IJASRaR International Journal of Applied Sciences and Radiation Research
ISSN: 3062-2751 www.ijasrar.com ijasrar@gmail.com
Vol. 2-No.1 (2025) pp. 144-148
Research Article

Loss of Trust: How Cybercrime Changes the Way Victims See the Internet

Girish Chavan*

Department of Bachelors of Computer Application, MIT Arts Commerce and Science College, Alandi-(D), Pune, India.
* **Corresponding Author Email:** officialgirishchavan2005@gmail.com **ORCID:** 0000-0002-5247-0050

Article History:

DOI: 10.22399/ijasrar.45
Received: Oct. 01, 2025
Revised: Dec. 06, 2025
Accepted: Dec. 12, 2025

Keywords:

Loss of trust,
Interrnet,
Cybercrime.

Abstract: The growing digitalization of contemporary existence has redefined victimization boundaries, transforming cybercrime into an essential psychological and social risk. This research examines the impact of cybercrime on reshaping human cognition and trust and the resulting Generalized Digital Distrust (GDD)—an adaptive cognitive disorder in which victims view all digital stimuli, such as harmless emails and reminders, as threats. Based on multidisciplinary literature, psychological theory, and policy documents, the study integrates quantitative findings and qualitative accounts to analyze emotional outcomes like anxiety (claimed by 63%), stress (73%), anger (86%), depression (18%), and suicidal thoughts (3%) in cybercrime victims.The study finds that the erosion of trust goes beyond cyberspace, impairing victims' social relations and self-concept via internalized blame, shame, and learned helplessness. GDD appears in the form of hyper-vigilance and cognitive distortion, which generates avoidance of required digital interactions, cyber fatigue, and final digital exclusion. Yet, a divergent adaptive pattern shows up, in which trauma-inducing conservatism promotes heightened cybersecurity practices—like multi-factor authentication and risk assessment—illustrating the double-edged nature of cyber-victimization.This study enriches the conceptualization of GDD as both a psychological and behavioral theory of post-cybercrime trauma. It promotes Trauma-Informed Computing (TIC) and cognition reflection–based interventions that rebuild digital confidence without inducing fear-based avoidance. The research concludes that cybercrime needs to be considered not merely as a financial or technical threat but as an invasive form of digital trauma calling for an integrative approach combining psychological healing, human-centered security design, and knowledge-based policy intervention in order to re-establish digital trust.

1. Introduction

The increasing digitalization of human life has radically reshaped the criminal landscape, rendering cybercrime an over-riding risk to psychological health and international security. Spurred by quickening technological innovations, such as the spread of Artificial Intelligence (AI), crime has been automated, scaled, and hyper-personalized to attack known psychological weak spots to enhance prevalent online offenses such as financial fraud and phishing. Phishing, in turn, is the most widespread cyber offense, with internet users reporting victimization by the hundreds of thousands each year.

The transition from physical to virtual contact has changed the character of criminal harm, which is frequently continuous, intangible, and continuously amplified by the dynamics of the internet. The consequent psychological trauma of cybercrime victimization is deep, involving direct loss of trust and extreme emotional distress. As contemporary, frequently AI-based, cyberattacks aim to manipulate the human mind and destroy basic digital trust, subsequent psychological harm is much greater. This inability to differentiate advanced digital deception from normal interaction exacerbates the trauma, creating a deep-rooted state of generalized suspicion and anxiety in relation to the entire digital world. This result indicates that cyberattacks serve as powerful tools of psychological warfare.

