verifiability:

Data Collection and Case Screening

The author established selection criteria based on legal authenticity and the actual scale of impact during the 2022–2025 period. Focus was placed on two groups of Critical Cases:

The first group concerns mechanisms of forced victimization and extreme consequences, based on documented cases involving Vietnamese laborers trafficked into scam compounds near the Cambodian border regions of An Giang and Tay Ninh[3]. This case group was also examined in relation to UNODC's regional analysis of cyber fraud and trafficking in persons for forced criminality in Southeast Asia, which identifies scam compounds as sites where victims may be coerced into participating in online fraud operations (UNODC, 2023).

The second group concerns psychological manipulation techniques and the process of cognitive confinement among laborers in scam compounds and special economic zones, based on documented victim testimonies and publicly reported coercive labor experiences in Southeast Asia.

Scenario Anatomy and Theoretical Triangulation

Empirical data were analyzed using Scenario Analysis based on Hadnagy's (2018) four-stage Social Engineering attack cycle framework, comprising four stages: *Information Gathering, Relationship Building, Manipulation, and Execution*. This stage focuses on identifying "cognitive breaking points" - where psychological levers (such as authority and urgency) are utilized to paralyze the victim's critical thinking.

Macro-Verification and Model Synthesis

To reinforce generalizability, micro-analytical results were cross-referenced with macro-data from INTERPOL's Operation First Light 2024, which documented the transnational scale of cyber-enabled fraud through large-scale arrests, asset seizures, and the identification of multiple online scam typologies, including phishing, investment fraud, romance scams, fake online shopping, and impersonation scams[4], as well as reports on economic losses during 2020–2025 from the Vietnam Government Electronic Newspaper (2025). The entire process was examined through the theoretical lens of behavioral decision-making and cognitive vulnerability under emotional pressure (Kahneman, 2011) to clarify the correlation between deviant behavior and vulnerabilities in modern cognitive defense systems.

[3] Dan Tri Newspaper. (2022, September 23). *Families receive ashes of Vietnamese laborers from Cambodian scam centers* [Article in Vietnamese]. https://dantri.com.vn/lao-dong-viec-lam/than-nhan-lao-dong-viet-bo-mang-tai-campuchia-don-tro-cot-con-tro-ve-20220923125532091.htm

[4] INTERPOL. (2024, June 27). *USD 257 million seized in global police crackdown against online scams.* https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams

Results

The research findings confirm the emergence of an industrialized criminal model in which social engineering techniques are no longer isolated acts but are operated through an assembly-line structure with a strict division of labor.

Behavioral Transformation and the KPI Pressure System

Empirical data reveal an industrialized criminal model aimed at systematically transforming the personalities and behavioral patterns of coerced laborers. This finding is consistent with UNODC's (2024) assessment that cyber fraud in East and Southeast Asia has become increasingly embedded within broader transnational organized crime structures involving casino-linked financial systems, underground banking, and money laundering mechanisms.

First, the behavioral transformation cycle begins immediately after victims are isolated from communication and freedom of movement. Individuals are subjected to high-intensity psychological training, including the memorization of manipulation scripts and constant exposure to virtual success narratives. Second, criminal groups create unrealistic economic expectations, often promising thousands of U.S. dollars, while imposing a brutal KPI system that forces individuals to approach hundreds of targets each day. Third, behavioral deviance is maintained through violence and coercive discipline, particularly against those who fail to meet quotas or attempt to resist.

Anatomy of the Four-Stage Human Hacking Script

Based on Southeast Asian cases and Hadnagy's (2018) framework, the study identifies a typical four-stage psychological attack structure. The first stage is targeting, in which offenders use digital data to identify vulnerable groups, including individuals experiencing loneliness, financial stress, or social isolation. The second stage is priming, where offenders build trust through professional aliases, romantic personas, or institutional impersonation in order to lower the victim's cognitive defense barriers.

The third stage is crisis activation, which represents the pivotal moment of cognitive destabilization. At this stage, offenders use urgency, authority, fear, or excessive reward cues to push victims into states of panic or emotional excitement. Logical thinking is weakened, consistent with Kahneman's (2011) theory that emotional pressure shifts individuals from analytical reasoning toward intuitive and impulsive decision-making. The final stage is execution, in which victims are induced to perform financial transactions on fraudulent platforms before the offender severs contact.

Recent AI-assisted fraud cases demonstrate that emerging technologies increasingly reinforce each stage of this manipulation cycle. Deepfake voice impersonation, AI-generated video calls, and automated emotional interaction systems allow offenders to simulate authority figures, relatives, or financial professionals with high psychological credibility. Consequently, AI does not replace traditional social engineering mechanisms, rather, it magnifies cognitive vulnerability by accelerating trust formation and reducing the victim's capacity for critical evaluation under emotional pressure.

