



The Psychological Profile of Cybercrime Victims: Vulnerability Factors and Implications for Prevention

Mihaela Rus

Faculty of Law and Administrative Sciences, Ovidius University, Constanța, Romania
The Institute of Philosophy and Psychology of the Romanian Academy

Abstract

The increasing prevalence of cybercrime has drawn significant attention to the characteristics of offenders and the technological aspects of cyber attacks. However, comparatively less research has focused on the victims of cybercrime and the psychological factors that may contribute to their vulnerability. Cybercriminals frequently exploit cognitive biases, emotional responses, trust mechanisms, and decision-making processes to deceive individuals and gain unauthorized access to personal information, financial resources, or digital accounts. Understanding the psychological profile of cybercrime victims is therefore essential for developing effective prevention and intervention strategies. This article examines the psychological characteristics associated with susceptibility to cyber victimization, including trust propensity, impulsivity, risk perception, digital literacy, loneliness, anxiety, and social influence. Drawing upon theories of victimology, cyberpsychology, and criminology, the study explores how individual psychological traits interact with online environments to increase the likelihood of becoming a victim of phishing, identity theft, online fraud, social engineering attacks, and other forms of cybercrime. Particular attention is given to the role of cognitive and emotional factors that cybercriminals deliberately manipulate during the commission of cyber offenses. The purpose of this article is to identify the main psychological risk factors associated with cybercrime victimization and to assess their implications for crime prevention policies, public awareness campaigns, and victim protection measures. By highlighting the human dimension of cybersecurity, the article contributes to a better understanding of cybercrime victimization and supports the development of multidisciplinary approaches that integrate legal, criminological, and psychological perspectives in combating cybercrime.

Keywords: cybercrime victims; psychological profile; victimization; cyberpsychology; phishing; social engineering; cybersecurity

1. Introduction

The rapid expansion of digital technologies has fundamentally transformed the way individuals communicate, conduct business, and access information. Alongside these advances,

cyberspace has created new opportunities for criminal activities that transcend geographical boundaries and exploit both technological and human vulnerabilities. Cybercrime has evolved from isolated incidents of computer misuse into a complex global phenomenon encompassing financial fraud, identity theft, phishing, ransomware attacks, cyberstalking, online harassment and social engineering schemes. According to international reports, cybercrime continues to grow in both frequency and sophistication, affecting individuals, businesses, and public institutions worldwide (Europol, 2023; INTERPOL, 2023).

The increasing reliance on digital environments has expanded the potential victim pool while simultaneously creating new forms of psychological manipulation. Unlike traditional crimes, many cyber offenses do not require physical proximity between offenders and victims, allowing perpetrators to target large numbers of individuals with relatively limited resources (Leukfeldt, 2014). Moreover, cybercriminals increasingly employ persuasive communication techniques that exploit cognitive shortcuts, emotional responses and interpersonal trust rather than relying solely on technological vulnerabilities (Hahnagy, 2018). Consequently, understanding cybercrime requires not only a technological perspective but also a comprehensive psychological approach that examines why certain individuals become more susceptible to online victimization.

The societal and economic consequences of cybercrime are substantial. Financial losses associated with online fraud, ransomware, identity theft and business email compromise amount to billions of dollars annually, placing considerable strain on national economies, organizations and households (Europol, 2023). Beyond direct financial damage, cybercrime generates indirect costs related to system recovery, legal proceedings, cybersecurity investments, reputational damage and productivity losses. At the societal level, repeated cyber incidents undermine public trust in digital services, electronic commerce and governmental institutions, potentially slowing digital transformation and economic development (INTERPOL, 2023).

Equally important are the psychological and social consequences experienced by victims. Research indicates that cybercrime victimization is frequently associated with anxiety, depression, chronic stress, feelings of shame and self-blame, loss of trust, reduced self-efficacy and in severe cases, symptoms comparable to post-traumatic stress disorder (Cross et al., 2016). Victims of online fraud and cyber-enabled deception often report significant emotional distress because they perceive themselves as personally responsible for having been manipulated. Such psychological outcomes may persist long after financial losses have been recovered, highlighting that the impact of cybercrime extends well beyond economic harm.

Despite growing academic interest in cybercrime, research has traditionally focused on offenders, attack methods, technological vulnerabilities, and digital forensic investigations. Considerably less attention has been devoted to understanding the characteristics of victims and the psychological mechanisms that increase vulnerability to cybercrime. This imbalance limits the development of effective prevention strategies because cybercriminals primarily exploit human behavior rather than technological weaknesses. Recent studies suggest that individual differences—including personality traits, cognitive biases, emotional regulation, digital literacy and social trust—may significantly influence susceptibility to online deception (Button et al., 2014; McCormac et al., 2017; Vishwanath et al., 2018). Consequently, adopting a victim-centered perspective is essential for advancing both theoretical knowledge and practical interventions.

From a victimological standpoint, cyber victimization should be understood as the result of a dynamic interaction between individual characteristics, situational factors and the digital environment. Theories such as Lifestyle-Routine Activities Theory (Cohen & Felson, 1979)

and contemporary victimization frameworks suggest that exposure to risk is shaped not only by offenders' motivations but also by victims' behavioral patterns, online routines, and psychological vulnerabilities. Therefore, identifying the factors that increase or reduce susceptibility to cybercrime represents an important step toward designing evidence-based prevention programs that address human behavior alongside technological security.

The present article aims to provide a comprehensive theoretical review of the psychological profile of cybercrime victims by synthesizing current literature on the individual factors associated with online victimization. Specifically, the paper examines the role of personality characteristics, cognitive biases, emotional vulnerabilities, interpersonal trust and demographic variables in increasing susceptibility to cybercrime. Furthermore, it discusses the psychological consequences of cyber victimization and explores the implications of these findings for the development of prevention strategies focused on education, digital literacy, behavioral interventions and public policy. By integrating perspectives from psychology, criminology, victimology, and cybersecurity, this review seeks to contribute to a more comprehensive understanding of cybercrime victimization and to support the development of multidisciplinary prevention approaches capable of addressing one of the most significant security challenges of the digital age.

2. Theoretical Perspectives on Cybercrime Victimization

Understanding cybercrime victimization requires an interdisciplinary perspective that integrates concepts from criminology, psychology, victimology, and information security. Unlike traditional crimes, cybercrime frequently relies on the interaction between technological opportunities and human behavior, making victimization a multidimensional process influenced by situational, cognitive, emotional, and social factors. Several theoretical frameworks provide valuable insights into why certain individuals become more vulnerable to cybercrime than others. Among the most influential are Lifestyle-Routine Activities Theory, the General Theory of Victimization, and the Social Engineering Framework. Together, these perspectives explain how daily online activities, individual psychological characteristics, and manipulative communication techniques interact to facilitate cybercrime victimization.

2.1 Lifestyle-Routine Activities Theory

Lifestyle-Routine Activities Theory (LRAT), proposed by Cohen and Felson (1979), is one of the most widely applied criminological frameworks for explaining victimization. Originally developed to account for patterns of conventional crime, the theory has been successfully adapted to cyberspace, where online routines create opportunities for offenders to identify and exploit suitable targets. According to LRAT, victimization occurs when three conditions converge: a motivated offender, a suitable target, and the absence of capable guardians (Cohen & Felson, 1979).

In digital environments, motivated offenders include cybercriminals engaging in activities such as phishing, identity theft, ransomware deployment, financial fraud, and online scams. The concept of a suitable target extends beyond physical accessibility to include individuals whose online behaviors increase their visibility and susceptibility. Frequent use of social networking platforms, participation in online marketplaces, extensive disclosure of personal information, weak password practices, and limited cybersecurity awareness all contribute to increased target suitability (Leukfeldt, 2014).

The notion of capable guardianship also acquires a broader meaning in cyberspace. Traditional guardians, such as police presence or physical security measures, are replaced by technological and behavioral protections, including antivirus software, multi-factor authentication, secure

browsing habits, privacy settings, organizational cybersecurity policies and digital literacy. When these protective mechanisms are absent or insufficient, opportunities for cybercrime increase substantially.

Importantly, LRAT emphasizes that victimization is not solely determined by offenders' intentions but also by individuals' routine online activities. Modern lifestyles characterized by continuous internet connectivity, mobile banking, cloud computing, remote work and social media engagement expose users to numerous interactions with unknown individuals and digital services. Each online activity potentially increases contact with motivated offenders, thereby elevating victimization risk (Reyns, 2015).

Empirical studies have consistently demonstrated that online exposure significantly predicts cyber victimization. Individuals who spend more time online, frequently engage in online shopping, interact with strangers through social media, or use multiple digital platforms generally report higher rates of phishing victimization, malware infections, and identity theft (Bossler & Holt, 2009). Consequently, LRAT provides a valuable theoretical foundation for understanding how everyday digital behaviors shape opportunities for cybercrime.

Nevertheless, critics argue that LRAT primarily explains situational exposure while paying relatively limited attention to the psychological characteristics that influence individuals' responses to cyber threats. This limitation highlights the need to complement routine activity perspectives with theories emphasizing individual vulnerability and cognitive processes.

2.2 General Theory of Victimization

While opportunity-based theories explain how exposure to cyber threats occurs, the General Theory of Victimization emphasizes why certain individuals are more susceptible to becoming victims under similar circumstances. Finkelhor and Asdigian (1996) proposed that victimization is influenced by individual characteristics that shape exposure to risk, vulnerability, and the ability to recognize or avoid dangerous situations.

Within the context of cybercrime, vulnerability extends beyond demographic characteristics to encompass a broad range of psychological and behavioral factors. Individual differences in personality, emotional regulation, cognitive processing, digital competence, and interpersonal trust influence how users perceive online risks and respond to suspicious communications. As Finkelhor and Asdigian (1996) argue, individual characteristics influence both exposure to risk and susceptibility to deception.

Recent psychological research has identified several factors associated with increased cybercrime victimization. Personality traits such as impulsivity, low conscientiousness, excessive trust, sensation seeking, and poor self-control have been linked to greater susceptibility to online fraud (Button et al., 2014; McCormac et al., 2017). Similarly, emotional states including loneliness, anxiety, stress and social isolation may reduce critical thinking and increase individuals' willingness to engage with fraudulent communications promising financial gain, emotional support, or urgent assistance.

Cognitive biases also play a central role in cyber victimization. Optimism bias may lead individuals to believe that cybercrime happens only to others, while overconfidence in one's digital abilities can reduce compliance with recommended cybersecurity practices. Confirmation bias may cause users to selectively interpret suspicious information as trustworthy when it aligns with their expectations or desires. These cognitive mechanisms explain why even technologically competent individuals may become victims of sophisticated cyberattacks.

Another important aspect of the General Theory of Victimization is the interaction between individual vulnerabilities and environmental conditions. Psychological characteristics rarely operate independently; instead, they influence how individuals respond to situational cues presented during cyberattacks. For example, a highly impulsive individual exposed to a carefully designed phishing email during periods of stress may be considerably more vulnerable than someone with stronger emotional regulation and greater cybersecurity awareness.

Overall, this perspective shifts attention from technological systems to human behavior, emphasizing that effective cybercrime prevention requires identifying psychological risk factors alongside technical security measures.

3. Social Engineering Framework

Among contemporary explanations of cybercrime victimization, the Social Engineering Framework offers perhaps the most direct psychological perspective. Rather than exploiting software vulnerabilities, social engineering attacks target human cognition, emotions, and decision-making processes. Hadnagy (2018) defines social engineering as the deliberate manipulation of individuals into performing actions or disclosing confidential information that benefits the attacker. Consequently, social engineering attacks exploit cognitive biases rather than technological vulnerabilities (Hadnagy, 2018).

Social engineering is fundamentally based on principles of persuasion derived from social psychology. Cybercriminals frequently exploit authority, urgency, reciprocity, scarcity, commitment, consistency, and social proof to influence victims' decisions. These persuasive techniques reduce analytical thinking and encourage rapid responses, particularly in situations involving perceived threats or attractive rewards.

