***EUROPEAN JOURNAL OF LIFE SAFETY AND STABILITY*** *(EJLSS)*
***ISSN2660-9630***
*www.ejlss.indexedresearch.org Volume 53, 2025 ||*




# Deteriorating Mental Condition Due to Cyber Fraud ( Depression, Anxiety, Phobia)

***Dr. Sangita Kumari***
*Assistant professor Department of psychology S.K Mahila college begusarai, L.N.M.U Darbhanga Bihar*

***Abstract:*** *In the rapidly digitising world, cyber fraud has emerged as one of the most insidious threats to individual well-being—not only in terms of financial loss but also due to its profound psychological consequences. While technological advances have brought unprecedented convenience, they have also opened gateways for cybercriminals to exploit vulnerabilities through phishing, identity theft, online scams, and social engineering. The emotional aftermath of such fraudulent experiences often goes unnoticed, yet it silently erodes the mental health of victims. This article explores the deteriorating psychological conditions—specifically depression, anxiety, and phobias—that arise from falling prey to cyber fraud.*

*Cyber fraud does not merely cause monetary damage; it shatters a person's sense of safety and trust. Victims often face humiliation, self-blame, and deep feelings of helplessness. These emotional responses, when left unaddressed, frequently develop into clinical depression. Many individuals also experience heightened anxiety, characterised by constant worry, sleeplessness, and panic attacks, especially when using digital devices or financial applications. A growing number even develop cyberphobia, an irrational fear of engaging with the internet or online platforms, fearing re-victimisation. These mental health issues can be so severe that they impair social interaction, job performance, and daily life functions.*

*Importantly, the psychological toll is not uniform. The elderly may experience deep trust violations and isolation, while younger victims may suffer reputational damage through blackmail or sextortion. Case studies from various countries show that many victims suffer in silence due to stigma, lack of awareness, or the absence of adequate mental health support systems. This silence exacerbates their trauma, pushing some towards suicidal thoughts or prolonged depressive episodes. Recovery is often slow and complex. While some victims benefit from professional psychological interventions like cognitive behavioural therapy (CBT), others find solace in peer support groups or digital detox strategies. However, one of the most significant barriers remains the lack of integrated support, where legal redressal and mental health aid do not go hand-in-hand. Public institutions and cybercrime cells often focus on technical investigation, while ignoring the need for trauma counselling and emotional rehabilitation.*

***Keywords:*** *Cyber fraud, Mental health impact, Depression, Anxiety disorders, Cyberphobia, Digital trauma, Online scams, Identity theft, Psychological consequences.*

***Date of Submission: 20-05-2025*** ***Date of Acceptance: 30-06-2025***

---

## Introduction

In the digital age, where nearly every aspect of our lives—from banking and communication to shopping and education—has migrated online, the threat of cyber fraud has become alarmingly widespread. What once required a physical presence or manipulation now only takes a few keystrokes. Cybercriminals can now infiltrate someone's financial life, personal identity, or even emotional space with chilling ease. While the financial implications of cyber fraud are widely discussed and documented, its **psychological consequences** remain deeply underexplored. Beneath the surface of data breaches and scam alerts lies a disturbing trend: a growing number of individuals suffering from **depression, anxiety, and phobia** as a direct result of falling victim to online fraud. Imagine a working professional who, after years of careful savings, loses everything overnight due to a well-disguised phishing attack. Or an elderly retiree who unknowingly gives access to a scammer impersonating a bank executive, only to be left not just penniless but also humiliated. The emotional toll of such experiences often includes **shame, helplessness, and persistent fear**—emotions that can spiral into serious mental health conditions. Victims report difficulty sleeping, a growing distrust of technology, withdrawal from social relationships, and in some cases, even suicidal thoughts. Unfortunately, these mental health struggles often go unnoticed or are dismissed as collateral damage of a technical crime.

Cyber fraud's psychological reach extends across all age groups, but it affects each demographic differently. Young adults may face reputational harm through social media exploitation or sextortion, while older adults might battle intense feelings of betrayal and loss of control. Children and adolescents exposed to online scams may carry the trauma into adulthood, altering their perceptions of trust and safety. As digital interactions increase, so does the **invisible trauma** they may carry. The irony is striking—technology designed to connect and empower has also become a conduit of deep psychological harm. Despite the growing number of cybercrime incidents, the integration of **mental health support into cybercrime response systems remains limited**. Most victims receive only technical advice or legal guidance, with little or no attention to the psychological distress they face. Furthermore, many suffer in silence due to fear of social judgement, or because they are unaware that what they are experiencing—such as persistent worry, avoidance of digital tools, or deep sadness—is actually a treatable mental health condition.

