JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 1 (Jan.-Mar.) | 2026 Art. 05

From Victimisation to Recovery: A Victim Centered Pathway of Cybercrime Harm and Response in Tamil Nadu

Prabha A
PhD Scholar, Department of Criminology and Criminal Justice,
Manonmaniam Sundaranar University, India

Prof. (Dr.) Beulah Shekhar
Adjunct Professor,
Department of Liberal Arts, Parul University, India

Ameenul Abdullah K S
PhD Scholar, Division of Criminology and Forensic Sciences,
Karunya Institute of Technology and Sciences, India

Recommended Citation
Prabha A, Prof. (Dr.) Beulah Shekhar, Ameenul Abdullah K S, *From Victimisation to Recovery: A Victim Centered Pathway of Cybercrime Harm and Response in Tamil Nadu*, 1 JILPS 68-89 (2026).
Available at www.jilps.in/archives/.

This Article is brought to you for free and open access by the Journal of International Law, Politics and Society by an authorized Lex Assisto & Co. administrator. For more information, please contact jilpslawjournal@gmail.com.

From Victimisation to Recovery, A Victim Centered Pathway of Cybercrime Harm and Response in Tamil Nadu

Prabha A
PhD Scholar, Department of Criminology and Criminal Justice,
Manonmaniam Sundaranar University, India

Prof. (Dr.) Beulah Shekhar
Adjunct Professor,
Department of Liberal Arts, Parul University, India

Ameenul Abdullah K S
PhD Scholar, Division of Criminology and Forensic Sciences,
Karunya Institute of Technology and Sciences, India

Manuscript Received	Manuscript Accepted	Manuscript Published
10 Dec. 2026	15 Jan. 2026	21 Jan. 2026

ABSTRACT

Cybercrime victimisation is often treated as a single incident, yet victims experience it as a process that produces layered harms and requires time sensitive response. This study presents qualitative findings drawn from a larger survey of cybercrime victims across three districts in southern Tamil Nadu, Tirunelveli, Tuticorin, and Kanyakumari. A total of 80 open ended narratives were analysed using an iterative thematic approach in Atlas.ti, based on three prompts addressing incident experience and impact, first hours response priorities, and institutional improvement expectations. Themes indicate that cybercrime commonly unfolds through staged tactics such as deception, impersonation, urgency, and coercive persistence, sometimes extending into harassment, blackmail, or continued intimidation. Victims reported multi domain harms including financial and banking disruption, psychological distress and fear of judgement, stigma related social withdrawal, and long term disruption of trust, privacy, and perceived digital safety. Victims repeatedly described the first few hours as the make or break window. In that time, they wanted help that is quick and practical, stopping the damage from spreading, saving whatever evidence is available, reporting early and getting the case to the right people without delay, securing accounts immediately, and leaning on trusted family or friends for support instead of handling everything alone. Stronger technical safeguards and platform controls, prompt and coordinated response, courteous victim care and clear guidance, case tracking and feedback, and prevention-focused public awareness were the main system-level *recommendations. Based on these integrated themes, this study proposes a Victim Pathway Model of Cybercrime Harm and Response linking offender tactics, layered harms, first hours actions, institutional response quality, and recovery outcomes. The results indicate very useful, real-world lessons. They can be transformed into a victim-informed checklist for the initial hours following an attack, along with explicit, institution-specific action items that assist teams in responding more quickly, providing greater victim support, and managing cybercrime cases more skilfully.*

KEYWORDS

Cybercrime Victimisation, Thematic Analysis, Institutional Response, First Hours Response, Victim Pathway Model Reporting, Tamil Nadu

1. INTRODUCTION

Cybercrime has evolved from a specialized threat to a widespread victimization issue that affects social media, messaging apps, banking, and regular internet use. Cyber victimization is not a single type of crime, according to victim survey statistics. It cuts across several forms, like online shopping scams, payment and banking fraud, malware and hacking, and technology enabled threats or harassment. These tendencies vary from person to person and manifest in quantifiable ways across various populations. The prevalence shifts depending on the offence type and how people are exposed, for example how they shop, bank, communicate, and use devices online (Reep van den Bergh & Junger, 2018). At the same time, cybercrime is not experienced as a single moment. It usually plays out like a chain of moments rather than a single event. It starts with a first point of contact, then grows through deception or coercion, and keeps going through repeated messages, unauthorised access, and the fear that the person will misuse things again. Seeing it as a process matters because victims are often forced to make high stakes decisions while panicking, and at the same time the evidence is delicate, it can be deleted quickly or become hard to trace and recover (Curtis & Oxburgh, 2023).