1.1. Defining Generalized Digital Distrust (GDD) and Hyper-Vigilance

The primary emphasis is on Generalized Digital Distrust (GDD), an overarching, post-victimization mindset in which formerly trusted or non-threatening digital stimuli (e.g., unwanted emails, harmless links, program alerts) are universally felt to be real-time vectors of threat. This is an immediate result of

the psychological impact of cybercrime, which typically consists of symptoms ranging from Post Traumatic Stress Disorder (PTSD), heightened frustration, hostility, and extreme anxiety.The natural response of the body to trauma—hyper-vigilance—has a survival benefit in that it heightens readiness. But in the digital environment, over-hyper-vigilance along a broad and unclear spectrum of digital signals turns maladaptive. Victims describe hyper-vigilance along with paranoia and intrusive thinking, which inhibits cognitive recovery. This appears as an attentional bias and impaired emotional regulation, manifesting in a cognitive system breakdown where the victim is unable to properly discriminate real threats from non-threats (threat misattribution). This creates rejection of essential digital interactions, resulting in generalized avoidance. In doing so, GDD develops from a psychological symptom to a cause of functional, professional, and social impairment, commonly resulting in digital exclusion and decreased productivity.

2. Methodology

This study utilizes a mixed-method research design that combines qualitative and quantitative analyses of available academic studies, policy assessments, and empirical research on cybercrime and its psychological impacts. The research methodically examines various sources to analyze several aspects of post-victimization influence, such as the frequency and severity of emotional distress, such as depression, anger, and anxiety, and the cognitive mechanisms such as cognitive distortion and learned helplessness that influence behavioral reactions following cyber-attacks. It also examines the extent to which financial loss severity contributes to psychological harm and probes the different behavioral consequences of victims—ranging from maladaptive digital withdrawal and avoidance, to adaptive behavioral changes that yield increased cybersecurity awareness. By combining statistical evidence, for example, percentages of victims expressing distress, with rich qualitative accounts obtained from victim testimony, the research formulates an integrated model for how Generalized Digital Distrust (GDD) might be understood. This framework emphasizes the way digital trauma has the potential to develop into permanent functional impairments but can, in some contexts, produce adaptive security patterns. The approach focuses on an integrative comprehension of the dynamic interrelationship between emotional trauma and behavioral resilience in ultimately building a foundation for evidence-based, trauma-informed intervention and policy suggestions for reestablishing trust in digital spaces.

3. Findings Synthesised from Literature

The current literature emphasizes the severe and complex psychological implications of cybercrime, with victims experiencing extreme emotional distress, cognitive disarray, and dissolution of relational trust. Quantitative results reveal anger (86%), stress (73%), and anxiety (63%) to be the most frequent emotional harms, with more serious outcomes including depression (18%) and suicidal thoughts (3%) as well. Victims generally report this experience as deeply distressing, involving insomnia, a "heart-sinking" realization of loss, and ongoing distress after they discovered their financial or identity breach. Aside from emotional injury, cognitive functioning is also negatively affected, since the majority of victims internalize blame, viewing themselves as silly or at fault for being duped. This self-blame results in shame, guilt, and secrecy, further distancing victims and continuing their psychological distress. Another important consequence is learned helplessness, as a result of the perceived impossibility of avoiding subsequent attacks or learning how the crime transpired. This leads to passive acceptance of continued risk or denial of reality, which strengthens patterns of self-blame and avoidance. Lack of social support aggravates this helplessness, leaving victims stuck in psychological turmoil. Relational deterioration is also evident, especially in sophisticated frauds such as romance scams, where trust erosion goes beyond technology to interpersonal relationships. The relatives and friends suffer secondary trauma from the denial or continued suspicion of the victim, causing damage to interpersonal trust and hindering recovery.

Surprisingly, the extent of financial loss does not always correspond with the severity of psychological damage. Research shows that comparatively modest financial damages can have catastrophic effects, particularly on poorer victims who have difficulty rebounding both financially and emotionally. This disconnect shows that policy reactions grounded only in economic redress tend to ignore the more profound emotional impact of victimization. In addition, crimes that enable persistent exposure, like deepfakes or revenge porn, instill permanent digital trauma—the harm is perpetually available online, instilling chronic stress and hyper-vigilance. Since digital traces remain permanent, victims experience

the trauma over and over again, substantiating psychological exhaustion and an ongoing feeling of insecurity in virtual environments. Overall, the study emphasizes that cybercrime imposes long-lasting emotional, cognitive, and relational damage, generating patterns of self-blame, hyper-vigilance, and distrust that far outlast the first offense. Successful mitigation thus calls for convergence of psychological counseling, trauma-sensitive care, and preventive digital literacy to diffuse the helplessness chain and restore confidence of victims in online interaction.

