

Mental Resilience and Psychological Vulnerability: Examining Protective Factors Against Cyber Scams

¹G. Amalarakkini, ²Dr. Shirley Moral C

¹PhD. Research Scholar, Department of Education, Madurai Kamaraj University, Madurai.

²Assistant Professor, Department of Education, Madurai Kamaraj University, Madurai

Abstract: Online fraud keeps growing, and so does the damage it leaves behind. The financial side of that damage gets counted; the psychological side usually does not. In this paper we look at two constructs that pull in opposite directions when a person encounters a scam. The first is psychological vulnerability, a mix of traits such as poor self-worth, impulsive decision-making and earlier mental health difficulties, which raises the chance of being deceived and worsens what follows. The second is mental resilience, the capacity to absorb the shock, steady oneself and act to limit further harm. Drawing on recent studies of scam victims, we bring together what is known about the factors that protect people: emotional intelligence, self-control, self-esteem, supportive relationships and digital literacy. We also weigh the formal responses available, from cognitive restructuring and trauma counselling to newer digital mental health services built around artificial intelligence. Our reading of the evidence is that no single measure works on its own. Prevention has to run through individuals, communities and institutions at the same time, backed by mental health education, accessible victim support, early screening and cooperation across sectors. The paper closes with a research agenda, arguing that longitudinal work and proper evaluation of interventions are the two steps most needed if the emotional cost of cyber fraud is to be brought under control.

Keywords: Cyber scams; psychological vulnerability; mental resilience; emotional distress; emotional intelligence; victim support.

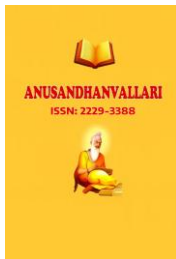
1. Introduction

Fraud has moved online, and it has moved fast. People are now targeted through websites, mobile apps, phone calls and text messages in nearly every country, and the schemes themselves grow more convincing each year. The COVID-19 period accelerated this shift because so much of daily life, from banking to shopping to simply staying in touch, migrated onto digital channels in a very short time. What the pandemic years also revealed, though far less visibly, is that the harm from these crimes does not stop at the bank balance (Balcombe, 2025).

People who are scammed describe a wide range of after-effects. Depression and anxiety appear frequently in the literature, alongside shame, embarrassment, post-traumatic stress reactions and a gradual withdrawal from social life. Rangappa (2025) In many accounts these problems last much longer than the financial loss itself. They are made worse by the stigma of having been fooled, and by how hard it can be to find psychological or institutional help that actually fits the situation. Trust suffers too, both trust in online spaces and trust between people (Balcombe, 2025; Kemp & Erades Pérez, 2023).

Some of the recent findings are stark. Victims report sleepless nights, constant rumination and a deep sense of being alone with the problem. A portion end up on psychotropic medication or in the care of mental health professionals. Yet many never seek help at all. Patel (2025) Self-blame gets in the way, and so does the fear of being judged, which also explains why so few incidents are ever reported to the authorities (Balcombe, 2025; Shi et al., 2023).

This paper takes up the psychological side of scam victimization. Our particular interest is mental resilience, understood as the capacity that lets some people recover from these experiences while others remain stuck in distress. We also look at the other side of the coin: psychological vulnerability, expressed through emotional



fragility, biased thinking and pre-existing mental health problems, which appears to raise both the risk of being deceived and the severity of the fallout afterwards (Pant & Chaubey, 2024).

Four questions guide the discussion. How exactly does resilience protect against the worst psychological outcomes? Which protective factors show up most consistently in the research? What would a workable set of interventions look like if it combined mental health support with cyber safety education across the individual, community and institutional levels? And what can new technology, particularly AI-supported mental health tools, realistically contribute?

There is a gap worth naming here. Cyber fraud is still treated mainly as a technical and financial problem, and the mental health consequences tend to fall through the cracks of that framing. Until that changes, resilience education and victim support will remain underdeveloped relative to the scale of the harm.