A second reason cybercrime requires a victim centred lens is that harm is rarely limited to financial loss alone. Research on online fraud victims highlights that monetary loss frequently coexists with emotional distress, self-blame, disrupted relationships, and practical burdens such as time spent on remediation and repeated contact with institutions (Cross et al., 2016). Victims also report longer term effects, including privacy anxiety, reduced trust in platforms, and avoidance of online services. These harms can shape whether a victim discloses the incident to family, seeks help, or disengages from formal reporting altogether. In policing contexts, reviews note that delayed reporting is common and is influenced by perceived police capability, victim confidence in the likelihood of action, and uncertainty about where and how to report cyber offences (Curtis & Oxburgh, 2023).

Under reporting is therefore a key challenge in cybercrime response. Studies of reporting decisions show that victims weigh perceived seriousness, expected outcomes, convenience, and prior experiences with authorities, and that reporting may be directed to organisations other than police, such as banks or platform channels, depending on offence type and victim expectations (van de Weijer et al., 2020). This creates a practical problem for criminal justice systems because delays reduce traceability, weaken evidentiary value, and can increase the likelihood of repeat victimisation. It also creates a victim support problem because silence and delayed help seeking can intensify distress and prolong uncertainty. Work on reporting experiences in online fraud further shows that victims often want clearer guidance, more supportive handling, and more consistent updates on case progress, not only a formal acknowledgement that a complaint was filed (Cross et al., 2016).

These facts have influenced India's national reporting and response systems, particularly with regard to financial cybercrime. The National Cyber Crime Reporting Portal enables citizens to submit complaints online and upload supporting details, and the national helpline 1930 is designed for rapid reporting of financial cyber fraud so that action can be initiated quickly with relevant stakeholders (I4C, n.d.; National Cyber Crime Reporting Portal, n.d.). The Indian Cyber Crime Coordination Centre, established by the Ministry of Home Affairs, explicitly positions itself as a coordination framework to support law enforcement agencies and stakeholders in responding to cybercrime in a comprehensive manner (I4C, n.d.). Policy communication also emphasises early reporting as a practical necessity in financial cyber fraud cases because the chance of containment and recovery is time sensitive (I4C, n.d.; National Cyber Crime Reporting Portal, n.d.). Even with these systems, there remains a gap in empirically grounded, district level evidence that captures cybercrime as a lived victim pathway. Much existing guidance is institution authored and focuses primarily on procedural steps. Fewer studies integrate three elements in one victim voiced account, the progression of victimisation tactics, the layered harms that follow, and the first hours priorities and institutional expectations that victims themselves identify. Victim narratives are especially useful here because they reveal the logic of escalation, the role of stigma and fear of judgement, and the practical constraints that shape containment, evidence capture, and reporting decisions.

This paper addresses that gap through a thematic analysis of open ended survey narratives collected across three districts in southern Tamil Nadu, Tirunelveli, Tuticorin, and Kanyakumari. The parent survey included 180 participants, and the qualitative dataset for this paper comprises 80 narrative responses to three prompts, describing what happened and its effects, what victims should do in the first hours, and what improvements victims expect from police, banks, platforms, and government. The aim is to develop a victim centred pathway model that links victimisation tactics to multi domain harms, connects harms to first hours priorities, and synthesises system level recommendations that can strengthen victim support, improve reporting pathways, and enhance institutional responsiveness.

2. LITERATURE REVIEW

Cybercrime victimisation is now widely recognised as a form of harm that extends beyond money loss. Reviews of victim survey research show that cyber enabled offences produce mixed and layered consequences, including financial loss, disruption of daily routines, emotional distress, and long term changes in online behaviour such as avoidance and heightened vigilance (Reep van den Bergh & Junger, 2018). Recent evidence also suggests that psychological impact varies substantially by both personal factors and incident circumstances, so two victims experiencing similar scams can report very different levels of distress, fear, or loss of control (Borwell et al., 2025). This matters for qualitative work because narrative accounts can reveal how victims interpret the incident, how shame or uncertainty shapes disclosure, and why certain harms persist even after financial containment.