This article seeks to bridge this critical gap by shedding light on the **psychological aftermath of cyber fraud**, focusing on three major outcomes: depression, anxiety, and the emergence of digital-related phobias like cyberphobia. By combining academic research, real-life cases, and therapeutic insights, it aims to advocate for a more holistic response to cyber fraud—one that includes emotional healing alongside legal recourse and digital security. As cyber fraud continues to evolve in complexity and scale, addressing its **mental health impact** is no longer optional—it is a necessary step toward building a safer and more compassionate digital future.

## 2. Understanding Cyber Fraud

Cyber fraud has quietly become one of the most devastating forms of modern crime. Unlike conventional crimes, it leaves no visible scars—only a trail of financial loss, emotional trauma, and shaken trust. As the internet becomes more deeply embedded in our everyday lives, cybercriminals have found increasingly creative and deceptive ways to exploit individuals. To understand its full psychological impact, we must first explore what cyber fraud looks like today, who it affects most, and how it has evolved with rapidly advancing technology.

At its core, **cyber fraud** involves the use of digital deception to commit a criminal act—usually with the intent to steal money, sensitive data, or even one's digital identity. One of the most common types is **banking fraud**, where victims are tricked into sharing OTPs, passwords, or clicking malicious links that compromise their bank accounts. **Investment scams** have also grown

alarmingly, with fraudulent apps and fake platforms promising unrealistic returns, particularly targeting middle-class professionals seeking financial security. Then there is the disturbing rise of **sextortion**, where perpetrators threaten to release explicit images or videos unless the victim pays a ransom or complies with demands—leaving individuals emotionally shattered. **Identity theft**, meanwhile, is a silent killer of digital trust. With just a few stolen details, fraudsters can impersonate someone, apply for loans, or destroy reputations within hours.

While anyone can be targeted, certain demographics are especially vulnerable. **Young people**, who are highly active online but often unaware of cyber risks, fall prey to social engineering, phishing, and sextortion. The **elderly**, on the other hand, are often less digitally literate and more trusting, making them prime targets for banking fraud and impersonation scams. Even well-educated **professionals**—those who believe they are "tech-savvy"—are not immune. The illusion of control often backfires, as scammers deploy increasingly sophisticated tactics that mimic real-world communication with alarming precision.

The **frequency of cyber fraud cases has skyrocketed**, especially in the post-pandemic world, where online transactions have become the norm. According to cybersecurity reports, there has been a significant uptick in fraud cases involving cryptocurrency scams, job frauds, and fake online shopping platforms. This surge reflects not just a change in how crimes are committed, but a shift in how they affect people—emotionally, socially, and psychologically.

Understanding the evolving nature of cyber fraud is crucial to formulating both preventive strategies and post-incident support systems. These crimes are no longer about just stolen money—they are about **stolen peace of mind**, and their true cost lies in the lingering trauma left behind.

## 3. Psychological Impact of Cyber Fraud

Behind every news headline about cyber fraud is a real person—often overwhelmed, anxious, and emotionally bruised. The consequences of falling victim to online fraud stretch far beyond financial loss. They pierce deeply into the psyche, often triggering mental health issues such as **depression**, **anxiety**, and even **phobia** or **post-traumatic stress disorder (PTSD)**. These emotional responses are not mere by-products—they are central to the victim's experience and often linger long after the technical damage is repaired.

### Depression: The Silent Companion of Cyber Loss

One of the most common psychological outcomes of cyber fraud is **depression**. Victims who lose their savings, investments, or identity often face an overwhelming sense of **helplessness**. For many, the financial blow is not just about money—it symbolizes shattered trust, a broken sense of security, and the fear of never recovering. This leads to intense feelings of **guilt**, especially when individuals blame themselves for "falling for it," despite the increasing sophistication of cyber scams. Depression caused by cyber fraud often manifests in **social withdrawal**, where victims isolate themselves out of shame or emotional exhaustion. Many report **disturbed sleep**, persistent sadness, loss of appetite, and even **suicidal ideation**. The trauma may affect their ability to function at work or maintain relationships, leaving them trapped in a cycle of silence and suffering. Without timely intervention, this depression can evolve into a long-term mental health crisis.