Phishing represents the most common form of social engineering. In phishing attacks, offenders impersonate trusted organizations such as banks, government agencies, online retailers, or employers to persuade recipients to disclose passwords, financial information, or other sensitive data. Advances in artificial intelligence and personalized data collection have significantly increased the sophistication and credibility of phishing campaigns, making them increasingly difficult to detect.

A more targeted variation is spear phishing, in which attackers customize messages using personal information obtained from social media, organizational websites, or previous data breaches. Because these communications appear highly credible and personally relevant, victims are more likely to trust the sender and comply with fraudulent requests. Spear phishing has become particularly prevalent in attacks targeting corporate employees, executives, researchers, and government officials.

Romance scams represent another psychologically sophisticated form of social engineering. In these schemes, offenders establish long-term emotional relationships with victims through dating platforms or social networking sites before requesting financial assistance or sensitive personal information. Unlike conventional phishing attacks, romance scams exploit emotional attachment, loneliness, empathy, and interpersonal trust. Victims often continue to believe the offender despite contradictory evidence, illustrating the powerful influence of emotional investment on decision-making.

The effectiveness of social engineering lies in its ability to exploit universal cognitive limitations rather than deficiencies in technical knowledge. Time pressure, emotional arousal, cognitive overload, and habitual decision-making reduce individuals' capacity for critical evaluation, making even experienced users vulnerable to deception (Vishwanath et al., 2018).

Consequently, cybersecurity is increasingly recognized as a behavioral challenge requiring psychological interventions in addition to technological safeguards.

Taken together, the Lifestyle-Routine Activities Theory, the General Theory of Victimization, and the Social Engineering Framework provide complementary explanations of cybercrime victimization. While LRAT emphasizes opportunities created by routine online behavior, the General Theory of Victimization focuses on individual susceptibility, and the Social Engineering Framework explains the psychological mechanisms through which offenders exploit human cognition and emotion. Integrating these perspectives provides a comprehensive theoretical foundation for understanding the psychological profile of cybercrime victims and informs the development of multidisciplinary prevention strategies.

3.1 Psychological Profile of Cybercrime Victims

Understanding why certain individuals become victims of cybercrime requires moving beyond technological explanations toward a comprehensive psychological perspective. While cybercriminals exploit digital infrastructures to initiate attacks, their success largely depends on manipulating human cognition, emotions, and behavior. Consequently, victimization is not merely a consequence of insufficient cybersecurity measures but also reflects the interaction between stable personality characteristics, cognitive biases, emotional states, social tendencies, and contextual factors.

Contemporary research indicates that there is no single "cybercrime victim personality." Rather, vulnerability emerges from the cumulative influence of multiple psychological characteristics that affect how individuals perceive risk, process information, make decisions, and respond to persuasive online communications (McCormac et al., 2017; Vishwanath et al., 2018). This multidimensional perspective is consistent with modern victimological approaches, which conceptualize victimization as a dynamic interaction between the individual and the digital environment.

3.2 Personality Traits

Personality represents one of the most stable predictors of human behavior and has received increasing attention in cybersecurity research. Individual differences influence risk perception, decision-making, trust formation, and compliance with cybersecurity recommendations. Consequently, personality traits may either increase susceptibility to cybercrime or function as protective factors against online deception.

The Five-Factor Model (FFM), commonly known as the Big Five, provides the most widely accepted framework for examining personality in relation to cybercrime victimization. The model includes openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism (Costa & McCrae, 1992). Although empirical findings are not always consistent, several traits have demonstrated meaningful associations with cybercrime vulnerability.

Among these dimensions, conscientiousness appears to be one of the strongest protective factors. Highly conscientious individuals tend to be organized, cautious, disciplined, and attentive to details. These characteristics promote secure online behaviors such as regularly updating passwords, verifying website authenticity, enabling multi-factor authentication, and following organizational cybersecurity guidelines. Conversely, individuals with low conscientiousness are more likely to neglect security precautions and engage in risky online practices. As McCormac et al. (2017) suggest, low conscientiousness may contribute to reduced cybersecurity behaviors.

Recent systematic evidence provides further support for the relationship between personality and phishing susceptibility, while also emphasizing substantial methodological heterogeneity. A 2025 systematic review of 26 eligible empirical studies found that extraversion, agreeableness, and neuroticism generally showed positive associations with phishing vulnerability, whereas conscientiousness emerged more consistently as a protective factor. However, the review also identified considerable variation in the methods used to operationalize and measure phishing susceptibility, indicating that personality effects should be interpreted as probabilistic and context-dependent rather than as stable predictors of victimization.

Agreeableness presents a more complex relationship with cybercrime victimization. Individuals high in agreeableness are generally trusting, cooperative, empathetic, and motivated to maintain harmonious interpersonal relationships. While these qualities facilitate positive social interactions, they may simultaneously increase vulnerability to social engineering attacks by making individuals more willing to believe persuasive messages or comply with requests from seemingly trustworthy sources. Fraudsters frequently exploit politeness, empathy, and the desire to help others during phishing and romance scams.

Neuroticism has also been associated with increased cybercrime susceptibility. Individuals scoring high on neuroticism tend to experience greater emotional instability, anxiety, and stress, which may reduce critical evaluation of online messages, particularly those involving urgency or fear. Cybercriminals commonly exploit these emotional responses through threatening communications that demand immediate action.

Although openness to experience and extraversion have shown less consistent relationships with victimization, some studies suggest that highly extraverted individuals may have broader online social networks and engage more frequently with unfamiliar contacts, thereby increasing exposure to potential offenders.

Beyond the Big Five, impulsivity has emerged as one of the strongest psychological predictors of cybercrime victimization. Impulsive individuals typically make rapid decisions without thoroughly evaluating potential consequences, making them particularly susceptible to phishing emails, fraudulent investment opportunities, and fake online marketplaces. Higher impulsivity has been associated with increased vulnerability to online fraud (Button et al., 2014). The effectiveness of many cyberattacks relies on creating a sense of urgency that discourages careful deliberation and encourages immediate responses.

Sensation seeking constitutes another relevant personality characteristic. Individuals who actively pursue novelty, excitement, and risk-taking experiences may engage more frequently with unfamiliar websites, download unverified applications, participate in online gambling, cryptocurrency investments, or interact with unknown users. Such behaviors inevitably increase opportunities for cybercriminals to initiate attacks.

Overall, personality traits do not directly determine cybercrime victimization but influence behavioral tendencies that either increase or reduce exposure to cyber threats. Consequently, personality should be viewed as one component within a broader constellation of psychological vulnerability factors.

3.3 Cognitive Vulnerabilities

Whereas personality traits represent relatively stable individual differences, cognitive vulnerabilities describe systematic patterns of information processing that influence decision-making during online interactions. Cybercriminals rarely rely solely on technical expertise;

instead, they exploit predictable cognitive biases that affect nearly all individuals under certain circumstances.

One of the most frequently observed biases is optimism bias, defined as the tendency to believe that negative events are more likely to happen to others than to oneself. Many internet users acknowledge the existence of phishing attacks and online fraud while simultaneously believing they possess sufficient skills to avoid becoming victims. This unrealistic optimism often reduces adherence to recommended cybersecurity practices.

Closely related is overconfidence, whereby individuals overestimate their ability to detect fraudulent communications. Technologically experienced users may become particularly vulnerable because confidence in their cybersecurity knowledge decreases vigilance. As cyberattacks become increasingly sophisticated and personalized, confidence alone no longer guarantees protection.

Confirmation bias further contributes to victimization by encouraging individuals to selectively interpret information that confirms existing expectations. For example, users expecting parcel deliveries may readily accept fraudulent shipping notifications, while individuals actively seeking employment may trust fake recruitment emails without carefully evaluating their authenticity.

Another important mechanism is heuristic processing. Dual-process theories of cognition distinguish between systematic, analytical thinking and rapid heuristic decision-making. Under conditions of time pressure or cognitive load, individuals often rely on mental shortcuts rather than careful evaluation. Victims frequently rely on heuristic rather than systematic processing when evaluating suspicious online communications (Vishwanath et al., 2018). Cybercriminals deliberately design phishing messages that trigger automatic responses through recognizable logos, familiar brands, or urgent requests.

Cognitive overload further amplifies vulnerability. Modern digital environments continuously expose users to emails, social media notifications, advertisements, instant messages, and organizational communications. This constant information flow reduces attentional resources available for critical evaluation, increasing the likelihood of overlooking warning signs or making rapid, intuitive decisions.

Taken together, these cognitive vulnerabilities illustrate that cybercrime often exploits universal features of human cognition rather than deficiencies in technical competence alone.

3.4 Emotional Factors

Emotional states substantially influence decision-making processes and represent another critical component of cybercrime victimization. Psychological research consistently demonstrates that emotions shape attention, memory, judgment, and risk perception, often overriding rational analysis during stressful situations.

Anxiety has received particular attention in cybercrime research. Individuals experiencing elevated anxiety are more likely to perceive urgent online communications as credible and respond impulsively to threatening messages claiming account suspension, security breaches, or financial losses. Fear-based phishing campaigns intentionally exploit these emotional reactions to reduce analytical thinking.

Loneliness represents another significant vulnerability factor. Social isolation increases the likelihood of seeking emotional connections through online platforms, making lonely individuals particularly susceptible to romance scams, catfishing schemes, and other forms of

interpersonal deception. Cybercriminals frequently invest considerable time in establishing emotional intimacy before requesting financial assistance or confidential information.

Chronic stress also impairs executive functioning, attention, and decision-making. Individuals experiencing occupational stress, financial difficulties, or family problems often possess reduced cognitive resources for evaluating suspicious online interactions. Under these circumstances, fraudulent messages requiring immediate action may receive less critical scrutiny.

Similarly, depressive symptoms may decrease motivation, concentration, and problem-solving capacity, increasing susceptibility to deceptive communications. Feelings of hopelessness or financial desperation may further enhance the attractiveness of fraudulent investment schemes or employment offers promising immediate financial relief.

An increasingly important area of research concerns emotion regulation. Individuals capable of effectively managing fear, frustration, excitement, or urgency are generally better equipped to resist manipulative online communications. Conversely, poor emotional regulation increases impulsive decision-making during emotionally charged situations. Emotional distress may impair critical judgment during online interactions (Cross et al., 2016).

Cybercriminals deliberately design attacks that evoke powerful emotional reactions—including fear, curiosity, empathy, excitement, greed, or compassion—because emotionally activated individuals are less likely to engage in careful analytical thinking. Consequently, emotional regulation has become a promising target for behavioral cybersecurity interventions.

3.5 Trust and Social Susceptibility

Human societies rely fundamentally on interpersonal trust. While trust facilitates cooperation and efficient communication, it simultaneously creates opportunities for deception in digital environments where identities can be easily manipulated.

Interpersonal trust refers to the expectation that others will behave honestly and benevolently. Individuals with high levels of generalized trust may initially assume that online communications originate from legitimate organizations or authentic individuals unless evidence suggests otherwise. Fraudsters frequently exploit social trust to manipulate victims into disclosing sensitive information (Leukfeldt, 2014).

Conformity also contributes to cybercrime vulnerability. Social engineering attacks frequently employ social proof by suggesting that "everyone has already completed this verification" or that "all employees are required to respond immediately." Such messages capitalize on individuals' tendency to align their behavior with perceived group norms.

Obedience to authority represents another powerful mechanism exploited by cybercriminals. Messages impersonating senior executives, government agencies, banks, or law enforcement organizations frequently induce compliance because individuals are psychologically inclined to obey perceived authority figures. Business Email Compromise (BEC) attacks provide a prominent example of authority-based manipulation.

Reciprocity constitutes an additional principle frequently exploited in online scams. Individuals who receive apparent assistance, gifts, discounts, or exclusive opportunities often experience a psychological obligation to reciprocate, making them more willing to provide personal information or financial assistance in return.