2. Conceptual Background

Two ideas anchor everything that follows. Psychological vulnerability refers to the cluster of personal and situational characteristics, such as low self-esteem, impulsivity, loneliness and a history of psychological distress, that make a person easier to deceive and harder hit once deception happens (Pant & Chaubey, 2024). Mental resilience is the opposite pole: the ability to withstand adversity, adapt to it and keep functioning (Balcombe, 2025). The two are related but not mirror images. Someone can carry several vulnerability factors and still show real resilience when the right support is in place. That is precisely why resilience can be built, and why building it matters.

One theoretical lens is particularly useful for making sense of what victims go through. Shattered Assumptions Theory holds that traumatic events break a person's basic beliefs about the world being safe and predictable. Applied to online fraud, the theory explains something victims often describe: the digital environment they used every day without a second thought suddenly feels hostile, and that feeling of lost safety can spread into offline life as generalized fear and mistrust (Pant & Chaubey, 2024). Seen this way, recovery is never just about getting money back. It is about rebuilding a sense of safety, control and self-worth that the scam took away.

3. Psychological Vulnerability and Its Consequences

In the context of cyber scams, psychological vulnerability means a heightened openness to emotional and cognitive harm. It grows out of several factors acting together: fragile self-esteem, an impulsive decision style, earlier episodes of distress, and dispositional tendencies toward anxiety or depression. These same factors often cloud judgment at the moment the scam is unfolding. Fraudsters know this and design their approaches around emotional pressure and mental shortcuts (Pant & Chaubey, 2024).

What follows victimization is a familiar cluster of symptoms. Shame and embarrassment come first for many people. Sleep suffers. Anxiety and repetitive worry set in, and mood drops. Underneath all of it sits a double injury, because the victim has lost money and lost trust at the same time. A large share of victims turn the blame inward, and that self-recrimination deepens the distress, pushes them away from other people and makes them far less willing to talk about what happened (Pant & Chaubey, 2024).

Stigma multiplies the damage. The fear of looking naive or careless keeps victims from asking for help, and untreated distress lasts longer than it needs to. The judgment does not always come from strangers either. Studies from Singapore found victims facing blame within their own families, which left them feeling even more isolated (Shi et al., 2023). The reluctance to disclose hurts recovery twice over: it delays professional care, and it cuts people off from the everyday social support that is itself protective.

There is also the deeper disruption described in the previous section. Consistent with Shattered Assumptions Theory, victimization can unsettle basic beliefs about safety and control, so that an ordinary digital routine

becomes a source of threat and the resulting mistrust lingers well beyond the incident (Pant & Chaubey, 2024). Psychological injury and social withdrawal feed each other in a loop. Breaking that loop requires interventions that work on the emotional and the social side at once.

4. Mental Resilience as a Protective Mechanism

Resilience is the capacity to take a hit, whether stress, trauma or loss, and return to normal functioning, sometimes with new coping skills gained along the way. For scam victims, resilience shows up as the ability to process the deception constructively instead of spiraling into rumination. Negative feelings are contained, emotional balance is held, and recovery gets underway (Balcombe, 2025).

Several ingredients feed this capacity. Emotional intelligence lets people recognize and regulate what they are feeling, which blunts the panic responses that scammers deliberately try to trigger. Desai (2024) Self-efficacy, the belief in one's own ability to act, encourages checking a suspicious claim rather than freezing or complying. Adaptive coping skills give structure to the recovery: problem-focused strategies, mindfulness practice and cognitive restructuring all help a person work through stress rather than be worked over by it. And relationships matter enormously. Family, friends and colleagues supply reassurance and practical guidance, and both make a measurable difference to how recovery goes (Pant & Chaubey, 2024; Balcombe, 2025).