### Anxiety Disorders: Living in a State of Fear

An equally debilitating effect of cyber fraud is the onset of **anxiety disorders**. Once targeted, many victims begin to live in a state of **constant fear**, worried that it could happen again. Even after changing passwords or speaking to the police, they often remain hyperaware and suspicious of every online interaction. This state of **hypervigilance**—where one is constantly on edge—can lead to **panic attacks**, sleeplessness, restlessness, and an inability to concentrate. Simple tasks like checking emails, logging into bank accounts, or answering unknown phone calls may become

sources of distress. Over time, anxiety erodes the victim's confidence and control, often interfering with daily life and work performance.

**Phobia and PTSD: When the Internet Becomes a Trigger**

In some cases, cyber fraud leaves victims with lasting **phobic responses** or symptoms consistent with **post-traumatic stress disorder (PTSD)**. A growing number of people now suffer from **cyberphobia**—a fear of using digital devices, the internet, or online services. This fear is not irrational in their minds; it is rooted in a traumatic experience where technology became the medium of betrayal. These individuals develop **avoidance behaviours**, refusing to engage in online banking, shopping, or even email communication. The result is a reduced quality of life in a world that increasingly demands digital participation. Additionally, trust becomes a major casualty. Victims may find it difficult to trust not only strangers online but also their close ones, believing that anyone could be a potential threat.

Severe forms of cyber fraud—such as **blackmail using private photos or identity abuse**—can result in **PTSD-like symptoms**, including flashbacks, nightmares, emotional numbness, and chronic fear. Victims relive the incident repeatedly, sometimes requiring trauma-focused therapy to begin healing. What makes these psychological impacts more dangerous is the **lack of awareness and support systems**. While legal procedures may be in place to address the fraud itself, few mechanisms are designed to address the mental scars left behind. Victims often do not seek help out of fear, shame, or unawareness that their suffering is legitimate and treatable.

Recognising cyber fraud as a **mental health threat**—not just a digital or legal issue—is critical. Only then can we begin to offer holistic healing that acknowledges the emotional wounds that lie behind the screens.

**4. Real-Life Case Studies**

The psychological toll of cyber fraud becomes truly tangible when viewed through the lens of real-life victims. Behind every statistic lies a story—a moment of vulnerability, a few mistaken clicks, and a world that collapses silently. These case studies, while anonymised to protect identities, reflect the deeply human cost of digital deception. They reveal how personal, professional, and social lives are disrupted—and how age, gender, and economic background influence the depth and nature of emotional impact.

**Case 1: The Young Professional Caught in a Crypto Scam**

Rohit, a 29-year-old software engineer from Bengaluru, was lured into a cryptocurrency investment scheme through a popular social media platform. The scammers impersonated financial experts and presented fake dashboards showing consistent profits. Eager to grow his savings, Rohit invested ₹4.5 lakhs—his life's savings. Within weeks, the platform vanished.

The financial loss was devastating, but the emotional impact ran deeper. Rohit experienced **acute guilt**, blaming himself for not recognising the red flags. He began avoiding conversations with family and friends, fearing their judgement. He lost focus at work, developed **severe anxiety**, and even stopped using his phone for anything beyond basic tasks. Therapy eventually helped him begin recovery, but he still struggles with trusting digital platforms.

**Case 2: Elderly Widow and Bank Impersonation**

Meera Devi, a 68-year-old widow from Lucknow, received a call from someone claiming to be a bank officer. Using clever manipulation and fear tactics, the caller convinced her to share her OTP. Within minutes, her pension account was emptied.

Already living alone, Meera felt **completely violated** and isolated. Her trust in people—and in her ability to make decisions—was shattered. She began avoiding all online activity and suffered from **cyberphobia**, refusing to use her phone or ATM card. Though her family tried to reassure her, she withdrew socially, and her **depression** grew unnoticed for months. A local NGO helped connect her with a counsellor and initiate a partial financial recovery, but her fear of technology persists.

**Case 3: College Student Trapped in Sextortion**

Priya, a 20-year-old college student, was manipulated into sharing personal photos in a romantic online chat. Soon after, she was blackmailed for money and threatened with exposure on social media. The shame and terror left her unable to attend classes or even speak to her parents. She began suffering from **nightmares, panic attacks**, and **suicidal ideation**.

Priya's case highlights how **gender and age** amplify the psychological trauma of cyber fraud. Women, especially young women, are often at greater risk of reputational harm. The mental scars from such violations are deeper, touching on identity, safety, and dignity. Only through the intervention of a college-based mental health program was Priya able to access trauma therapy and begin her long road to healing.