These social psychological mechanisms demonstrate that cybercrime extends beyond technical attacks to become a sophisticated process of interpersonal influence. Understanding social

susceptibility is therefore essential for developing prevention programs emphasizing critical evaluation of online social interactions.

3.6 Demographic Moderators

Although psychological characteristics play a central role in cybercrime victimization, demographic variables moderate how these vulnerabilities manifest across different populations.

Age has received considerable attention within cybercrime research. Contrary to common stereotypes, empirical evidence suggests that age alone is an inconsistent predictor of cyber victimization, whereas digital literacy appears to play a more substantial role (Burnes et al., 2017). Older adults may experience greater vulnerability due to limited technological experience and lower familiarity with emerging cyber threats. Conversely, younger individuals often exhibit greater online exposure, increased social media engagement, and higher risk-taking behaviors, which may offset their technological competence.

Educational attainment generally contributes to improved analytical thinking and information evaluation; however, formal education alone does not guarantee cybersecurity awareness. Highly educated individuals remain vulnerable when cyberattacks exploit emotional responses or sophisticated psychological manipulation rather than technical ignorance.

Digital literacy has emerged as one of the strongest protective factors against cybercrime. Individuals possessing greater knowledge of online security practices, phishing indicators, password management, and privacy protection are generally better equipped to identify fraudulent communications and respond appropriately. Nevertheless, cybersecurity education should incorporate psychological awareness alongside technical knowledge to address cognitive and emotional vulnerabilities.

Socio-economic status may also influence victimization patterns. Individuals experiencing financial hardship may be more attracted to fraudulent investment opportunities, fake employment offers, lottery scams, or financial assistance schemes promising rapid economic improvement. Conversely, individuals with higher incomes may become attractive targets for investment fraud, cryptocurrency scams, or business email compromise.

Importantly, these demographic variables do not operate independently but interact with personality, cognition, and emotional functioning. Consequently, cybercrime victimization should be conceptualized as the outcome of multiple interacting psychological and contextual factors rather than any single demographic characteristic.

In summary, the psychological profile of cybercrime victims is inherently multidimensional. Personality traits shape behavioral tendencies, cognitive biases influence information processing, emotional states affect decision-making, social susceptibility facilitates manipulation, and demographic characteristics moderate overall vulnerability. Understanding these interacting dimensions provides the theoretical basis for developing evidence-based prevention strategies that address the human factors underlying cybercrime victimization.

4. Methodology of Research

4.1 Research Design

The present study adopts a theoretical and narrative literature review design to examine the psychological factors associated with cybercrime victimization and their implications for prevention. A narrative review approach is particularly appropriate when the objective is not

merely to aggregate empirical findings, but to integrate heterogeneous theoretical perspectives and evidence from different disciplinary traditions into a coherent conceptual interpretation of a complex phenomenon (Snyder, 2019; Sukhera, 2022). Given the multidimensional nature of cybercrime victimization, the study therefore combines insights from psychology, criminology, victimology, and cybersecurity in order to explain how individual characteristics, cognitive processes, emotional responses, social influences, demographic factors, and patterns of online behavior may interact with situational and offender-related factors to increase vulnerability to cybercrime. Contemporary cybersecurity research increasingly recognizes that effective prevention requires an interdisciplinary approach integrating technological safeguards with psychological, behavioral, and organizational dimensions (Khadka & Ullah, 2025).

This interdisciplinary orientation is particularly relevant because cybercrime victimization cannot be adequately understood exclusively through technological or security-based explanations. Although technological vulnerabilities provide opportunities for cyber offending, research increasingly demonstrates that human behavior constitutes an important component of cybersecurity risk. Psychological characteristics, cognitive biases, risk perception, trust, impulsivity, habitual online behavior, and responses to persuasive or manipulative communication can influence individuals' susceptibility to different forms of online victimization (Bada & Nurse, 2020; Norris et al., 2019). Accordingly, the analytical framework adopted in this study considers cybercrime victimization as the outcome of an interaction between individual vulnerability and the characteristics of the digital environment, rather than as the consequence of a single psychological or technological factor.

The disciplinary integration employed in the review consequently operates at several complementary levels. From a psychological perspective, the analysis focuses on individual differences, cognitive mechanisms, emotional functioning, decision-making processes, and behavioral patterns that may influence susceptibility to online manipulation. The criminological perspective contributes explanations concerning criminal opportunity, offender–victim interaction, and the convergence of motivated offenders, suitable targets, and insufficient guardianship within digital environments. Routine activity theory remains particularly relevant in this respect because patterns of online exposure and digital routines can modify opportunities for cyber victimization (Leukfeldt & Yar, 2016; Pratt et al., 2010). The victimological perspective directs attention toward vulnerability, victim–offender dynamics, consequences of victimization, and the importance of avoiding explanations that inadvertently transfer responsibility from offenders to victims. Finally, the cybersecurity perspective situates psychological vulnerability within the broader technological environment in which online threats, social engineering techniques, malicious communications, compromised accounts, and other forms of digitally mediated offending occur.

The literature base is intentionally broad in order to reflect this interdisciplinary orientation. Sources considered include peer-reviewed academic articles, scholarly books, theoretical models and conceptual frameworks, empirical studies of cybercrime and online victimization, reports produced by international and European organizations, and selected grey literature and industry publications where these provide relevant evidence concerning emerging cyber threats. Combining academic and institutional sources is particularly useful in cybercrime research because technological and criminal practices may evolve more rapidly than conventional academic publication cycles. Nevertheless, peer-reviewed research constitutes the principal evidentiary foundation of the analysis, while institutional and grey literature is used primarily to contextualize emerging patterns and contemporary cybersecurity challenges.

The review process is organized into four interconnected analytical stages: identification, screening, synthesis, and integration. During the identification stage, literature relevant to

psychological vulnerability and cybercrime victimization is located and selected according to its conceptual and empirical relevance to the research objectives. The subsequent screening stage evaluates the relevance, quality, and substantive contribution of the identified sources. Although the present study is designed as a theoretical and narrative review rather than a systematic review, transparent identification and selection of relevant literature remains important for strengthening methodological rigor and reducing arbitrary source selection (Snyder, 2019).

The third stage consists of thematic and conceptual synthesis. Rather than treating individual studies as isolated findings, the analysis identifies recurring psychological and behavioral dimensions across the reviewed literature and examines the relationships among them. Narrative synthesis is particularly suitable for integrating heterogeneous evidence when studies differ in theoretical orientation, methodological design, populations, and measurement strategies (Popay et al., 2006). The purpose is therefore to identify convergent findings, conceptual relationships, and explanatory patterns that can contribute to a more comprehensive understanding of why some individuals may be more vulnerable than others to particular forms of cybercrime.

The final stage involves interdisciplinary integration. Findings derived from psychology, criminology, victimology, and cybersecurity are brought together within a unified conceptual framework. This stage is essential because psychological characteristics should not be interpreted independently of the social and technological environments in which cybercrime occurs. Individual vulnerabilities may become criminologically relevant only under particular conditions of online exposure, offender targeting, persuasive manipulation, or insufficient protective mechanisms. Consequently, the analytical model moves away from deterministic explanations in which specific personality traits or psychological characteristics are assumed to directly cause victimization.

Based on this synthesis, six principal domains of individual vulnerability are considered: personality traits, cognitive biases, emotional functioning, social influence mechanisms, demographic factors, and routine online behaviors. These dimensions should be understood as interacting rather than independent predictors. Personality characteristics may influence risk-taking or trust; cognitive biases may affect the evaluation of suspicious information; emotional states may reduce deliberative decision-making; social influence mechanisms may increase responsiveness to authority, urgency, reciprocity, or social proof; demographic and contextual factors may shape exposure to particular threats; and routine online behaviors may increase or decrease opportunities for offender contact. The interaction between these factors provides a more theoretically meaningful explanation of cybercrime vulnerability than approaches based on isolated individual characteristics.

Importantly, the concept of vulnerability employed in this study does not imply that victims are responsible for their victimization. Cybercrime is produced by intentional offender behavior, technological opportunity structures, and broader social and organizational conditions. Psychological vulnerability should therefore be interpreted probabilistically: particular characteristics or behaviors may increase susceptibility under certain circumstances, but they neither determine victimization nor diminish offender responsibility. This distinction is especially important from a victimological perspective, as cybersecurity interventions based excessively on individual responsibility may contribute to victim blaming and overlook the role of platform design, organizational security, offender manipulation, and structural conditions.

The principal purpose of the research design is consequently to develop a comprehensive conceptual framework explaining how psychological vulnerabilities interact with online

contexts and offender strategies to influence the risk of cybercrime victimization. The framework conceptualizes victimization as a dynamic process in which individual characteristics intersect with environmental exposure and offender techniques. This approach is consistent with contemporary human-centered cybersecurity perspectives, which emphasize that effective prevention requires attention not only to technical systems but also to the cognitive, behavioral, and social conditions under which individuals interact with those systems (Bada & Nurse, 2020).

The expected output of the review is an integrated conceptual model linking the identified vulnerability domains to cybercrime victimization and, subsequently, to prevention. Such a framework has both theoretical and practical implications. At the theoretical level, it facilitates dialogue between psychological explanations of individual vulnerability and criminological explanations of criminal opportunity. At the practical level, identifying the mechanisms through which personality, cognition, emotion, social influence, demographic characteristics, and online routines interact may contribute to the development of more targeted and evidence-based prevention strategies. Cybercrime victimization may generate significant psychological consequences that extend beyond immediate financial or informational losses, affecting both emotional well-being and victims' sense of security (Borwell et al., 2025).

Ultimately, the research design reflects the assumption that effective cybercrime prevention requires a human-centered and interdisciplinary perspective. Technological security measures remain indispensable, but they cannot fully address offences that deliberately exploit psychological and social mechanisms. By synthesizing evidence across psychology, criminology, victimology, and cybersecurity, the study seeks to provide a conceptual foundation for interventions that combine technological protection with psychological awareness, digital literacy, behavioral risk reduction, and more effective communication of cybersecurity risks. The resulting framework therefore positions individual vulnerabilities not as isolated causes of victimization, but as components of a broader interaction between human behavior, offender strategies, and the digital environment.

4.2 Research Objectives

The general objective of the present study is to develop a comprehensive understanding of the psychological dimensions associated with cybercrime victimization by examining the individual characteristics, cognitive and emotional mechanisms, social influences, and behavioral patterns that may contribute to vulnerability in digital environments. In addition to identifying potential vulnerability factors, the study seeks to explore the psychological consequences of cybercrime and to translate the resulting theoretical insights into relevant directions for prevention, cybersecurity education, and victim support.

The first research objective is to identify the principal psychological characteristics associated with cybercrime victimization. This objective focuses on individual-level factors that may influence how people perceive, evaluate, and respond to potentially harmful situations in digital environments. Particular attention is directed toward personality characteristics and psychological dispositions that may affect trust, risk perception, decision-making, interpersonal interaction, and responses to online persuasion. Rather than assuming that specific personality traits inevitably lead to victimization, the analysis seeks to determine how such characteristics may operate as vulnerability factors when combined with particular online circumstances and offender strategies.

The second research objective is to examine the cognitive, emotional, and social mechanisms that may increase individuals' susceptibility to cybercrime. From a cognitive perspective, the study considers how information processing, judgment, cognitive biases, attention, and

decision-making may influence the recognition of online threats. The emotional dimension addresses the ways in which fear, urgency, curiosity, loneliness, empathy, excitement, or other affective states may alter decision-making and increase responsiveness to manipulative messages. The social dimension focuses on mechanisms such as trust, authority, reciprocity, social proof, interpersonal influence, and perceived familiarity. Examining these dimensions together makes it possible to conceptualize cybercrime susceptibility as a dynamic process in which cognition, emotion, and social influence interact rather than operate independently. Individual differences in personality may contribute to variations in susceptibility to phishing and other forms of socially engineered cybercrime (Islam et al., 2025).