A consistent theme across the literature is under reporting and delayed reporting, driven by a combination of emotional barriers and institutional expectations. A systematic review focused on the UK concludes that cybercrime is underreported and that reporting decisions are shaped by trust in police, perceived usefulness of reporting, convenience, and misunderstandings about which agency can act, with victims often uncertain about the right reporting channel or sceptical about outcomes (Sikra et al., 2023). Studies on internet fraud that concentrate on victims paint a similar pattern. People say the damage goes beyond just losing money; it also affects relationships, emotions, and self-esteem. Many also explain why they hesitate to report. They feel embarrassed, worry they will be blamed, and get discouraged by reporting systems that feel scattered, confusing, and slow, with very little feedback about what happens after they file a complaint (Cross et al., 2016). This is echoed by policing-focused evaluations, which point out that victims may put off reporting because they believe law enforcement is incapable or won't act appropriately, which further degrades the quality of the evidence and limits prospects for prompt intervention (Curtis & Oxburgh, 2023).

However, studies on reporting behavior reveal something unsettling but significant. Victims may decide not to report at all or to remain silent the next time if they believe the police's response is ineffective. According to survey results, many victims of cybercrime are unhappy with the way their cases are handled, and they frequently cite perceived indifference or delay as a major deterrent to reporting (van de Weijer et al., 2020). Even when cases involve technology facilitated harassment or coercion, delayed reporting can trigger credibility judgements and victim blaming attitudes among responders, which can intensify secondary victimisation and reduce willingness to seek help in future incidents (Chatzisymeonidis & Pina, 2024).

More and more studies also treat the first few hours after victimisation as the key window, because cyber harms can snowball fast. Offenders often keep the victim engaged through ongoing calls or messages, trigger repeated authentication prompts to get codes or approvals, move money quickly, and lock people out of their own accounts, which makes recovery and evidence capture much harder. In India, institutional guidance foregrounds immediate reporting for financial cyber fraud through the national helpline and portal, reflecting the policy assumption that speed can increase the chances of containment and recovery (National Cyber Crime Reporting Portal, n.d.). This aligns with victim narratives in prior work that emphasise rapid containment steps, documentation of evidence, and early escalation to relevant institutions as practical coping priorities, alongside the need for emotionally supportive communication that reduces panic and self-blame (Cross et al., 2016; Curtis & Oxburgh, 2023).

Despite this growing evidence base, there remains a gap in district level, victim voiced qualitative synthesis from Indian contexts that ties together three elements in one integrated account. First, the lived sequence of cybercrime tactics and escalation. Second, the full spectrum of harms including psychological, social, and trust disruption. Third, victim defined priorities for the first hours and for institutional improvement across police, banks, platforms, and government. The thematic analysis of open ended responses from Tirunelveli, Thoothukudi, and Kanyakumari directly addresses this gap by centring victims' own language to map incident progression, harms, coping actions, and system expectations, while also enabling cross district comparison within the same analytic framework.

3. METHODOLOGY

3.1 Study design and approach

This article reports the qualitative findings drawn from a larger pragmatic mixed methods study on cybercrime victimisation in southern Tamil Nadu. The parent study used a cross sectional survey design and combined structured items with open ended questions to capture both patterned trends and lived experiences of victimisation.

3.2 Study setting

The study was conducted in three districts of southern Tamil Nadu, Kanyakumari, Tirunelveli, and Thoothukudi. Together, these districts reflect different socio economic profiles and a mix of urban, semi urban, and rural settings. This made them a useful context for capturing a wide range of cybercrime experiences and understanding how people seek help and navigate reporting pathways.

3.3 Participants and sampling

The target population comprised adults aged 18 years and above who self-identified as direct victims of at least one cybercrime incident. Inclusion criteria required participants to reside in one of the three districts and to understand English or Tamil, since the tool was administered bilingually. Individuals below 18 years, indirect victims, or those unwilling to consent were excluded to maintain ethical and analytic clarity.

Because cybercrime victims constitute a hidden population with no complete sampling frame, non-probability sampling was adopted. Recruitment used purposive and snowball approaches, with the survey link circulated through digital networks and printed forms administered through local community and institutional contacts to reach victims with varying access and comfort levels.