**5. Coping Mechanisms and Recovery**

Recovering from cyber fraud is not just about recovering lost money—it's about healing the mind and rebuilding a sense of control over life. The emotional scars left by cybercrime can last for months or even years, especially when accompanied by shame, self-blame, or isolation. Fortunately, a combination of **psychotherapy, community support, mindful digital practices, and family involvement** can significantly aid in the recovery process and help victims rediscover emotional stability.

**Psychotherapy: Rewiring the Emotional Response**

One of the most effective tools in dealing with the emotional impact of cyber fraud is **Cognitive Behavioural Therapy (CBT)**. CBT helps victims reframe negative thought patterns—such as guilt ("I should have known better") or fear ("It will happen again")—into more balanced, constructive perspectives. Victims are taught to identify irrational fears and replace them with rational coping strategies. In more severe cases, especially where trauma symptoms like flashbacks or panic attacks persist, **trauma-focused therapy** can provide deeper healing. These approaches help individuals process the event without reliving it in harmful ways. Therapists may use narrative techniques, somatic practices, or even Eye Movement Desensitization and Reprocessing (EMDR) to reduce the emotional charge associated with the cyber fraud incident.

**Support Groups and Peer Counselling: You Are Not Alone**

Many victims of cyber fraud suffer in silence because they feel ashamed or fear they won't be understood. **Peer support groups** offer a safe space for individuals to share experiences, listen to others, and feel validated. Knowing that others have been through similar ordeals and have emerged stronger can be deeply empowering. Some NGOs and mental health platforms now run **cyber fraud survivor circles** where victims can anonymously engage in group therapy or peer counselling. These platforms reduce isolation, promote mutual learning, and foster resilience—often proving as effective as individual therapy in restoring self-worth and confidence.

**Digital Detox and Mindful Technology Use**

After falling prey to online fraud, many victims experience digital anxiety—hesitating to engage in even basic online tasks. A **digital detox**, even temporarily, can be a crucial step in breaking this cycle of fear and dependence. This involves stepping away from social media, online transactions, and non-essential screen time to reset one's relationship with technology. Later, **mindful**

**technology use** can be reintroduced, where individuals are taught to use digital platforms with purpose, caution, and emotional awareness. Techniques like setting digital boundaries, using screen-time tracking apps, and cultivating non-digital hobbies support a healthier online-offline balance.

### The Role of Family and Social Support

Perhaps one of the most underrated aspects of recovery is the **support of loved ones**. A non-judgmental, emotionally available family can make all the difference. Victims who feel heard, believed, and supported tend to heal faster and are more likely to seek help early. Friends and family can also assist in practical recovery—helping report fraud, managing finances temporarily, or accompanying the victim to therapy sessions. Their empathy, patience, and encouragement often act as emotional anchors during moments of distress. Recovery from cyber fraud is a journey—not just of restoring trust in the digital world, but of **restoring trust in oneself**. With the right mix of therapeutic support and community understanding, victims can transform trauma into resilience and re-emerge stronger.

## 6. Legal and Institutional Support

When someone falls victim to cyber fraud, the immediate instinct is often panic or shame—not a structured plan for legal action or mental health support. Unfortunately, this emotional paralysis is one of the main reasons many cases go unreported, and victims suffer in silence. India has made commendable strides in building legal and institutional frameworks for cybercrime redressal, yet **awareness, accessibility, and psychological integration** remain critical gaps that must be addressed.

### Cybercrime Cells and Legal Redressal Mechanisms

India's **cybercrime ecosystem** has evolved in recent years, particularly with the launch of the **National Cyber Crime Reporting Portal (cybercrime.gov.in)**, which allows victims to file complaints digitally and anonymously. Each state and major city has dedicated **cybercrime cells**, many of which work in tandem with the local police to investigate and prosecute offences ranging from identity theft and financial fraud to cyberbullying and sextortion. Moreover, under the **Information Technology Act (2000)** and relevant sections of the **Indian Penal Code (IPC)**, several legal provisions address digital impersonation, hacking, blackmail, and financial fraud. However, navigating these systems can be daunting—especially for individuals already overwhelmed by emotional trauma. While these frameworks exist, the **on-ground reality** reveals bottlenecks: delayed responses, lack of digital literacy among police officials, and underreporting due to societal shame, particularly in cases involving women or sexual blackmail.