The third research objective is to analyze the psychological consequences experienced by victims of cybercrime. Cybercrime victimization may extend beyond immediate financial loss, compromised accounts, or unauthorized access to personal information. Victims may experience emotional distress, anxiety, fear, shame, anger, reduced interpersonal trust, feelings of insecurity, or changes in their subsequent online behavior. The study therefore examines victimization not simply as a discrete criminal event but as an experience that may have broader psychological and behavioral consequences. This objective also contributes to a more victim-centered understanding of cybercrime by emphasizing the importance of psychological recovery and appropriate support mechanisms.

The fourth research objective is to explore the relationship between psychological vulnerability factors and different forms of cybercrime, with particular attention to phishing, social engineering, identity theft, and romance scams. Different cybercrime strategies may exploit different psychological mechanisms. Phishing may rely heavily on urgency, authority, familiarity, or attentional limitations, whereas social engineering may involve more complex interpersonal manipulation and trust-building processes. Identity-related offences may exploit routine disclosure of personal information and insufficient risk perception, while romance scams frequently involve prolonged emotional engagement, attachment, trust, and interpersonal manipulation. The purpose of this objective is therefore to determine whether different forms of cybercrime are associated with distinctive configurations of psychological vulnerability rather than assuming the existence of a single generalized profile of the cybercrime victim.

The fifth research objective is to identify evidence-based implications for cybercrime prevention, cybersecurity education, and victim support. Understanding psychological vulnerability has limited practical value unless the identified mechanisms can inform strategies designed to reduce victimization and mitigate its consequences. The study therefore seeks to translate theoretical and empirical findings into preventive implications that acknowledge the importance of the human factor within cybersecurity. Such implications may include strengthening digital literacy, improving threat recognition, developing psychologically informed cybersecurity education, reducing susceptibility to manipulative communication, and designing interventions adapted to different patterns of vulnerability.

At the same time, prevention strategies should avoid placing excessive responsibility on individuals who become victims of cybercrime. Psychological vulnerability should not be interpreted as personal culpability or as evidence that victims are responsible for the offences committed against them. Instead, vulnerability emerges through the interaction between individual characteristics, digital environments, technological opportunities, and deliberate offender strategies. Prevention should consequently address not only individual behavior but also the design of digital systems, security mechanisms, communication practices, institutional responsibilities, and the manipulative strategies employed by offenders.

4.3 Research Questions

Building on the interdisciplinary framework of the study, the research questions were formulated to examine cybercrime victimization from a psychological perspective, while simultaneously considering the cognitive, emotional, social, and behavioral mechanisms through which vulnerability may emerge. Existing research suggests that cybercrime victimization cannot be explained through a single individual characteristic. Rather, vulnerability appears to result from interactions between individual differences, routine online activities, situational factors, persuasive strategies, and the specific characteristics of the digital environment (Norris et al., 2019; Whitty, 2019). Accordingly, the present study addresses seven interrelated research questions.

RQ1. Which psychological characteristics are most frequently associated with cybercrime victimization?

The first research question seeks to identify the psychological characteristics that are most consistently associated with vulnerability to cybercrime. Previous research has examined factors such as trust, impulsivity, risk-taking tendencies, self-control, psychological vulnerability, and patterns of online behavior as possible correlates of online victimization (Norris et al., 2019; Whitty, 2019). However, these characteristics should not be understood as deterministic predictors of victimization. Their influence may depend on the interaction between individual dispositions, situational circumstances, online exposure, and offender strategies. RQ1 therefore provides the broad conceptual foundation for identifying recurrent psychological vulnerability factors across the reviewed literature.

RQ2. How do personality traits influence vulnerability to cybercrime?

The second research question focuses specifically on the role of personality. Personality traits may influence how individuals perceive risk, establish interpersonal trust, interact with unfamiliar persons online, disclose personal information, and respond to persuasive communications. Research investigating susceptibility to phishing and other forms of cybercrime has suggested that individual differences can contribute to variation in security-related behavior, although the relationship between personality and victimization is complex and context dependent (Halevi et al., 2017; Norris et al., 2019). The purpose of RQ2 is therefore to examine whether particular personality characteristics repeatedly emerge as vulnerability factors and under what circumstances their influence becomes relevant.

RQ3. What cognitive biases contribute to successful cyberattacks?

Cybercriminals frequently exploit limitations in human judgment and decision-making rather than relying exclusively on technological vulnerabilities. Phishing and social engineering attacks, for example, may use contextual cues and persuasive techniques to encourage rapid decisions and reduce critical evaluation of suspicious requests. Susceptibility may consequently be influenced by attentional limitations, heuristic processing, overconfidence, familiarity, and other cognitive mechanisms affecting threat recognition and decision-making (Vishwanath et al., 2018). RQ3 examines these cognitive mechanisms to determine how biases in information processing and judgment may increase the likelihood that deceptive online communications result in successful victimization.

RQ4. What role do emotional factors play in online decision-making and victimization?

The fourth research question examines the emotional dimension of cybercrime vulnerability. Online offenders frequently construct situations designed to elicit strong emotional responses, including fear, urgency, excitement, curiosity, affection, sympathy, or anxiety. Such emotional activation may affect the way information is processed and may encourage individuals to act

before adequately evaluating the credibility or potential consequences of a request. This mechanism is particularly relevant in social engineering and online fraud, where manipulation frequently involves both cognitive and emotional processes (Norris et al., 2019; Whitty, 2019). RQ4 therefore investigates how emotional states interact with online decision-making and whether particular affective mechanisms contribute to increased susceptibility to victimization.

RQ5. How do social influence mechanisms increase susceptibility to social engineering attacks?

Social engineering is fundamentally based on the manipulation of human interaction. Offenders may exploit perceived authority, trust, reciprocity, familiarity, social proof, urgency, or interpersonal relationships to persuade targets to disclose information or perform actions that compromise their security. Research on phishing and social engineering demonstrates that successful attacks frequently depend on the ability to manipulate social and psychological cues rather than on sophisticated technical intrusion alone (Hadnagy, 2018; Vishwanath et al., 2018). RQ5 therefore examines how mechanisms of social influence operate within cybercriminal interactions and how they may interact with individual psychological vulnerabilities.

RQ6. What are the principal psychological consequences of cybercrime victimization?

Cybercrime victimization can generate consequences that extend substantially beyond immediate financial or informational losses. Victims of online fraud and related offences may experience emotional distress, anxiety, anger, shame, embarrassment, reduced trust, feelings of vulnerability, and changes in subsequent online behavior. The psychological and social consequences of cybercrime may therefore constitute an important dimension of victim harm that is insufficiently represented when cybercrime is assessed exclusively through financial losses or technical damage (Button et al., 2020; Cross et al., 2016). RQ6 seeks to identify and synthesize the principal psychological consequences reported across different forms of cybercrime victimization.

RQ7. Which prevention strategies are most effective in reducing psychological vulnerability to cybercrime?

The final research question translates the preceding analysis into preventive implications. Traditional cybersecurity interventions have frequently emphasized information provision and technical awareness. However, knowledge of cybersecurity risks does not necessarily translate automatically into secure behavior. Effective prevention may therefore require interventions that address decision-making processes, habitual behavior, emotional manipulation, social engineering techniques, and the contexts in which risky online decisions occur (Bada & Nurse, 2020). RQ7 consequently examines which evidence-based strategies appear most promising for reducing psychologically mediated vulnerability, strengthening threat recognition, improving cybersecurity education, and supporting safer online decision-making.

4.4 Literature Search Strategy and Eligibility Criteria

The literature search strategy was designed to identify relevant theoretical and empirical contributions addressing the psychological dimensions of cybercrime victimization. Given the interdisciplinary nature of the research topic, the search was conducted across several major international scientific databases covering psychology, criminology, behavioral sciences, health sciences, and technology-related research. The principal databases consulted were Web of Science Core Collection, Scopus, PsycINFO, PubMed, and IEEE Xplore. In addition, Google Scholar was used as a supplementary search resource to identify potentially relevant publications that might not have been captured through the primary database searches.

The use of multiple databases was considered necessary because research on cybercrime victimization is distributed across several disciplinary fields and is therefore unlikely to be comprehensively represented within a single bibliographic database. PsycINFO was particularly relevant for identifying psychological and behavioral research, while Web of Science and Scopus provided broader multidisciplinary coverage. PubMed was included to capture research addressing psychological well-being, mental health, and the consequences of victimization, whereas IEEE Xplore facilitated the identification of studies situated at the intersection of human behavior, cybersecurity, and digital technologies. Google Scholar complemented these searches by facilitating the identification of additional academic and interdisciplinary sources.

The literature search primarily covered publications produced between 2014 and 2025, thereby emphasizing relatively recent research capable of reflecting the rapidly changing nature of digital environments, online behavior, and cybercrime. However, seminal theoretical contributions published before 2014 were retained when they were considered necessary for establishing the conceptual foundations of the study or for explaining theoretical models that continue to influence contemporary research. This approach enabled the review to combine recent empirical evidence with established theoretical perspectives.

The search considered different categories of scholarly material, including peer-reviewed journal articles, academic books, conference proceedings, and relevant reports. The selection of sources was guided primarily by their relevance to the psychological understanding of cybercrime victimization. Particular attention was given to research examining personality characteristics, cognitive processes and biases, emotional functioning, social influence mechanisms, behavioral patterns, and other individual-level factors potentially associated with vulnerability to cybercrime. Studies examining the psychological consequences experienced by victims and research addressing prevention or intervention strategies were also considered relevant to the objectives of the review.

Inclusion Criteria

Specific inclusion criteria were established to ensure that the selected literature corresponded to the conceptual scope and research objectives of the study. Studies were included when they explicitly investigated the psychological aspects of cybercrime victimization or examined psychological and behavioral factors potentially associated with vulnerability in digital environments.

Particular consideration was given to research investigating personality characteristics, cognitive mechanisms, emotional factors, and behavioral vulnerabilities. This included studies exploring how individual differences may influence online decision-making, risk perception, trust, susceptibility to manipulation, responses to persuasive communication, or engagement in behaviors that may increase exposure to cybercrime.

Studies examining the psychological consequences of cybercrime victimization were also eligible for inclusion. This criterion was necessary because the research seeks not only to explain why individuals may become vulnerable to cybercrime but also to understand the psychological impact of victimization. Accordingly, research addressing emotional distress, anxiety, fear, shame, loss of trust, perceived insecurity, behavioral changes, and related psychological consequences was considered relevant.

A further inclusion criterion concerned studies addressing cybercrime prevention or intervention strategies. Research examining cybersecurity awareness, digital literacy, behavioral interventions, educational programs, victim support, or psychologically informed

prevention strategies was included where it contributed to understanding how identified vulnerability factors might be reduced or managed.

The review primarily prioritized peer-reviewed academic literature written in English. This requirement was introduced to ensure a consistent basis for evaluating and comparing the selected research and to focus the analysis on sources subjected to academic quality-control procedures. Nevertheless, relevant academic books, conference proceedings, and reports were also considered where they provided important theoretical, empirical, or contextual contributions directly related to the objectives of the study.

Exclusion Criteria

Corresponding exclusion criteria were applied to maintain the psychological and victimological focus of the review. Studies focusing exclusively on technical aspects of cybersecurity were excluded when they did not incorporate a meaningful human, psychological, behavioral, or victimological dimension. Thus, research concerned exclusively with malware architecture, cryptographic systems, network security protocols, software vulnerabilities, intrusion detection, or other purely technical cybersecurity issues was considered outside the scope of the review unless it explicitly addressed human factors relevant to cybercrime victimization.

Studies concentrating exclusively on cyber offenders were similarly excluded when they did not address victims, victimization processes, or factors associated with individual susceptibility. Although offender behavior is relevant to understanding cybercrime more broadly, the central analytical focus of the present study is the psychological profile, vulnerability, experiences, and consequences associated with victimization. Research on offender characteristics was therefore retained only where it contributed directly to understanding offender–victim interaction or the psychological mechanisms used to manipulate potential victims.