3.4 Sample size and qualitative dataset

The parent survey included 180 participants across the three districts. From this survey, 80 narrative responses from the open ended components form the qualitative dataset analysed in this article.

3.5 Data collection instrument and open ended prompts

Data were collected using a structured questionnaire titled “Impact of Cybercrimes on the Victims,” administered through Google Forms and printed copies. Alongside close ended sections capturing incident characteristics, reporting behaviour, and impact domains, the questionnaire included open ended items that invited participants to describe experiences in their own words.

This article analyses responses to three open ended prompts:

1. "In your own words, what happened and how did it affect you?"
2. "What steps should victims take in the first hours after such incidents?"
3. "What would you ask police, banks, platforms, or government to improve?"

3.6 Data management and analysis using Atlas.ti

All narrative responses were imported into Atlas.ti as primary documents and organised into document groups by district and prompt to support structured comparison. Analysis followed an iterative thematic approach. First, meaningful text segments were marked as quotations and assigned concise descriptive codes. Next, codes were refined through repeated reading and constant comparison across participants, with merging and splitting of codes to improve consistency and conceptual clarity. Related codes were then clustered into higher order categories, which were synthesised into final themes representing recurring patterns in victimisation tactics, harms, first hour priorities, and institutional expectations.

Atlas.ti's assisted code suggestion features were used only for preliminary organisation and retrieval support. All coding decisions, code definitions, and theme boundaries were manually reviewed and finalised by the researcher through direct verification of linked quotations, ensuring that interpretations remained grounded in participants' original accounts.

3.7 Rigour and trustworthiness

Systematic documentation and traceability throughout Atlas reinforced rigor.Ti. An audit trail from early coding to final themes was created by using memo writing to document coding guidelines, modifications, and analytical reflections. Each theme claim might be linked to specific supporting passages thanks to the connections made between quotations and codes. Code frequency views, code distribution tables, and co occurrence inspections were used to examine prominence and relationships among concepts and to check for patterns that appeared across prompts and districts.

3.8 Ethical considerations

Ethical safeguards were applied due to the sensitive nature of cybercrime victimisation. Participation was voluntary and based on informed consent. Data were anonymised and identifying details were removed.

Participant excerpts are reported verbatim where possible and attributed to pseudonyms to maintain anonymity. Participants could skip questions or withdraw at any point. Data were stored securely in password protected formats, and care was taken to minimise distress during participation, consistent with the ethical procedures described for the parent study.

4. ANALYSIS & FINDINGS

This section presents themes derived from 80 open ended narratives across Tirunelveli, Tuticorin, and Kanyakumari. Findings are organised as a victim pathway, starting with the victimisation process and harms, moving to first hours response priorities, and concluding with system level improvement expectations.

4.1 Cybercrime tactics and the victimisation process

Victims rarely described cybercrime as one sudden incident. Most narratives sounded like a step by step trap. It often began with impersonation, like a familiar brand, a courier, a bank, or even a known contact. Then came pressure, urgency, repeated calls or messages, and demands for OTPs or quick payments. The initial defeat was not the end for a number of victims. They talked of repeated messaging, threats, blackmail, and ongoing communication that sustained the terror. In general, victims reported intimidation and escalation as part of the harm, particularly when perpetrators believed they could still get in touch with the victim or their contacts.

Sextortion or honey trap threats including reputational exposure, courier impersonation involving Aadhaar references and OTP flooding, and victims alleging trade or investment fraud started with compromised accounts are examples of representative excerpts.

4.2 Financial and economic harm

Many participants reported direct monetary loss through unauthorised transactions, OTP based fraud, and investment scams. But the harm was not only the rupee amount. Victims spoke about what happened after, accounts being frozen, routine banking getting disrupted, and constant worry about further withdrawals. Due to the fact that the money involved was necessary for daily necessities, home savings, or educational expenses, a number of occurrences were classified as severe. These narratives demonstrate that economic injury encompasses both immediate loss and disruption of financial operations, which exacerbates anxiety and unease.

4.3 Psychological and emotional impact

A strong pattern across narratives was emotional distress. Victims described fear, anxiety, anger, shame, confusion, and helplessness. The emotional burden often came from not knowing what would happen next, whether personal data would be misused, and whether the situation would escalate. Numerous testimonies indicated that self-blame and fear of being judged influenced disclosure choices and seeking assistance. Victims reported severe emotional repercussions from perceived humiliation and loss of control even in cases when loss was minimal, indicating that the psychological toll of cybercrime is not exclusively dependent on monetary loss.