4. Discussion

The analysis illustrates that cybercrime victimization is a double-edged phenomenon that, at the same time, produces maladaptive psychological withdrawal and adaptive security-led resilience. The post-victimization behavior paradox shows two contrasting paths that are determined by the victim's thought and affect patterns. On the one hand, the victims can fall into maladaptive outcomes—defined by Generalized Digital Distrust (GDD), chronic stress, hyper-vigilance, and shame—resulting in Cyber Fatigue and complete digital exclusion. These individuals tend to altogether bypass online participation, resulting in emotional numbness and learned helplessness. Conversely, the same experience can be eliciting adaptive advantage based on negative reinforcement learning, in which fear becomes motivation for precautionary behavior. This results in more robust cybersecurity behaviors like secure password management, use of antivirus tools, and a more reserved online presence—behaviors related to the target hardening concept, which studies indicate can help fend off almost 90% of possible cyber-threats.

Cognitive reflection is then the critical variable in identifying which path a victim takes. Individuals with more Thoughtfully Reflective Decision-Making (TRDM) have a higher tendency to shift trauma-evoked vigilance into useful digital prudence. This is greatly dependent on psychological care and the ability of the individual to self-regulate. In the absence of such psychological care, reflective thinking is compromised by trauma or lost altogether as a result of lack of support, resulting in the victim resorting to defensive avoidance with consequent Cyber Fatigue and social isolation. Yet, when trauma-informed awareness and counseling interventions are introduced at an early stage, victims are able to redirect fear into purposeful cybersecurity habits. Thus, recovery depends on enabling such a cognitive transition—from emotionally reactive hyper-vigilance to reflective, intentional caution—restoring victims' agency, confidence, and educated trust within digital environments.

5. Future Implementation Recommendations

Future recommendations for implementation highlight the imperative need to reform cybercrime response models to treat the intense psychological trauma that the victims endure. First and foremost, the implementation of Trauma-Informed (TI) digital environments is essential. Fear-based security alerts conventionally exacerbate anxiety and hyper-vigilance, driving victims into avoidance. In contrast, Trauma-Informed Computing (TIC) integrates design principles of safety, trust, collaboration, and enablement into user experience and security. Online platforms need to promote trust, communicate purposes with clarity, and give control back to users to reclaim their agency and offset the underlying chronic anxiety driving Generalized Digital Distrust (GDD) and exclusion.

Policy reactions need to develop beyond financial loss as their main concern. Research indicates that even limited financial loss can inflict life-changing psychological damage, particularly to at-risk groups. As a result, psychological recovery must take precedent, with the need for specialized training in trauma-informed management of technology-facilitated crime for law enforcement, legal professionals, and mental health workers. Immediate emotional counseling to victims is critical to assuage extreme anger, stress, and self-blame. Prevention should focus on ongoing education and problem-solving competencies in order to enable individuals to overcome helplessness and active digital protection.

Future studies need to explore the larger economic and societal costs of GDD and Cyber Fatigue, including effects on workforce productivity and public use of digital services. Controlled testing of TIC-based security interfaces will also measure their impact on ameliorating symptoms of GDD and promoting adaptive security behavior. More research into cognitive interventions, specifically those that augment Thoughtfully Reflective Decision-Making (TRDM), is required to refine psychological interventions promoting long-term digital resilience. Cumulatively, they hold the promise of a

comprehensive framework addressing not just technological vulnerabilities but also human and emotional aspects of victimization by cybercrime.