### Mental Health Helplines and NGO Support

Recognising the emotional damage cyber fraud inflicts, several **mental health organisations and NGOs** have stepped up. Services like **iCall (by TISS)** and **Fortis Mental Health Helpline** offer free psychological support via phone, especially for victims of cybercrime-related trauma. NGOs like **Cyber Peace Foundation** and **RATI Foundation** not only help victims report incidents but also guide them through digital safety training and emotional recovery. These institutions often act as a **bridge** between law and empathy—helping victims feel heard while guiding them through often intimidating legal corridors. However, their reach is still largely urban, with rural and lower-income communities lacking both access and awareness of such services.

### Challenges in Legal Awareness and Reporting

Perhaps the biggest obstacle is the **lack of awareness**—many victims are unaware of their rights, don't know how to file a cyber complaint, or fear being blamed. In many cases involving sextortion

or financial scams, victims hesitate to come forward due to stigma, fearing judgment from family, society, or even law enforcement. Additionally, **legal procedures are often not trauma-informed**. Victims may be asked to recount distressing experiences without psychological support, which can worsen existing anxiety or depression. Language barriers, digital illiteracy, and slow-paced legal systems further add to the pain.

### The Way Forward: Integrated Legal-Psychological Support

A more effective system would integrate **legal redressal with psychological first aid**. Every cybercrime reporting unit should have trained mental health professionals who can support victims emotionally during the complaint process. Legal literacy campaigns—especially in schools, colleges, and through vernacular media—can empower individuals to act decisively rather than freeze in fear. Moreover, collaboration between **law enforcement, psychologists, NGOs, and tech companies** can create a more empathetic and efficient cyber safety net—one that protects not just data and money, but also **the dignity and mental well-being** of every citizen.

## 7. Preventive Strategies and Public Awareness

In the battle against cyber fraud, **prevention is not just better than cure—it is essential**. While legal and psychological support play a crucial role after a crime has occurred, building a **digitally aware, emotionally resilient, and ethically guided society** is the first line of defense. From personal cyber hygiene to systemic public awareness campaigns, the key to reducing cyber fraud lies in **equipping individuals with knowledge, tools, and responsible digital behaviour**.

### Cyber Hygiene and Digital Literacy Campaigns

Just as we teach children to wash their hands to prevent illness, **cyber hygiene** must become second nature to all internet users. This includes practices like using strong passwords, enabling two-factor authentication, avoiding suspicious links, keeping software updated, and being cautious of online requests for personal or financial information. India has taken steps through initiatives like **Cyber Surakshit Bharat** and **Digital India's awareness programs**, which educate users about safe digital practices. However, these efforts must go deeper, especially at the grassroots level, using **vernacular languages, visual media, and interactive tools** to ensure inclusivity across age and literacy levels. Digital literacy needs to extend beyond technical skills to include **emotional awareness**—how to identify manipulation, resist online peer pressure, and recognise red flags like urgency, flattery, or secrecy in communication.

### Promoting Responsible Technology Use

The internet is not inherently harmful—it is how we use it that determines its impact. Promoting **responsible technology use** means encouraging people to set healthy boundaries: limiting screen time, avoiding oversharing, and verifying before trusting. This also includes promoting empathy and ethics online. Just as people are taught civic values in real life, **digital citizenship education** can instill values of respect, responsibility, and vigilance. Schools, workplaces, and families can play an active role in cultivating these attitudes.

### The Role of Schools, Workplaces, and Communities

Schools are the ideal starting point for shaping safe digital behaviour. Cyber safety modules should be integrated into regular curricula—not just as an IT lesson, but as part of **life skills and mental health education**. Roleplays, workshops, and real-life stories can make these lessons engaging and memorable. Workplaces, too, can contribute by conducting regular **cybersecurity training**, including information on phishing scams, safe handling of data, and mental health resources in case of fraud. Community centers, self-help groups, and local government bodies must act as

**information hubs**, particularly for vulnerable populations like the elderly, women, and small business owners.

### Media as a Double-Edged Sword

The media—both traditional and digital—has immense potential to **spread awareness** about cyber threats, legal recourse, and recovery mechanisms. Television campaigns, radio jingles, and social media influencers can be powerful tools in normalising conversations around cyber fraud and mental health.

However, media must also act with **sensitivity toward victims**. Sensationalism or victim-blaming can deter others from reporting crimes. Journalists and platforms must adhere to ethical guidelines that protect the dignity and privacy of those affected.