Resilience changes behaviour, not just feelings. People with stronger resilience are more likely to take protective steps after a scam: verifying information online, consulting sources they trust, reporting the incident and adjusting their digital habits so the same thing cannot happen again easily (Balcombe, 2025). In other words, resilience works on two fronts. It shields mental health from deterioration, and it turns a bad experience into more careful behaviour going forward.

Given how heavy the mental health toll of scams can be, we would argue resilience is the single most important asset an individual can hold in this domain. The practical lesson follows directly: resilience-building should sit inside cyber awareness and victim support programmes, not alongside them as an afterthought.

5. Protective Factors Against Online Fraud

Research on cybercrime victimization points to a fairly consistent set of protective factors, ones that lower the odds of falling for fraud in the first place and soften the psychological blow when prevention fails. Self-esteem, self-control and emotional intelligence lead the list. Together they help people manage emotional pressure, resist impulsive choices and hold onto a stable sense of self that offenders find harder to exploit (Zych et al., 2024).

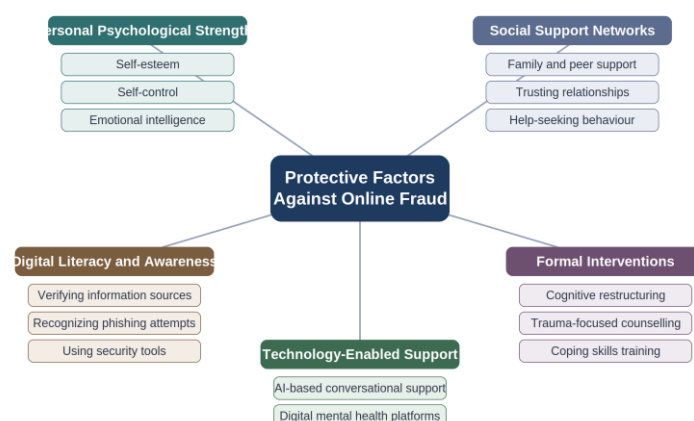


Figure 1. Protective factors against online fraud.

Social bonds form a second layer. Trusting relationships act as a safety net: they ease isolation, make asking for help feel normal, and give victims the confidence to say what happened to them. Across the studies reviewed by Zych et al. (2024), the presence of such relationships consistently softened the effects of cyber victimization and supported the return of resilience.

A third layer is behavioural. Awareness, digital literacy and simple risk management habits, such as checking where information comes from, spotting phishing attempts and using basic security tools, all reduce exposure. People with higher digital literacy are victimized less often, for the straightforward reason that they recognize and disengage from deceptive approaches earlier (Balcombe, 2025).

When prevention fails, formal help becomes the priority. Cognitive-behavioural work, and cognitive restructuring in particular, helps victims replace beliefs like pervasive self-blame or blanket mistrust with healthier appraisals. Trauma counselling addresses the heavier consequences, including anxiety, depression and post-traumatic stress, and has proved central to lasting recovery (Balcombe, 2025).

Technology now belongs in this picture as well. AI-based conversational tools can offer psychological support on demand and at scale: an empathetic first point of contact, guidance on safer practices, and help managing acute distress. Digital platforms of this kind get around three of the classic barriers to care, namely stigma, cost and distance, and they can route people toward professional services when the situation calls for it (Balcombe, 2025).

Reading these findings together, one conclusion stands out. Protection is layered. Personal strengths, supportive relationships, informed habits and accessible services reinforce each other, and none is sufficient alone. Resilience against online fraud is better understood as a property of a person's whole environment than as a trait carried around in isolation.

6. Building Resilience: Multi-Level Prevention Strategies

Because the harm from cyber fraud is psychological, social and systemic all at once, prevention has to operate on several levels at the same time. Measures confined to a single level leave predictable gaps. What victims and at-risk groups need is a coordinated structure that runs from the individual through the community up to institutions, with early identification threaded through the whole.