Systematizing the Mechanisms of Cognitive Manipulation in Vietnam

The study establishes that social engineering in Vietnam primarily targets cognitive structures rather than technical loopholes. Based on behavioral decision-making theory and cognitive vulnerability frameworks, these mechanisms are systematized in Table.

Social Consequences and Double Victimization in Vietnam

The parallel between international cases and the situation in Vietnam—where losses have reached nearly VND 40 trillion during the 2020–2025 period—underscores the urgency of the

Table. Systematization of psychological manipulation mechanisms causing cognitive destabilization

Таблица. Систематизация механизмов психологического манипулирования, вызывающих когнитивную дестабилизацию

Psychological Mechanism	Empirical Manifestation (Vietnam Case Study)	Impact on Victims (Behavioral Decision-Making Perspective)
Cognitive Urgency	Impersonating police to threaten arrest or investment platforms requiring deposits within "golden hours" (5–10 minutes).	Reduction of rationality in behavioral control, instinctive reactions, interruption of consequence forecasting.
Authority and Trust Traps	Exploiting cultural collectivism, using the prestige of law enforcement or cross-border romance scams.	Erosion of critical cognitive barriers, voluntary acceptance of irrational commands without fact-checking.
Displacement of Responsibility	Attributing financial risks to "luck," "algorithms," or "system errors."	Fragmentation of behavioral self-regulation, passivity toward the attacker's script due to belief in irrational factors.

problem[5]. Double victimization becomes evident when trafficked laborers not only lose their freedom and are coerced into criminal activity, but may also suffer severe physical consequences, as reflected in reported cases involving Vietnamese families in An Giang and Tay Ninh who received the ashes of relatives from Cambodian scam centers[6].

Study Limitations

Although the study is primarily based on verified media reports, official data, and public investigative materials, these sources remain valuable for examining a rapidly evolving cybercrime landscape in which direct access to criminal organizations is inherently constrained. Due to the transnational nature of scam centers, access to internal criminal records and victim interview data remains limited. Future research should expand through in-depth interviews with rescued victims, law enforcement officers, and cybersecurity professionals to enrich qualitative data on personality transformation, coercive control, and behavioral manipulation under conditions of forced criminality.

Conclusion and Recommendations

The research confirms that social engineering techniques have evolved into an industrialized criminal form that directly threatens economic stability and socio-psychological security. The success of these crimes lies not primarily in breaking technical barriers, but in neutralizing critical thinking and triggering cognitive destabilization, emotional compliance, and impulsive decision-making among victims.

[5] Vietnam Government Electronic Newspaper. (2025, December 29). *Cybercrime causes nearly VND 40 trillion in losses during the 2020–2025 period* [In Vietnamese]. https://baochinhphu.vn/toi-pham-mang-gay-thiet-hai-gan-40000-ty-dong-giai-doan-2020-2025-102251229175200352.htm

[6] Dan Tri Newspaper. (2022, September 23). *Families receive ashes of Vietnamese laborers from Cambodian scam centers* [Article in Vietnamese]. https://dantri.com.vn/lao-dong-viec-lam/than-nhan-lao-dong-viet-bo-mang-tai-campuchia-don-tro-cot-con-tro-ve-20220923125532091.htm

The Collapse of the Cognitive Shield

A key conclusion of this study is the confirmation of logical thinking paralysis under coercive psychological pressure. Drawing on Kahneman's (2011) behavioral decision-making theory, social engineering scripts are designed to bypass System 2 processing and force victims to react instinctively through System 1 responses. By forcing immediate responses to fabricated emergencies, offenders ensure that even highly educated individuals may become vulnerable to manipulative compliance.

Building the Human Firewall

To counter this challenge, the author proposes a proactive prevention model based on two layers of cognitive protection.

Re-Establishing Cognitive Control Through Critical Thinking

In this context, critical thinking acts as a psychological pause mechanism. Critical thinking supports system switching by activating System 2 processing and creating a temporal gap for rational evaluation before financial transactions are executed. It also strengthens professional skepticism by encouraging individuals to question timing, pressure, and procedural logic: Why now? Why the urgency? Does the request follow lawful procedures? Finally, critical thinking helps individuals identify emotional blind spots, such as fear, greed, or excessive euphoria, which are commonly exploited by social engineering offenders.