## 8. Conclusion

In an age where our lives are increasingly lived online—through banking apps, social media profiles, digital wallets, and remote work—the **threat of cyber fraud has become a deeply personal issue**, not just a technological one. The growing frequency and sophistication of such crimes, combined with the psychological wounds they leave behind, reveal a disturbing truth: **cyber fraud is not just a financial crime, but a mental health crisis in disguise**. Victims often endure far more than monetary loss. As this article has explored, they grapple with shame, fear, paranoia, helplessness, and in some tragic cases, even suicidal ideation. Depression, anxiety, phobias, and post-traumatic stress are not rare outcomes—they are common, underreported consequences of what can appear on the surface as a "digital" offence. The emotional cost is compounded by **social stigma, lack of awareness, and a poorly integrated support system**. Yet this need not be our reality. India and many other nations have begun to take steps in the right direction—establishing cybercrime cells, launching mental health helplines, and promoting digital literacy. But these efforts are often fragmented and **fail to address the deep emotional needs of victims**. A more humane, holistic approach is necessary—one that sees the cyber fraud victim not just as a complainant, but as a person in need of both **legal justice and emotional healing**.

At the heart of this solution lies **integration**. Legal frameworks must work in tandem with psychological care. Cybercrime helplines should offer trauma-informed responses. Police personnel must be sensitised to deal with victims empathetically, especially in cases involving blackmail or sextortion. Schools should not only teach cybersecurity but also emotional resilience in digital spaces. Communities, workplaces, and media must foster environments that encourage reporting without shame and offer solidarity rather than suspicion. Furthermore, **preventive strategies** rooted in education, ethical digital behaviour, and cyber hygiene can create a generation of informed, cautious, and emotionally grounded netizens. We must shift the narrative from fear of technology to **respectful, responsible engagement** with it.

There is also a moral imperative here—to **protect the most vulnerable**: the elderly who may fall for phishing emails, the youth who may overshare personal data, or professionals whose digital identities can be exploited. Ensuring their safety is not just the job of governments or cybersecurity firms—it is a **collective societal responsibility**. Ultimately, the fight against cyber fraud is not only about codes and algorithms; it's about **compassion, care, and consciousness**. We must build a digital ecosystem where people feel safe not only because firewalls protect them, but because the society behind those screens supports them. A world where technology connects us must also be one where **human empathy sustains us**.

## Reference:

1. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and*

*cyber-attacks during the pandemic*. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

2. Cross, C., & Blackshaw, D. (2021). *Cybercrime and mental health: Impact, support, and prevention*. International Journal of Cyber Criminology, 15(1), 68–82. https://doi.org/10.5281/zenodo.4641671
3. Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2020). *The aftermath of fraud victimization: Examining psychological distress and coping*. Criminal Justice and Behavior, 47(5), 551–568. https://doi.org/10.1177/0093854819892025
4. Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and Their Victims*. Routledge. https://doi.org/10.4324/9781315670101
5. .Perri, F. S., & Lichtenwald, T. G. (2020). *Cognitive behavioral therapy as a treatment for fraud victimization trauma: A case study approach*. Journal of Forensic Psychology Practice, 20(3), 239–253. https://doi.org/10.1080/15228932.2020.1778123
6. Cross, C., Richards, K., & Smith, R. (2016). *Improving the support for cybercrime victims: Learning from fraud victims' experiences*. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(4), Article 5. https://doi.org/10.5817/CP2016-4-5
7. Sharma, R., & Dhawan, S. (2021). *Bridging the gap between cyber law and mental health: A psychosocial approach to cybercrime victim support in India*. Journal of Law and Mental Health, 14(2), 35–52. https://doi.org/10.2139/ssrn.3892041
8. Indian Council for Research on International Economic Relations (ICRIER). (2020). *Mapping the gaps: India's cybercrime ecosystem*. Retrieved from https://icrier.org/pdf/India_Cybercrime_Report_2020.pdf
9. Bada, A., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber hygiene in the digital age: Preventive strategies and education*. Computers & Security, 83, 353–367. https://doi.org/10.1016/j.cose.2019.02.010
10. Ministry of Electronics and Information Technology (MeitY). (2022). *Cyber Surakshit Bharat: A framework for digital safety and awareness*. Retrieved from https://www.meity.gov.in
11. Hadlington, L. J. (2021). *Cybercrime and mental health: Understanding the psychological consequences of online victimisation*. In T. J. Holt (Ed.), **The Palgrave Handbook of International Cybercrime and Cyberdeviance** (pp. 835–850). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-23665-8_43
12. National Crime Records Bureau (NCRB). (2023). *Cyber Crime in India: Annual Statistics Report*. Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in