Publications lacking sufficient empirical or theoretical relevance to psychological vulnerability were also excluded. The mere presence of terms such as cybercrime, cybersecurity, online fraud, or digital behavior was not considered sufficient for inclusion. Eligible sources needed to contribute directly to at least one of the principal analytical dimensions of the study, including psychological characteristics, cognitive biases, emotional processes, social influence, behavioral vulnerability, psychological consequences, or prevention.

Finally, duplicate publications and non-scientific sources were excluded from the principal evidence base. Duplicate records identified across databases were considered only once. Sources lacking adequate academic or institutional credibility were not included in the core synthesis.

Search strategy

Search terms were organized around three principal conceptual domains: **cybercrime/victimization**, **psychological vulnerability**, and **specific forms of cybercrime or prevention**. Boolean operators were used to combine terms within and across these domains.

The core search string was structured as follows:

(“cybercrime” OR “cyber victimization” OR “online victimization” OR “phishing” OR “online fraud” OR “social engineering” OR “identity theft” OR “romance scam*”) AND (“psychological vulnerability” OR “personality” OR “personality traits” OR “impulsivity” OR “trust” OR “risk perception” OR “cognitive bias*” OR “emotional vulnerability” OR

“loneliness” OR “anxiety” OR “digital literacy” OR “decision making”) AND (“victim*” OR “susceptibility” OR “vulnerability” OR “prevention” OR “intervention”).

Additional targeted searches were conducted using combinations such as:

(“phishing” OR “social engineering”) AND (“personality” OR “cognitive bias*” OR “trust” OR “impulsivity” OR “risk perception”);

(“online fraud” OR “romance scam*” OR “identity theft”) AND (“loneliness” OR “anxiety” OR “emotional vulnerability” OR “psychological distress”);

(“cybercrime victimization” OR “phishing susceptibility”) AND (“digital literacy” OR “cybersecurity awareness” OR “prevention” OR “training” OR “intervention”).

Search syntax was adapted where necessary to the indexing conventions and search functions of each database.

Table 1. Database Search Strategy

Database	Search period	Main concepts searched
Web of Science Core Collection	2014–2025	Cybercrime victimization × psychological vulnerability × prevention
Scopus	2014–2025	Cybercrime, phishing, online fraud × personality, cognition, emotion, trust
PsycINFO	2014–2025	Victimization × personality, cognitive biases, emotional vulnerability, decision-making
PubMed	2014–2025	Cyber victimization × psychological distress, mental health, vulnerability
IEEE Xplore	2014–2025	Phishing/social engineering × human factors, susceptibility, cybersecurity behavior
Google Scholar	2014–2025 + seminal works	Supplementary interdisciplinary and citation searching

Note. Seminal theoretical publications published before 2014 were additionally retained when directly relevant to the conceptual framework.

The study-selection process was conducted in sequential stages. Database and supplementary searches initially identified 187 records. After removal of 35 duplicate records, 152 records remained for title and abstract screening. At this stage, 14 records were excluded because they did not meet the predefined relevance criteria. The full texts of 138 publications were subsequently assessed for eligibility. Following full-text assessment, 9 publications were excluded, primarily because they lacked a substantive psychological or victimological component, focused exclusively on technical cybersecurity issues, or did not provide evidence relevant to the research questions. A final total of 129 sources was retained for the narrative synthesis.

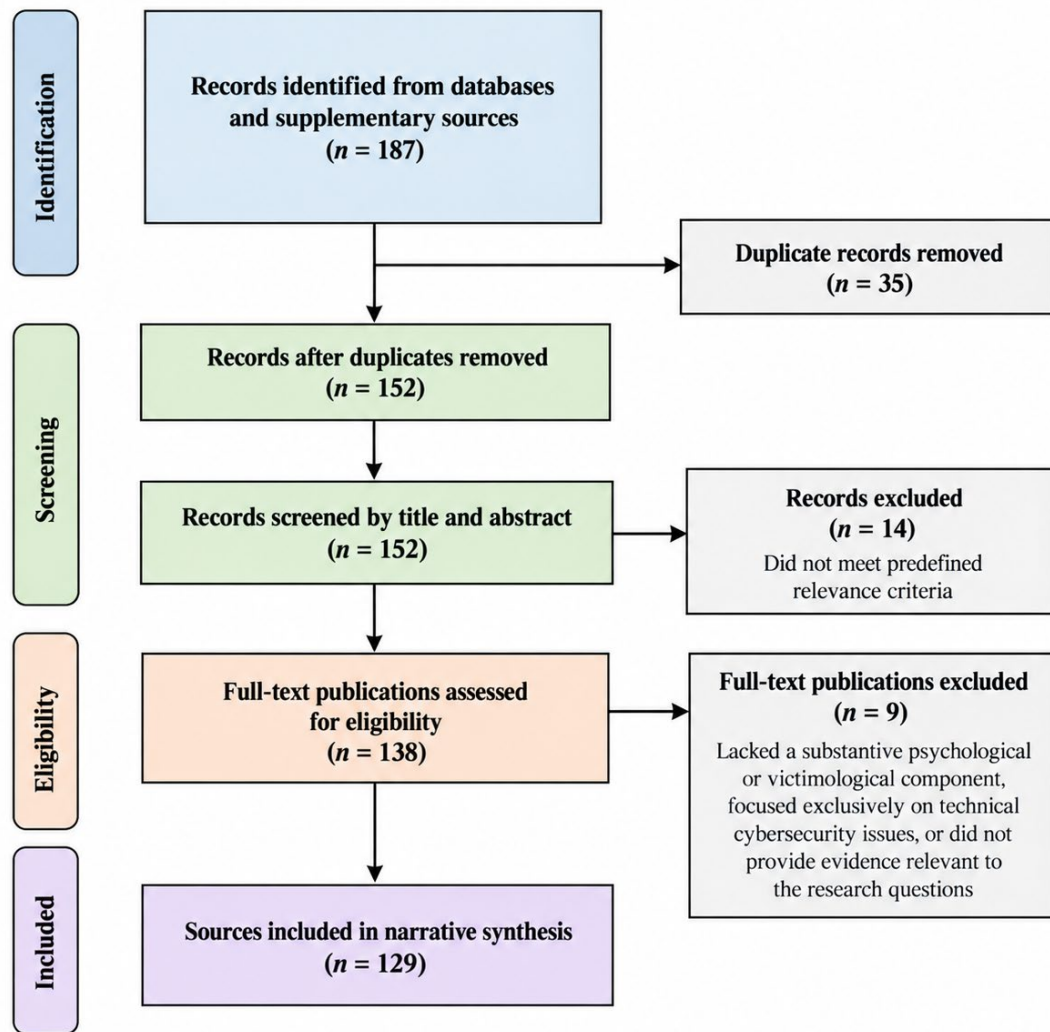


Figure 1. PRISMA-Style Flow Diagram of Literature Identification and Selection for the Narrative Review

Figure 1. Conceptual Representation of Cybercrime Victimization and Prevention

5. Future Research Priorities

The findings of the present study indicate several important directions for future research aimed at advancing the understanding, prevention, and management of cybercrime victimization. Although existing research has identified numerous psychological, cognitive, emotional, social, and behavioral factors associated with vulnerability in digital environments, important conceptual and methodological gaps remain. Future research should therefore move beyond isolated vulnerability factors and develop more dynamic, interdisciplinary, and empirically robust approaches capable of explaining how individual characteristics interact with technological, social, and cultural environments.

One important direction concerns the development of artificial intelligence-based predictive models of cybercrime vulnerability. Future studies could employ machine-learning techniques to examine complex combinations of psychological, behavioral, demographic, and digital variables associated with victimization. Rather than identifying isolated risk factors, predictive

models could detect patterns and interactions associated with different forms or levels of vulnerability and potentially support more targeted preventive interventions.

However, the development and deployment of such systems require explicit ethical safeguards. First, the collection and processing of psychological, behavioral, and digital data should comply with principles of data minimization, purpose limitation, informed consent, privacy, and data security, with particularly sensitive psychological information receiving enhanced protection. Second, predictive models should be routinely evaluated for algorithmic bias and discriminatory effects, since unrepresentative training data or inappropriate proxy variables may disproportionately classify particular demographic or social groups as vulnerable. Third, meaningful transparency and explainability should be provided so that individuals and relevant professionals can understand the principal factors contributing to vulnerability assessments.

Importantly, AI-generated vulnerability assessments should not be treated as deterministic classifications or used to stigmatize, exclude, penalize, or restrict individuals. Human oversight should remain integral to consequential decisions, and individuals should have appropriate mechanisms to question or contest automated assessments. Predictive outputs should therefore function primarily as tools for prevention, education, and protective support, rather than as instruments of surveillance or behavioral control. Where feasible, privacy-preserving approaches, secure data governance, periodic independent audits, and continuous monitoring of model performance should be incorporated throughout the system lifecycle.

Finally, the ethical use of AI in this context requires maintaining a clear distinction between vulnerability and responsibility. Identifying an individual as potentially more susceptible to cybercrime must never imply responsibility for subsequent victimization. Responsibility remains with offenders who deliberately exploit technological opportunities and psychological or social mechanisms. AI-based vulnerability prediction should consequently be designed according to a human-centered and harm-prevention approach, in which proportionality, fairness, autonomy, privacy, and victim protection remain central throughout model development and deployment.

A second priority involves the development of cross-cultural comparative research. Psychological vulnerability to cybercrime should not be assumed to operate identically across societies. Cultural values, interpersonal trust, attitudes toward authority, digital literacy, perceptions of privacy, social norms, communication styles, and patterns of technology use may influence both exposure to cyber threats and responses to manipulative strategies. Comparative studies involving participants from different countries and cultural contexts could clarify which vulnerability mechanisms are relatively universal and which are culturally dependent. Such research would also contribute to the development of culturally sensitive prevention strategies rather than relying on uniform cybersecurity interventions across diverse populations.

A third direction concerns the need for longitudinal research on vulnerability, victimization, and recovery. Much of the available evidence is based on cross-sectional designs that identify associations between psychological characteristics and victimization at a particular point in time. Such studies provide valuable information but are limited in their ability to establish temporal and causal relationships. Longitudinal research could examine how vulnerability develops over time, whether particular psychological characteristics precede victimization or are modified by the victimization experience, and how victims recover psychologically and behaviorally following cybercrime. This approach could also identify longer-term risk and protective factors and distinguish temporary reactions from persistent psychological consequences.

Future research should also explore the neuropsychological mechanisms underlying cybercrime vulnerability. Decision-making in digital environments involves cognitive control, attention, impulse regulation, emotional processing, reward evaluation, trust, and risk perception. Understanding the neuropsychological processes involved in these functions could provide a more detailed explanation of why individuals respond differently to deceptive or manipulative online stimuli. Experimental paradigms, cognitive assessment methods, and, where scientifically justified, neuroimaging techniques could be employed to investigate responses to simulated phishing, social engineering, fraudulent requests, and other cybercrime scenarios. Such research may contribute to the development of interventions designed to strengthen cognitive control, threat recognition, and psychological resilience.

Another major priority is the design of personalized prevention and cybersecurity education programs. Traditional cybersecurity education frequently provides standardized recommendations regardless of individual differences. However, the present analysis suggests that vulnerability may emerge through different psychological pathways. Some individuals may be particularly susceptible to urgency or authority cues, others to emotional manipulation, interpersonal trust, cognitive overload, or routine online behaviors. Future interventions could therefore be tailored according to relevant patterns of vulnerability. Personalized training may incorporate adaptive learning systems and carefully designed AI-assisted tools capable of adjusting educational content according to users' knowledge, behavioral patterns, or identified learning needs. The effectiveness of such interventions should be evaluated not merely through increases in cybersecurity knowledge but through measurable and sustained behavioral change.