4.4 Social and relational impact and stigma

For many, victimisation spilled into their social world. Some described being mocked or judged by peers. Others withdrew before anyone could comment, to avoid gossip or embarrassment. Reduced internet activity, altered posting habits, and damaged relationships with friends and family were among the narratives. This topic emphasizes how reputational worry can become harmful in and of itself, influencing coping mechanisms and possibly making isolation worse during the healing process.

4.5 Trust, privacy, and digital safety disruption

Many victims described a longer term shift in how safe the digital world felt. They reported heightened vigilance, privacy concerns, fear of identity misuse, and reduced confidence in online platforms and services. Some accounts framed victimisation as a turning point that led to stronger privacy settings and more cautious online behaviour. Beyond strangers, perceived flaws in the mechanisms meant to safeguard accounts, data, and financial transactions also contributed to the decline in confidence.

4.6 Coping, help seeking, and recovery actions

Victims described a wide range of responses. Some acted quickly, blocking offenders, freezing bank accounts, preserving evidence, informing family, and trying to file complaints. Others moved into withdrawal, uninstalling apps, reducing platform use, or avoiding online activity. It is evident that healing involves both social and technological aspects. These trends demonstrate that recovery is both social and technological, and that victims' perceptions of institutional support affect whether or not they seek official assistance.

4.7 First hours priorities after cybercrime

4.7.1 Immediate containment and loss prevention

Victims kept coming back to one core idea, the first few hours decide how far the damage spreads. They talked about cutting off contact right away, blocking numbers and accounts, refusing to share OTPs or send more money, and taking quick steps to stop the situation from escalating. Panic and haste are seen as exploitable vulnerabilities in the early stages, as seen by the victims' advice to remain composed in order to prevent rash actions.

4.7.2 Evidence preservation and documentation

Another strong priority was saving proof before it disappears. Victims mentioned screenshots, chat threads, call logs, transaction details, emails, and suspicious links. The message was simple, evidence can vanish fast, and waiting makes recovery and action harder. This theme underlines the practical reality that victims often carry the responsibility of preserving digital evidence before institutional processes begin.

4.7.3 Reporting and escalation pathways

Early reporting was described as necessary, even when people felt embarrassed or worried about being judged. Victims recommended using the right routes quickly, cyber helplines or cyber cells, official portals, and immediate escalation to banks to contain transactions. This topic demonstrates an understanding that timely reporting can stop further damage and that traceability and recovery are time-sensitive.

4.7.4 Account security and cyber hygiene actions

Alongside reporting, victims described instant account protection steps, securing compromised accounts, changing passwords, tightening privacy settings, and avoiding unknown links. These steps were presented as essential for preventing future exposure as well as for preventing recurrent victimization, implying that victim education and behavior modification start as soon as the incident occurs.

4.7.5 Emotional stabilisation and social support

Many victims described the early hours as emotionally fragile. They advised reaching out to trusted people, family, close friends, or someone who can help think clearly, and not staying alone with the stress. A smaller fraction indicated mistrust or unhappiness with the institutional reaction, suggesting that victims' decision to approach the police or not may be influenced by formal agencies' supportive communication.

4.7.6 Follow up, legal recourse, and system navigation

For victims, early response did not end with filing a complaint. They expected guidance on what happens next, how to track the case, and what steps to take if the problem continues. According to this topic, victims define "early response" as obtaining explicit communication and tangible action in addition to registering a complaint.

4.8 Institutional improvement expectations

4.8.1 Faster and coordinated response

Because delays give criminals more time to escalate and transfer money, victims have repeatedly requested speed from police, banks, and reporting platforms. Some also mentioned operational obstacles and delays, such slow follow-up or portal problems, implying that responsiveness is essential to system confidence.

4.8.2 Respectful handling and clear victim communication

Many recommendations were about how victims are treated. They wanted empathy, a non judgemental approach, clear instructions, and transparent updates. They also emphasized the need to prevent victim blaming and reduce secondary victimisation during reporting and follow up.