6. Conclusion

Victimization from cybercrime results in a fundamental and lasting change in the way people connect with the virtual world, tending to result in Generalized Digital Distrust (GDD) and over-hyper-vigilance. The short-term psychological impacts—loss of trust, worry, and self-blame—will send victims either to become more security-conscious and defensive or to retreat from using the digital world entirely. One important determinant of positive adaptation seems to be the capacity of the victim to use reflective, considered decision-making to convert increased risk perception into effective action for protection. Because cybercrime is an ongoing and multifaceted phenomenon, combating cybercrime involves methods beyond technical remediation to incorporate trauma-informed support and design, promoting sustainable digital well-being and resilience.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

1. Cyber risk and cybersecurity: a systematic review of data availability - PMC, accessed on October 17, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/
2. AI and Serious Online Crime | Centre for Emerging Technology and Security, accessed on October 17, 2025, https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime
3. The Latest Cyber Crime Statistics (updated July 2025) | AAG IT Support, accessed on October 17, 2025, https://aag-it.com/the-latest-cyber-crime-statistics/
4. Digital Trauma and Victimology: Rethinking Justice in the Age of Cybercrime | Virtuosity Legal, accessed on October 17, 2025, https://virtuositylegal.com/digital-trauma-and-victimology-rethinking-justice-in-the-age-of-cybercrime/
5. Protecting Minds in the Digital Age: A Review Based Study on ..., accessed on October 17, 2025, https://ijip.co.in/index.php/ijip/article/view/8563
6. Psychological Trauma and Cybercrime | Canadian Occupational Safety, accessed on October 17, 2025, https://www.thesafetymag.com/ca/news/opinion/psychological-trauma-and-cybercrime/252447
7. Keeping Your Guard Up: Hypervigilance Among Urban Residents Affected By Community and Police Violence, accessed on October 17, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC7263347/
8. Psychological Impact of Cybercrime - NABHS, accessed on October 17, 2025, https://nabhs.org/psychological-impact-of-cybercrime/
9. Experiences of victims of fraud and cyber crime - GOV.UK, accessed on October 17, 2025, https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime
10. The social and psychological impact of cyberattacks - ResearchGate, accessed on October 17, 2025, https://www.researchgate.net/publication/338313135_The_social_and_psychological_impact_of_cyberattacks
11. The Social and Psychological Impact of Cyber-Attacks - arXiv, accessed on October 17, 2025, https://arxiv.org/pdf/1909.13256
12. "Falling into a Black Hole": A Qualitative Exploration of the Lived ..., accessed on October 17, 2025, https://www.tandfonline.com/doi/full/10.1080/15564886.2025.2481267
13. Impact of Media-Induced Uncertainty on Mental Health: Narrative-Based Perspective - PMC, accessed on

October 17, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12175740/

14. Social media and moral panics: Assessing the effects of technological change on societal reaction - PubMed Central, accessed on October 17, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC7201200/
15. The Role of User Behaviour in Improving Cyber Security Management - Frontiers, accessed on October 17, 2025, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.561011/full
16. An exploratory study of cyber hygiene behaviors and knowledge, accessed on October 17, 2025, https://par.nsf.gov/servlets/purl/10083310
17. Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection - Digital Commons @ USF - University of South Florida, accessed on October 17, 2025, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=9991&context=etd
18. Engaging in cyber hygiene: the role of thoughtful decision-making and informational interventions - PubMed Central, accessed on October 17, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11576173/
19. A scoping review of trauma-informed care principles applied in design and technology, accessed on October 17, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12304634/
20. Trauma-Informed Approaches to Victims of Technology-Facilitated Crime | Office of Juvenile Justice and Delinquency Prevention, accessed on October 17, 2025, https://ojjdp.ojp.gov/media/video/33351
21. Trauma-Informed Computing: Towards Safer Technology Experiences for All - Emily Tseng, accessed on October 17, 2025, https://emtseng.me/assets/Chen-2022-CHI_Trauma-Informed-Computing.pdf