Future research should simultaneously promote the development of human-centered and multidisciplinary cybersecurity frameworks. Cybercrime victimization cannot be fully explained or prevented through technological solutions alone. More comprehensive frameworks should integrate cybersecurity with psychology, criminology, sociology, victimology, public health, education, and related disciplines. Such approaches would make it possible to examine the interaction between technological systems and human behavior while also considering motivation, social context, psychological well-being, offender strategies, and structural conditions. The objective should be to develop cybersecurity systems that are not only technically robust but also compatible with the cognitive and behavioral characteristics of their users.

A particularly important research direction involves examining how multiple vulnerability factors interact. Personality traits, cognitive biases, emotional regulation, digital literacy, social influence, demographic characteristics, cultural context, and routine online behaviors are unlikely to operate independently. Future studies should therefore investigate interaction effects and identify combinations of factors associated with increased or reduced vulnerability. Advanced statistical approaches, longitudinal models, person-centered analyses, and systems-based methods may help researchers move from lists of isolated predictors toward more comprehensive explanatory models. This would support a conceptualization of cybercrime vulnerability as a dynamic and context-dependent process rather than as a stable individual characteristic.

Greater attention should also be devoted to protective factors and cyber resilience. Research has frequently concentrated on characteristics that increase vulnerability, while comparatively less attention has been given to the psychological and behavioral characteristics that enable individuals to recognize, resist, and recover from cyber threats. Future studies should investigate factors such as critical evaluation, adaptive coping, emotional regulation, digital competence, security habits, social support, and willingness to seek assistance or report victimization. Understanding protective mechanisms may be particularly valuable for

designing prevention strategies that strengthen individual and community resilience rather than focusing exclusively on deficits and vulnerabilities.

Another priority is the translation of scientific findings into evidence-based prevention, victim-support practices, and public policy. Research findings have limited practical impact if they remain disconnected from the institutions responsible for cybersecurity education, victim assistance, law enforcement, digital platform governance, and public policy. Future research should therefore evaluate how psychological evidence can be converted into practical programs, guidelines, educational interventions, and policy measures. Stronger collaboration between researchers, cybersecurity professionals, psychologists, victim-support organizations, law-enforcement agencies, policymakers, and digital service providers could facilitate this process.

Particular attention should be directed toward psychological support and recovery following cybercrime victimization. Prevention remains essential, but not all cybercrime can be prevented. Research should consequently examine which forms of psychological, social, informational, and institutional support are most effective after victimization. Different forms of cybercrime may require different responses. Victims of financial fraud, identity theft, cyberstalking, romance scams, or prolonged social engineering may experience substantially different forms of harm and may therefore benefit from differentiated support strategies. Future research should identify both immediate and long-term interventions capable of reducing distress, restoring confidence, rebuilding trust, and supporting safe re-engagement with digital environments.

Finally, future research should maintain a clear distinction between vulnerability and responsibility. Identifying psychological characteristics associated with cybercrime susceptibility should never result in the transfer of responsibility from offenders to victims. Individuals become victims because offenders intentionally exploit opportunities, technological systems, interpersonal relationships, and psychological mechanisms. The purpose of vulnerability research should therefore be to improve prevention and protection rather than to construct a stereotypical profile of the “ideal” cybercrime victim. This ethical principle should remain central to the development of predictive models, personalized interventions, cybersecurity education, and public communication.

Taken together, these priorities suggest that the next generation of cybercrime victimization research should move toward dynamic, longitudinal, cross-cultural, interdisciplinary, personalized, and human-centered models. Future studies should examine not only who may be vulnerable, but also how vulnerability develops, under what circumstances it becomes relevant, how multiple factors interact, which mechanisms protect individuals, and how victims recover following cybercrime. Integrating these directions could contribute to the ultimate objective of reducing cybercrime victimization, improving psychological well-being and recovery, strengthening digital resilience, and building safer, more inclusive, and more trustworthy digital environments.

6. Discussion

The findings of the present review support the conceptualization of cybercrime victimization as a complex and multidimensional phenomenon that cannot be adequately explained solely through technological vulnerabilities. Although technical weaknesses create opportunities for cybercriminal activity, the probability of victimization also depends on the interaction between psychological characteristics, cognitive processes, emotional states, social influence mechanisms, demographic characteristics, and routine online activities. From this perspective, cybercrime vulnerability should not be understood as a stable individual characteristic but

rather as a dynamic condition emerging from the interaction between the individual, the digital environment, and the strategies employed by offenders.

One of the central findings concerns the role of psychological characteristics. Individual differences may influence how people perceive online risks, establish trust, evaluate suspicious information, and respond to persuasive or potentially deceptive communications. Characteristics such as impulsivity, interpersonal trust, sensation seeking, self-esteem, self-efficacy, and conscientiousness may affect online decision-making and security-related behavior. However, these characteristics should not be interpreted as direct or deterministic causes of victimization. Their relevance emerges primarily when they interact with particular situational opportunities and offender strategies.

The findings further emphasize the importance of cognitive processes in explaining cybercrime susceptibility. Online decision-making frequently occurs under conditions of information overload, time pressure, uncertainty, and limited attention. Under such circumstances, individuals may rely on heuristics and mental shortcuts rather than systematic evaluation. Cognitive biases such as optimism bias, overconfidence, and confirmation bias may reduce the perceived probability of victimization or encourage individuals to interpret suspicious information in accordance with their pre-existing expectations. These mechanisms are particularly relevant to phishing and social engineering, where attackers frequently design messages to encourage rapid responses while discouraging critical evaluation.

A third important dimension involves emotional states. Anxiety, stress, loneliness, social isolation, emotional dysregulation, and other forms of psychological distress may influence decision-making and potentially increase vulnerability under particular circumstances. Cybercriminals can deliberately generate or exploit emotional states such as fear, urgency, curiosity, affection, sympathy, excitement, or anticipated reward. Strong emotional activation may temporarily interfere with reflective decision-making, making individuals more likely to respond to requests that they might otherwise recognize as suspicious.

This emotional dimension is particularly relevant to cybercrimes involving prolonged interpersonal manipulation. Romance scams, for example, may involve the gradual construction of emotional attachment and trust before financial or other requests are introduced. Other social engineering strategies may create fear through threats, urgency through artificial deadlines, or excitement through promises of financial gain. Consequently, emotional vulnerability should be considered in interaction with the offender's deliberate manipulation strategies rather than interpreted exclusively as an intrinsic characteristic of the victim.

The review also identifies social influence mechanisms as an important component of cybercrime victimization. Human behavior is influenced by perceived authority, conformity, reciprocity, interpersonal liking, familiarity, and social norms. Cybercriminals can reproduce or simulate these cues within digital environments. Fraudulent communications may imitate trusted institutions, employers, financial organizations, public authorities, colleagues, relatives, or other legitimate actors. Social engineering therefore operates partly by transferring ordinary mechanisms of interpersonal trust and social influence into deceptive digital contexts.

Demographic factors represent another relevant, although complex, dimension. Age, gender, educational background, income, occupation, socioeconomic status, cultural context, and level of digital experience may influence both exposure to particular cyber threats and the ability to recognize them. Nevertheless, demographic characteristics should not be treated as simple predictors of victimization. Their effects may be mediated or moderated by digital literacy, online routines, technological experience, social context, and the specific type of cybercrime

under consideration. Consequently, demographic vulnerability is more appropriately understood as contextual rather than deterministic.

The final major dimension concerns routine online activities. The amount of time spent online, the platforms used, patterns of social media engagement, information-sharing practices, digital communication habits, security behaviors, and the use of protective mechanisms all influence opportunities for exposure to cybercrime. Increased online activity does not automatically produce victimization, but certain patterns of digital behavior may increase contact with potential offenders or expose individuals to environments in which manipulation and fraud are more likely to occur.

Taken together, these findings suggest that cybercrime victimization emerges through a multidimensional interaction:

psychological characteristics + cognitive processes + emotional states + social influence + demographic context + routine online activities → differential vulnerability to cybercrime.

The model should not be interpreted as suggesting that these characteristics inevitably result in victimization. Rather, they influence susceptibility within specific environmental and situational conditions. Cybercrime occurs when offender strategies successfully exploit the interaction between human characteristics and digital opportunities.

An important implication of this interpretation is that the human factor occupies a central position in cyber resilience. Strengthening cybersecurity therefore requires more than technical protection. Awareness and education should be accompanied by improvements in critical thinking, online decision-making, emotional regulation, digital literacy, safe online behavior, and the capacity to recognize manipulative communication. Cyber resilience should consequently be understood as involving both technological protection and psychological and behavioral preparedness.

6.1 Theoretical Implications

The findings have several theoretical implications for understanding cybercrime victimization. Most importantly, no single theoretical framework appears sufficient to explain the complexity of vulnerability in digital environments. Instead, the results can be interpreted through the complementary contribution of three broad perspectives: Lifestyle–Routine Activities Theory, individual vulnerability approaches to victimization, and the Social Engineering Framework.

Lifestyle–Routine Activities Perspective

The Lifestyle–Routine Activities perspective provides an important explanation for the relationship between everyday digital behavior and exposure to cybercrime. Within digital environments, routine activities determine where individuals spend time, which platforms they use, with whom they communicate, what information they disclose, and what security practices they adopt. These activities influence the probability of encountering potential offenders and becoming accessible as targets.

From this perspective, cybercrime opportunities emerge through the convergence of a motivated offender, an accessible or suitable target, and insufficient guardianship. In the digital environment, guardianship may include technological safeguards, privacy settings, platform moderation, security monitoring, cybersecurity knowledge, and individual protective behavior.

The theoretical relevance of this approach lies primarily in explaining exposure and opportunity. Greater digital engagement may increase opportunities for offender–victim contact, while weak security practices or limited monitoring can reduce effective guardianship.

However, routine activity alone cannot fully explain why individuals exposed to similar digital risks respond differently to the same fraudulent or manipulative stimulus.

Individual Vulnerability and Victimization

A second theoretical perspective concerns individual vulnerability. This approach helps explain why exposure does not produce equivalent outcomes for all individuals. Personality characteristics, cognitive biases, emotional vulnerabilities, self-control, demographic circumstances, digital competence, and life circumstances may influence how individuals evaluate risk and respond to suspicious or manipulative situations.

The theoretical implication is that exposure and susceptibility should be analytically distinguished. Two individuals may encounter the same phishing message but interpret and respond to it differently because of variations in attention, trust, emotional state, prior experience, cognitive processing, or digital literacy. Individual vulnerability therefore contributes to understanding the psychological processes that occur between exposure to a threat and the behavioral response to that threat.

At the same time, vulnerability is contextual. Psychological characteristics do not operate independently of the situation in which decisions are made. Victimization risk is likely to increase when individual vulnerabilities interact with favorable criminal opportunities and carefully designed manipulation strategies.

Social Engineering Framework

The Social Engineering Framework provides a third complementary explanation by shifting attention from the characteristics of victims toward the deliberate strategies employed by offenders. Cybercriminals frequently exploit predictable psychological mechanisms rather than relying exclusively on technological intrusion.

Persuasion, authority, urgency, reciprocity, trust, familiarity, and emotional manipulation can be deliberately incorporated into fraudulent communications. These mechanisms may encourage rapid compliance, discourage verification, or create a false sense of legitimacy. Manipulative communications are particularly effective when they activate automatic or emotionally driven responses before reflective evaluation can occur.

This perspective is important because it prevents psychological explanations of cybercrime from becoming victim-centered in a problematic sense. Vulnerability does not itself produce cybercrime. Rather, offenders deliberately identify and exploit psychological mechanisms that are part of normal human cognition and social behavior.

The three theoretical perspectives can therefore be integrated into a sequential explanatory model:

Routine activities create exposure → individual characteristics influence susceptibility → offender manipulation activates or exploits vulnerability → decision-making occurs within the specific digital context → victimization may result.

This integrated framework provides a more comprehensive theoretical explanation than any of the perspectives considered independently. Lifestyle and routine activities explain where and when opportunities emerge; individual vulnerability approaches help explain why susceptibility varies between individuals and situations; and social engineering explains how offenders deliberately transform these vulnerabilities into opportunities for successful manipulation.