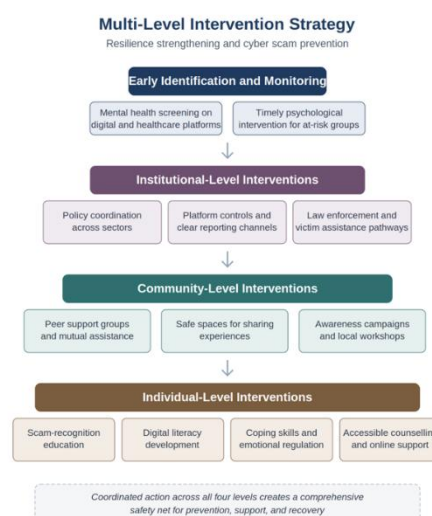


Figure 2. Multi-level interventions for resilience-building and cyber scam prevention.

6.1 Individual-Level Interventions

At the individual level, the work starts with education. Training in scam recognition and digital literacy gives people the tools to spot manipulation before it costs them anything. Coping skills sit alongside this: emotional regulation, mindfulness, stress management and cognitive-behavioural techniques all strengthen the psychological reserves a person can draw on if victimization happens anyway. Counselling should be easy to reach, including online, so that victims can process the experience and gradually rebuild their confidence in digital spaces.

6.2 Community-Level Interventions

Communities carry a load that formal services cannot. Peer support groups and moderated safe spaces let victims speak without fear of judgment, learn from one another and pick up practical advice on avoiding repeat victimization. These settings work directly against the isolation that scams so often produce. Local awareness campaigns and workshops push the effect outward, building vigilance and mutual support into the surrounding community.

6.3 Institutional-Level Interventions

Institutions set the frame within which everything else happens. Policy should require coordination among technology companies, healthcare providers, law enforcement and mental health services, because a defence assembled across sectors covers ground that no single sector can. Work from the banking industry points the same way: fraud prevention succeeds when risk management, detection and response are treated as one connected system rather than a set of separate controls (Barik & Singh, 2025). Platform operators have their own part to play, through controls that limit the spread of scam content and reporting channels simple enough that people actually use them.

6.4 Early Identification and Continuous Monitoring

Catching problems early changes outcomes. Screening built into digital platforms and healthcare settings can flag at-risk individuals and recent victims before distress becomes entrenched, opening the door to timely psychological support. Folding resilience training into wider cyber awareness campaigns has a similar long-run effect, since it leaves people with durable skills for a threat environment that will keep evolving whether we prepare for it or not.

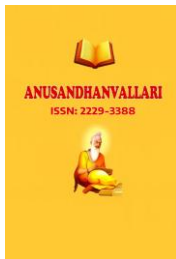
The strategy sketched here is deliberately layered. It treats the psychological, social and technological dimensions of scam harm as parts of one problem, which is what they are.

7. Discussion and Future Directions

The evidence reviewed in this paper points to a simple imbalance. The financial cost of cyber fraud is measured, reported and acted upon; the psychological cost is mostly not. Prevention policy reflects this, leaning heavily on technical controls and enforcement while victim mental health remains an afterthought. Correcting the imbalance means treating mental health as a first-order objective of anti-fraud strategy, not a footnote to it.

The evidence base itself has limits that should be acknowledged. Most available studies are cross-sectional, so claims about what causes what, between vulnerability, victimization and psychological outcome, rest on weaker ground than one would like. Samples tend to come from single countries, and stigma, family dynamics and help-seeking norms differ enough across cultures that generalization is risky. Evaluations of interventions are thin, and thinnest of all for the newer AI-based support tools, where claims about scalability have run ahead of actual outcome measurement.

The research agenda follows from these gaps. Longitudinal designs are needed to trace psychological trajectories from pre-existing vulnerability through the acute aftermath and into long-term adjustment. Cross-cultural



comparisons would show how disclosure norms and stigma shape recovery in different settings. Controlled trials should test both the conventional interventions, meaning cognitive-behavioural therapy, trauma counselling and peer support, and the technological ones, meaning AI-driven chat support and digital screening, to establish what works, for whom and at what cost. One further step would help policymakers directly: building mental health outcome measures into cybercrime reporting systems, so that the scale of the psychological problem finally becomes visible in official data.