The Execution Layer: The "5-NOs" Strategy

The Vietnam People's Public Security has operationalized critical thinking into the "5-NOs" rule through five practical behavioral refusal principles:

No Fear: Maintaining composure to verify information directly with authorities.

No Greed: Rejecting unrealistic financial lures.

No Disclosure: Maintaining strict confidentiality of OTP codes and personal data.

No Access: Avoiding suspicious links and unauthorized digital access points.

No Transfer: Treating financial transfer as the final checkpoint against asset misappropriation.

The implementation of the "5-NOs" rule in Vietnam may therefore be understood as a cognitive education strategy. It functions as a behavioral nudge that establishes a simple choice architecture, directing citizens toward safer default responses under conditions of uncertainty, emotional pressure, or urgency (Thaler & Sunstein, 2009). This interpretation is also supported by recent Vietnam-based evidence suggesting that digital literacy plays an important role in strengthening personal information security and protective behavior in digital environments (Phan et al., 2025).

Implementation Experience and Policy Recommendations

The core strength of the Vietnamese model lies in creating a social prevention ecosystem in which state and community coordination is maximized. First, multi-layered coordination should combine mass media communication with community-based awareness campaigns led by local police forces. Second, citizens should be trained as security sensors capable of detecting and interrupting manipulation scripts before offenders achieve behavioral compliance. Third, states facing similar threats should treat the Human Firewall as a strategic priority equal to technical cybersecurity infrastructure.

In the emerging era of AI-driven deception and deepfake-enabled fraud, traditional technical cybersecurity measures alone are increasingly insufficient. Future prevention strategies must therefore prioritize cognitive defense capacity, critical thinking education, and behavioral awareness as essential components of national cybersecurity frameworks. In this context, the Human Firewall model represents not only a community-based prevention strategy but also a sustainable defense mechanism against the evolving psychological threats posed by artificial intelligence-enhanced cybercrime.

Ultimately, the battle against social engineering is a struggle to protect human cognition and rationality. Vietnam's experience with the "5-NOs" model demonstrates that when technical rules are transformed into a social prevention ecosystem with active citizen participation, psychological manipulation can be more effectively interrupted. This research provides a practical model for countries facing similar challenges and contributes to the broader goal of building a safer and more humane digital society.

References

Cialdini, R. B. (2009). *Influence: Science and practice (5th ed.)*. Pearson Education.

Greavu-Şerban, V., Constantin, F., & Necula, S.-C. (2025). Exploring heuristics and biases in cybersecurity: A factor analysis of social engineering vulnerabilities. *Systems*, 13(4), Article 280. https://doi.org/10.3390/systems13040280

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

Kahneman, D. (2011). *Thinking, fast and slow.* Farrar, Straus and Giroux.

Pham, K.-L., Le, T.-D., Tran, A.-D., Tran, M.-T., & Dang-Nguyen, D.-T. (2024). Vietnamese user awareness against scams in cyberspace: An empirical survey. In *Proceedings of the 1st Workshop on Security-Centric Strategies for Combating Information Disorder (SCID '24)* (pp. 1–6). Association for Computing Machinery. https://doi.org/10.1145/3660512.3665525

Phan, B. T., Do, P. H., & Le, D. Q. (2025). The impact of digital literacy on personal information security: Evidence from Vietnam. In *Proceedings of the International Conference on Emerging Challenges: Sustainable Strategies in the Data-driven Economy (ICECH 2024)* (pp. 475–489). Atlantis Press. https://doi.org/10.2991/978-94-6463-694-9_32

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57, Article 324. https://doi.org/10.1007/s10462-024-10973-2

Siegel, H. (1980). Critical thinking as an educational ideal. *The Educational Forum*, 45(1), 7–23. https://doi.org/10.1080/00131728009336046

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth and happiness* (2nd ed.). Penguin Books.

UNODC. (2023). *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia.* https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf

UNODC. (2024). *Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat.* https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

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

Whitty, M. T. (2013). The scammers' persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665–684. https://doi.org/10.1093/bjc/azt009

Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage Publications.

About the author

Ninh Van Ngo – Lecturer at the People's Security Academy, Ministry of Public Security.

Информация об авторе

Нин Ван Нго – преподаватель Академии народной безопасности при Министерстве общественной безопасности Социалистической Республики Вьетнам.

Автор заявляет об отсутствии конфликта интересов.
The author declare no conflicts of interests.

Поступила в редакцию 21.05.2026
Одобрена после рецензирования 06.07.2026
Опубликована 30.07.2026

Submitted May 21, 2026
Approved after reviewing July 06, 2026
Accepted July 30, 2026