The principal theoretical implication is therefore that cybercrime victimization should be understood through an interactional model, rather than through exclusively technological, behavioral, or psychological explanations.

6.2 Practical Implications

The multidimensional character of cybercrime victimization has direct implications for prevention. Traditional cybersecurity measures remain essential, but technological safeguards alone are insufficient when attacks deliberately target human judgment, emotions, trust, and behavior. Effective prevention should therefore combine technological protection with behavioral cybersecurity education, digital literacy, psychological resilience, emotional regulation, and awareness of social engineering techniques.

Technological safeguards

The first component remains technological protection. Firewalls, encryption, secure systems, multi-factor authentication, threat detection, security monitoring, software updates, and effective vulnerability management can substantially reduce opportunities for cybercrime. These measures are particularly important because prevention should not depend exclusively on an individual's ability to identify every potential threat.

Technological systems should ideally be designed to compensate for predictable human limitations. Security mechanisms that reduce dependence on individual vigilance can provide an important protective layer, particularly when users are distracted, stressed, inexperienced, or confronted with highly sophisticated manipulation.

Behavioral cybersecurity education

The second component concerns behavioral cybersecurity education. Training should move beyond the simple transmission of information about cyber threats and address actual decision-making behavior. Individuals should learn to identify suspicious situations, verify information and sources, interrupt impulsive responses, and develop routines that reduce unnecessary exposure.

Cybersecurity education should therefore emphasize practical behavioral skills. Simulation-based training, realistic scenarios, repeated exposure to examples of manipulation, and immediate feedback may be particularly useful for transforming abstract knowledge into protective behavior.

Digital literacy

A third component is digital literacy. Individuals require not only technical knowledge but also the ability to critically evaluate websites, messages, digital identities, online content, and communication patterns. Digital literacy should include an understanding of how digital environments operate, how information can be manipulated, how personal data may be exploited, and how apparently legitimate communications can conceal fraudulent intentions.

Improved digital literacy can strengthen individuals' ability to detect inconsistencies, verify information, and make more informed decisions when confronted with uncertainty.

Psychological resilience training

The fourth component concerns psychological resilience. Prevention programs could strengthen self-efficacy, adaptive coping, confidence in responding to cyber threats, and willingness to seek assistance when necessary. Resilience is particularly important because complete prevention of cybercrime is unrealistic. Individuals should therefore be prepared not

only to avoid threats but also to respond effectively when suspicious events or actual victimization occur.

Psychological resilience may also reduce shame and encourage reporting. Individuals who understand that sophisticated manipulation can affect a wide range of people may be more willing to seek assistance rather than conceal victimization.

Emotional regulation

The fifth component involves emotional regulation. Since cybercriminals frequently use urgency, fear, anxiety, affection, curiosity, and anticipated rewards to influence decisions, individuals may benefit from strategies that help them recognize emotional manipulation and delay action.

A simple but potentially important preventive principle is to create psychological distance between emotional activation and behavioral response. When a communication generates unusually strong urgency, fear, excitement, or pressure, individuals should be encouraged to stop, verify the information independently, and avoid making immediate decisions.

Awareness of social engineering techniques

Finally, prevention requires explicit awareness of social engineering strategies. Individuals should understand common tactics such as phishing, pretexting, baiting, impersonation, fraudulent authority cues, artificial urgency, and emotionally manipulative requests.

Education should focus not merely on memorizing specific scam formats, which can rapidly become outdated, but on recognizing the underlying principles used by offenders. Understanding why a communication attempts to create urgency, establish false authority, evoke emotion, or discourage verification may provide more durable protection than learning to recognize individual examples of fraud.

Taken together, these practical implications support an integrated model of prevention:

technological safeguards + behavioral education + digital literacy + psychological resilience + emotional regulation + social engineering awareness → stronger cyber resilience and reduced vulnerability.

The practical objective should therefore be to create multiple complementary layers of protection. Technology protects systems, education supports safer choices, digital literacy strengthens critical evaluation, psychological resilience improves adaptive responses, emotional regulation reduces impulsive decisions, and social engineering awareness facilitates the recognition of manipulation.

Ultimately, effective cybercrime prevention requires a human-centered and multidisciplinary approach. Psychology, criminology, victimology, cybersecurity, education, technology, and the social sciences should be integrated rather than treated as separate domains. Such an approach recognizes that secure digital environments depend not only on stronger technologies but also on individuals and communities that are informed, psychologically prepared, digitally competent, and capable of responding adaptively to evolving cyber threats.

Accordingly, the prevention of cybercrime victimization can be conceptualized through the following integrated pathway:

Technology protects systems → people make safer decisions → psychological resilience supports adaptive responses → emotional regulation reduces manipulation → awareness strengthens threat recognition → cyber resilience increases → victimization risk decreases.

This integrated perspective provides a bridge between theoretical explanations of cybercrime vulnerability and practical strategies for prevention, while maintaining the fundamental principle that responsibility for cybercrime remains with offenders rather than with the individuals whose psychological or behavioral characteristics may be deliberately exploited.

To integrate the findings across vulnerability domains and translate them into practical prevention strategies, Table 2 maps the principal psychological and behavioral vulnerability mechanisms identified in the reviewed literature onto the forms of cybercrime in which they are particularly relevant and the corresponding targeted interventions. The mapping emphasizes that vulnerability domains are neither mutually exclusive nor deterministic; rather, different forms of cybercrime frequently exploit multiple interacting psychological and contextual mechanisms.

Table 2. Integrative Mapping of Psychological Vulnerability Domains, Cybercrime Types, and Targeted Preventive Interventions

Vulnerability domain	Specific vulnerability factors/mechanisms	Cybercrime types particularly relevant	Targeted preventive interventions
Personality and behavioral dispositions	Impulsivity, low conscientiousness, sensation seeking, excessive trust, risk-taking	Phishing; online fraud; investment scams; fraudulent marketplaces	Behavioral cybersecurity training; decision-delay strategies; personalized risk feedback; repeated phishing simulations
Cognitive vulnerabilities	Optimism bias, overconfidence, confirmation bias, heuristic processing, attentional limitations, cognitive overload	Phishing; spear phishing; identity theft; fraudulent notifications; credential theft	Threat-recognition training; simulated phishing exercises; just-in-time warnings; critical-evaluation checklists; periodic booster training
Emotional vulnerability	Anxiety, stress, loneliness, fear, urgency, emotional dysregulation, financial desperation	Romance scams; extortion scams; emergency/impersonation fraud; investment and employment scams	Emotion-regulation strategies; awareness of emotional manipulation; pause-before-action protocols; targeted support for vulnerable users
Trust and social influence	Authority, reciprocity, social proof, familiarity, interpersonal trust, conformity	Social engineering; Business Email Compromise; impersonation fraud; romance scams; spear phishing	Social-engineering awareness; identity-verification protocols; independent confirmation of high-risk requests; scenario-based training
Digital literacy and demographic/contextual factors	Limited cybersecurity knowledge, low digital competence,	Phishing; identity theft; online fraud; account	Digital-literacy programs; accessible

Vulnerability domain	Specific vulnerability factors/mechanisms	Cybercrime types particularly relevant	Targeted preventive interventions
	unfamiliarity with emerging threats, socioeconomic vulnerability	compromise; financial scams	cybersecurity education; tailored interventions for different user groups; guided security configuration
Routine online behaviors and exposure	Extensive information disclosure, weak password practices, interaction with unknown users, unsafe browsing, high platform exposure	Identity theft; account takeover; phishing; malware-enabled fraud; social-media scams	Multi-factor authentication; password-management education; privacy-setting interventions; reduced unnecessary disclosure; secure-browsing practices
Combined/multidimensional vulnerability	Interaction between personality, cognition, emotion, social influence and situational exposure	Sophisticated spear phishing; romance scams; personalized fraud; AI-assisted social engineering	Adaptive and personalized training; repeated simulations; booster sessions; layered technical and behavioral safeguards; targeted interventions based on vulnerability patterns

As Table 2 illustrates, effective cybercrime prevention requires more than generalized cybersecurity awareness. Different forms of cybercrime exploit different configurations of cognitive, emotional, social, and behavioral vulnerability. Prevention should therefore increasingly move toward layered and targeted interventions combining digital literacy, behavioral training, repeated phishing simulations, periodic reinforcement, identity-verification procedures, and technological safeguards. Importantly, the purpose of such targeting is to strengthen protective capacities rather than to classify or stigmatize individuals as inherently vulnerable victims.

7. Limitations and Potential Sources of Bias

The present review has several methodological limitations that should be considered when interpreting its findings. First, although the literature search was conducted across multiple multidisciplinary databases and supplemented by Google Scholar, the narrative nature of the review introduces an inherent risk of selection bias. Unlike a systematic review, a narrative synthesis necessarily involves a degree of researcher judgment in determining the conceptual relevance of individual publications and in integrating heterogeneous evidence. To reduce this risk, predefined inclusion and exclusion criteria were applied consistently, and the selection process was documented through a PRISMA-style flow diagram.

A second limitation concerns publication bias. Peer-reviewed literature may disproportionately represent studies reporting statistically significant, theoretically novel, or otherwise publishable findings, whereas null, inconsistent, or negative findings may be less likely to appear in indexed journals. Consequently, the associations identified between psychological characteristics and cybercrime vulnerability should not be interpreted as evidence that these factors operate uniformly across populations or cybercrime contexts. Particular caution is warranted where conclusions are based on a relatively limited number of studies or where findings across studies are inconsistent.

The interdisciplinary character of the field constitutes an additional source of heterogeneity. The reviewed literature encompasses psychology, criminology, victimology, behavioral science, and cybersecurity, and the included studies differ substantially in research design, sampling strategies, operational definitions, measurement instruments, populations, and forms of cybercrime examined. Such methodological heterogeneity limits direct comparability between studies and precludes the interpretation of the present synthesis as a quantitative estimate of the magnitude of individual vulnerability factors. The review therefore emphasizes patterns of convergence and divergence across the literature rather than pooled effect estimates.

An additional limitation concerns the predominance of English-language publications and the primary search period of 2014–2025. Although seminal earlier publications were retained when theoretically necessary, these eligibility decisions may have resulted in language and temporal selection biases. Relevant evidence published in other languages, in less widely indexed journals, or outside the specified period may consequently be underrepresented.

Particular consideration was given to the treatment of grey literature. Peer-reviewed academic research constituted the principal evidentiary foundation of the review because such publications have undergone formal scholarly evaluation and generally provide greater methodological transparency. Grey literature—including reports produced by governmental, European, international, professional, and cybersecurity organizations—was not assigned evidentiary weight equivalent to peer-reviewed empirical research. Instead, these sources were used primarily to contextualize rapidly evolving cybercrime patterns, emerging technologies, contemporary threat environments, and policy or institutional developments that may not yet be adequately represented in academic publications.

Grey-literature sources were considered according to source authority, methodological transparency, recency, relevance to the research questions, and consistency with peer-reviewed evidence. Greater weight was given to reports issued by established governmental, intergovernmental, or recognized professional organizations that clearly described their data sources or analytical procedures. Industry reports and other non-peer-reviewed materials were interpreted more cautiously and were not used as the sole evidentiary basis for substantive claims regarding psychological vulnerability when peer-reviewed evidence was available.

The inclusion of selected grey literature nevertheless involves a potential source-quality and reporting bias, since institutional and industry reports may differ in methodological rigor, transparency, objectives, and reporting practices. At the same time, excluding such material entirely could introduce another form of bias in a rapidly evolving field such as cybercrime, where new attack strategies and victimization patterns may emerge more quickly than conventional academic publication cycles allow. The present review therefore adopted a hierarchical approach to evidence: peer-reviewed empirical research was prioritized for substantive psychological conclusions, theoretical scholarship was used for conceptual interpretation, and credible grey literature was used primarily for contextual and contemporary information.