8. Conclusion

The argument of this paper can be stated briefly. Mental resilience is the main line of defence against the psychological harm of cyber scams. It allows people to recover from victimization and hold onto their wellbeing. Psychological vulnerability works the other way, turning low self-esteem, prior mental health difficulty and emotional sensitivity into a higher risk of anxiety, depression and social isolation after a scam (Balcombe, 2025; Pant & Chaubey, 2024).

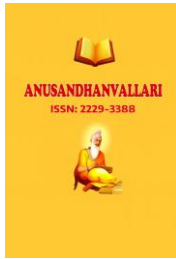
The investment case is clear. Mental health education, accessible support services and resilience-building technologies all deserve far more attention than they currently receive. Digital tools, especially AI-driven conversational support and trauma-informed platforms, can reach victims who would never walk into a clinic because of stigma, and can do so anonymously and at scale (Balcombe, 2025). Peer support and structured coping skills training round out the picture on the human side.

Research should now concentrate on two things: longitudinal studies of how the psychological effects of scams evolve, and rigorous evaluation of interventions across both psychological and technological forms. Just as important is the integration of mental health thinking into cyber prevention and awareness programmes, so that protection covers emotional harm and not only financial loss.

Cyber fraud is not going away. But a society that combines education, social support, sensible policy and well-designed technology can blunt its effects considerably, and can make sure that the people it reaches anyway are not left to recover alone.

References:

- [1] Balcombe, L. (2025). The mental health impacts of internet scams. *International Journal of Environmental Research and Public Health*, 22(6), 938. <https://doi.org/10.3390/ijerph22060938>
- [2] Barik, T. R., & Singh, C. B. (2025). 360-degree approach to cyber risk management as a strategic tool for fraud detection and prevention in banking. *Bank Quest*, 96(1), January–March, 37–48.
- [3] Desai, A. U. (2024). A Review of the Applications of Machine Learning in Cybersecurity and its Challenges. *Journal of Digital Security and Forensics*, 1(1), 26–29. <https://doi.org/10.29121/digisecforensics.v1.i1.2024.17>
- [4] Kemp, S., & Erades Pérez, N. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health*, 20(7), 5404. <https://doi.org/10.3390/ijerph20075404>
- [5] Pant, R., & Chaubey, U. (2024). Protecting minds in the digital age: A review based study on psychological impact of cybercrime. *International Journal of Indian Psychology*, 12(3), 2240–2247. <https://doi.org/10.25215/1203.220>
- [6] Patel, N. (2025). Polygraphy as a Tool for Forensic Psychological Evaluation in Cases of Workplace Harassment: Advances and Ethical Concerns. *Journal of Digital Security and Forensics*, 2(2), 50–57. <https://doi.org/10.29121/digisecforensics.v2.i2.2025.66>



-
- [7] Rangappa, A. S. (2025). Agentic AI and Cyber Security: Autonomous Threat Hunting, Intrusion Detection, and Adaptive Defense Mechanisms in A World of Increasingly Sophisticated Cyber Attacks. *Journal of Digital Security and Forensics*, 2(1), 128–138. <https://doi.org/10.29121/digisecforensics.v2.i1.2025.86>
- [8] Shi, J., Burton, J., & Ekberg, J. (2023). Unveiling the unseen wounds—A qualitative exploration of the psychological impact and effects of cyber scams in Singapore. *Social Sciences*, 12(4), 515. <https://doi.org/10.3390/socsci12040515>
- [9] Zych, I., Baldry, A. C., Farrington, D. P., & Latzman, R. D. (2024). Umbrella review of meta-analyses on the risk factors, protective factors, consequences and interventions of cyberbullying victimization. *Nature Human Behaviour*. <https://doi.org/10.1038/s41562-024-02011-6>