Finally, the findings should not be interpreted as establishing a fixed or deterministic psychological profile of the cybercrime victim. The evidence reviewed indicates substantial interaction between individual characteristics, situational circumstances, digital environments, offender strategies, and forms of cybercrime. Accordingly, the vulnerability factors identified in this review represent probabilistic and context-dependent associations rather than characteristics that inevitably lead to victimization.

8. Conclusions

The present study highlights that cybercrime has become one of the major security challenges of the digital era, affecting individuals, organizations, institutions, and societies worldwide. The continuous expansion of digital technologies has generated unprecedented opportunities for communication, economic activity, access to information, and social interaction. At the same time, these developments have created new opportunities for criminal behavior and have enabled cyber offenders to employ increasingly sophisticated techniques capable of exploiting not only technological vulnerabilities but also fundamental characteristics of human cognition, emotion, and social behavior.

A central conclusion emerging from the analysis is that cybercrime victimization cannot be adequately explained solely through technological weaknesses or demographic characteristics. Although technological security, digital infrastructure, age, education, socioeconomic status, and digital experience may influence exposure and vulnerability, these factors represent only part of a substantially more complex process. Victimization emerges from the interaction between individual characteristics, psychological mechanisms, contextual circumstances, patterns of digital behavior, and deliberate offender strategies.

The findings indicate that vulnerability to cybercrime can be conceptualized through six interconnected dimensions: personality traits, cognitive biases, emotional functioning, social influence mechanisms, demographic characteristics, and routine online behaviors. These dimensions do not operate independently. Instead, they interact dynamically and may become more or less relevant depending on the type of cybercrime, the characteristics of the digital environment, the individual's psychological state at a particular moment, and the manipulation techniques employed by the offender.

Personality characteristics may influence interpersonal trust, impulsivity, risk-taking, self-control, and responses to uncertainty. Cognitive biases and heuristic processing may affect the ability to recognize suspicious communications and accurately evaluate online risks. Emotional states can influence judgment, particularly when offenders deliberately generate fear, urgency, excitement, sympathy, affection, or anticipated reward. Social influence mechanisms, including authority, reciprocity, conformity, familiarity, and interpersonal trust, may further increase the persuasive effectiveness of fraudulent communications. These processes are embedded within demographic and cultural contexts and interact with routine online behaviors that determine exposure to potential offenders and risky digital environments.

An important conclusion of the study is therefore that there is no single psychological profile of the cybercrime victim. Individuals who become victims of cybercrime cannot be characterized through one stable personality type, demographic category, cognitive weakness, or behavioral pattern. Different combinations of factors may produce vulnerability under different circumstances. An individual who demonstrates strong cybersecurity knowledge may nevertheless become susceptible under conditions of emotional pressure, while another individual may be exposed primarily because of routine online behavior, excessive trust, limited digital literacy, or a highly convincing social engineering strategy.

Accordingly, vulnerability should be understood as probabilistic, contextual, and dynamic rather than deterministic. Psychological characteristics may modify susceptibility, but they do not inevitably lead to victimization. This distinction is particularly important because research into victim vulnerability carries the risk of unintentionally encouraging victim-blaming interpretations. The identification of psychological vulnerability factors should never imply that victims are responsible for the criminal acts committed against them. Responsibility remains with offenders who deliberately exploit technological opportunities and predictable characteristics of human cognition, emotion, and social interaction.

The findings also demonstrate the importance of understanding the relationship between human vulnerabilities and offender strategies. Contemporary cybercrime increasingly exploits psychological mechanisms through phishing, impersonation, social engineering, identity-related fraud, romance scams, and other forms of digitally mediated deception. Consequently, the human factor should not be conceptualized merely as the weakest element of cybersecurity. Human behavior can also represent an important component of cyber resilience when individuals possess appropriate knowledge, critical thinking skills, emotional regulation, digital competence, and effective protective habits.

This perspective has significant implications for prevention. Effective cybersecurity cannot depend exclusively on technological safeguards such as encryption, authentication, firewalls, monitoring systems, and software security. Although such mechanisms remain indispensable, they should be complemented by behavioral cybersecurity education, digital literacy, critical thinking, psychological resilience, emotional regulation, awareness of social engineering strategies, and accessible victim-support mechanisms. Prevention should therefore operate simultaneously at technological, psychological, behavioral, educational, organizational, and social levels.

The analysis further suggests that cybersecurity education should move beyond conventional awareness campaigns based primarily on the transmission of information. Knowing that phishing, fraud, or social engineering exists does not necessarily ensure that individuals will recognize these threats under conditions of urgency, emotional activation, cognitive overload, or sophisticated manipulation. Prevention programs should therefore strengthen the ability to recognize manipulation, interrupt automatic responses, verify information independently, tolerate uncertainty, and make reflective decisions before complying with suspicious requests.

Cyber resilience consequently emerges as a broader concept than technical protection. It involves the capacity to anticipate threats, recognize manipulation, make informed decisions, regulate emotional responses, adopt protective behaviors, seek assistance when necessary, and recover effectively following victimization. Building such resilience requires cooperation between cybersecurity specialists, psychologists, criminologists, victimologists, educators, policymakers, law-enforcement agencies, digital platforms, and other relevant stakeholders.

From a theoretical perspective, the study supports an integrated understanding of cybercrime victimization in which exposure, susceptibility, manipulation, and context operate together. Routine online activities influence exposure to potential offenders; individual psychological characteristics affect susceptibility; cognitive, emotional, and social mechanisms influence decision-making; and offender strategies deliberately exploit these processes. Victimization is therefore most appropriately understood as the potential outcome of interactions among multiple factors rather than as the consequence of a single vulnerability.

This relationship can be summarized as follows:

Individual characteristics + cognitive biases + emotional functioning + social influence + demographic and cultural context + routine online behavior + offender strategies → dynamic vulnerability to cybercrime.

The principal contribution of this perspective lies in shifting the focus from the search for a stereotypical “vulnerable victim” toward an understanding of situations and interactions that create vulnerability. Such a shift has important implications for both research and practice because it encourages prevention strategies designed to modify environments, strengthen protective mechanisms, improve decision-making, and disrupt offender manipulation rather than simply attempting to identify individuals presumed to be at risk.

Ultimately, understanding the complex interaction between psychological, behavioral, social, demographic, and technological factors is essential for developing more effective responses to cybercrime. A safer digital society requires an integrated approach in which technology protects systems, education strengthens knowledge, psychological interventions reinforce resilience, digital literacy supports critical evaluation, and institutional mechanisms provide effective protection and assistance.

The prevention of cybercrime victimization should therefore be understood not as an exclusively technological objective but as a multidisciplinary societal challenge centered on the interaction between people and digital environments. By recognizing both human vulnerability and human capacity for resilience, future cybersecurity strategies can move toward more comprehensive, adaptive, and evidence-based approaches capable of reducing victimization, supporting victims, strengthening cyber resilience, and contributing to a safer and more trustworthy digital society.

8.1 Evidence for the Effectiveness of Cybersecurity Interventions

Recent empirical and meta-analytic evidence provides a more nuanced assessment of the effectiveness of cybersecurity education and behavioral interventions. A meta-analysis of 69 studies examining cybersecurity training among end-users found an overall positive effect of training (Cohen’s $d = 0.75$, 95% CI [0.58, 0.92]). The effect was particularly pronounced for proximal outcomes such as cybersecurity knowledge and attitudes ($d = 1.02$, 95% CI [0.58, 1.46]). However, the estimated effect on actual behavioral change was considerably smaller and statistically uncertain ($d = 0.36$, 95% CI [−0.09, 0.80]). These findings indicate that cybersecurity training can substantially improve knowledge and attitudinal readiness, but that transferring these improvements into sustained secure behavior remains more difficult (Prümmer et al., 2025).

This distinction is particularly important for phishing prevention. Evidence from large-scale field studies suggests that repeated phishing simulations may contribute to improved threat recognition over time. In a multicenter study involving six U.S. healthcare institutions, 95 simulated phishing campaigns, and nearly three million simulated emails, 14.2% of emails were clicked. Compared with earlier exposure, participation in 6–10 phishing campaigns was associated with substantially lower odds of clicking on a subsequent simulated phishing message (adjusted OR = 0.511, 95% CI [0.382, 0.685]), while exposure to more than ten campaigns was associated with an even lower likelihood (adjusted OR = 0.335, 95% CI [0.282, 0.398]). These results support the potential value of repeated exposure and simulation-based learning rather than reliance on a single awareness intervention.

Nevertheless, evidence regarding phishing training is not uniformly positive. In another healthcare study involving 5,416 employees who received all 20 simulated phishing campaigns, click rates generally decreased over repeated campaigns, but mandatory training

introduced for employees with recurrent simulation failures did not produce a substantial additional reduction in phishing susceptibility. Employees identified as repeatedly susceptible continued to demonstrate higher click rates following training. This suggests that conventional training alone may be insufficient for individuals displaying persistent vulnerability and that intervention intensity should not automatically be equated with behavioral effectiveness.

More recent experimental evidence reinforces this caution. An eight-month randomized controlled experiment involving more than 19,500 employees and ten simulated phishing campaigns found no significant relationship between recent completion of conventional cybersecurity awareness training and subsequent phishing-simulation failure. Embedded training delivered following simulated phishing failures also produced only very small absolute differences between trained and untrained users. These findings suggest that commonly deployed anti-phishing training formats may have limited behavioral impact when implemented without sufficient engagement, personalization, or reinforcement (Lain et al., 2025).

Taken together, the available evidence supports a shift from one-off cybersecurity awareness sessions toward repeated, behaviorally informed interventions. Phishing simulations can provide users with opportunities to recognize deceptive cues under conditions that approximate real-world attacks, while periodic booster training may reinforce previously acquired knowledge and counteract the decay of security awareness over time. However, the evidence also indicates that repetition alone is not necessarily sufficient. Intervention effectiveness is likely to depend on training content, timing, user engagement, feedback, attack difficulty, and individual differences in vulnerability.

Accordingly, prevention strategies should combine repeated phishing simulations, immediate or timely feedback, periodic booster sessions, and targeted training for recurrently susceptible users. Evaluation should extend beyond knowledge acquisition and include behavioral outcomes such as simulated-phishing click rates, credential submission, reporting behavior, and retention of protective behaviors over time. This distinction is critical because the available meta-analytic evidence demonstrates that improvements in cybersecurity knowledge and attitudes are substantially larger than demonstrated changes in actual behavior.

References

- Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In V. Benson & J. McAlaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press. <https://doi.org/10.1016/B978-0-12-816203-3.00004-6>
- Borwell, J., Jansen, J., & Stol, W. (2025). The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors. *European Journal of Criminology*, 22(4), 603–624. <https://doi.org/10.1177/14773708241312506>
- Button, M., Lewis, C., & Tapley, J. (2020). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, 33, 36–54.
- Cross, C., Richards, K., & Smith, R. G. (2016). *Improving responses to online fraud victims: An examination of reporting and support*. Australian Institute of Criminology.
- Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
- Halevi, T., Memon, N., & Nov, O. (2017). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2544742>

- Islam, A., Rashid, M. M., Othman, F., Kaosar, M. G., & Islam, L. (2025). Identifying personality traits associated with phishing susceptibility. *Security Journal*, 38(1). <https://doi.org/10.1057/s41284-025-00466-4>
- Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24, Article 119. <https://doi.org/10.1007/s10207-025-01032-0>
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. <https://doi.org/10.1080/01639625.2015.1012409>
- Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34, 231–245. <https://doi.org/10.1007/s11896-019-09334-5>
- Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K., & Duffy, S. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews*. ESRC Methods Programme.
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. <https://doi.org/10.1177/0022427810365903>
- Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security*, 150, 104206. <https://doi.org/10.1016/j.cose.2024.104206>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Sukhera, J. (2022). Narrative reviews: Flexible, rigorous, and practical. *Journal of Graduate Medical Education*, 14(4), 414–417. <https://doi.org/10.4300/JGME-D-22-00480.1>
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146–1166. <https://doi.org/10.1177/0093650215627483>
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292. <https://doi.org/10.1108/JFC-10-2017-0095>