4.8.3 Stronger technical safeguards and monitoring

Victims called for better fraud detection, stronger verification, improved transaction monitoring, and more security features on platforms. A number of them also emphasized the necessity for cybercrime response units to have more technological capability, particularly better forensic and investigative support. Stronger controls over areas that facilitate scams, harassment, and exploitation, as well as quicker removal of phony websites and scam accounts, were frequently requested.

4.8.4 Stronger regulation and deterrence

Victims called for stricter cyber laws and stronger enforcement. Their suggestions placed a strong emphasis on accountability and deterrence, reflecting the idea that insufficient penalties let criminals keep pursuing victims. Lastly, victims have continuously advocated for useful public education on how to recognize scams, safer online practices, and straightforward advice that others may take to avoid becoming victims.

4.8.5 **Integrated interpretation**

Taken together, victims framed cybercrime as a pathway of deception and escalation that creates layered harms, financial, emotional, social, and trust related. Their first hours priorities focused on stopping the spread, saving evidence, reporting quickly, securing accounts, and getting immediate support. Their system-level recommendations placed a heavy emphasis on speed, courteous communication, greater technology safeguards, and prevention-focused awareness, demonstrating that institutional responsiveness and victim-sensitive service delivery are just as important to recovery and confidence as victim action.

Table 1. Victimisation process and harms, themes

Theme	What it captures	Representative quotation 1	Representative quotation 2
Cybercrime tactics and victimisation process	Deception, impersonation, pressure, escalation, harassment	“I got message from my friend's Instagram account… introduced about a trading platform… asked 5000 for banking charge… after that they didn't reply.” (Ajay)	“He impersonated… sent me some dirty online images… blackmailed me… I tried to file an online complaint.” (Nikhil)
Financial and economic harm	Unauthorised withdrawals, OTP fraud, investment scams, secondary banking disruption	“Money was withdrawn from my account without my authorization… caused me financial loss… I had to immediately block my bank account.” (Reshma)	“I lost over 25000 rupees, and that was my college fee.” (Ajay)
Psychological and emotional impact	Fear, anxiety, shame, anger, helplessness, fear of blame	“I felt ashamed and helpless… I couldn't tell anyone because I was scared, they will blame me.” (Indira)	“I'm very scared of online banking sites now.” (Sneha)

Social and relational impact and stigma	Mockery, withdrawal, reputational anxiety, reduced sharing and interaction	"My friends laughed at me and mocked me." (Shankar)	"Aftermath is, I stopped sharing pics." (Arun)
Trust, privacy, and digital safety disruption	Privacy concerns, fear of identity misuse, reduced trust, increased vigilance	"Lost trust and now takes time to trust someone." (Murali)	"Someone misused my personal information online without my permission… stress and fear about my privacy." (Sanjay)
Coping, help seeking, and recovery actions	Blocking, banking actions, complaint attempts, support seeking	"I had to immediately block my bank account, file a complaint, and follow up with the bank and authorities." (Reshma)	"I instantly called my parents informed them everything and got my account frozen." (Pooja)

Table 2. First hours response protocol, themes

Theme	**What it captures**	**Representative quotation 1**	**Representative quotation 2**
Immediate containment and loss prevention	Stop contact, block, avoid OTP and payments, act fast	"Call cyber cell, do not panic, do not transfer money to anyone, do not trust any Instagram ID because it may be hacked…" (Aravind)	"In the first hours, stop all communication, block the account…" (Sanjana)

Evidence preservation and documentation	Screenshots, logs, links, transaction details, prevent evidence loss	“Take screenshots to preserve evidence…” (Sanjana)	“People should be aware of the links and redirecting… take screenshots…” (Hari)
Reporting and escalation pathways	Report quickly via cyber channels, police, bank escalation	“Report to cyber cell, complain to the authorities… report to the proper authority.” (Ganesh)	“Block and report the account…” (Krishna)
Account security and cyber hygiene actions	Secure accounts, privacy settings, avoid suspicious links	“Secure the account…” (Sanjana)	“People should be aware of the links and redirecting…” (Hari)
Emotional stabilisation and social support	Calm down, talk to trusted people, avoid isolation	“Relax, talk to somebody they believe…” (Meera)	“Talk to somebody…” (Pavithra)
Follow up, legal recourse, and system navigation	Need updates, guidance, case tracking, legal support	“Seek legal help…” (Shruti)	“I would not suggest police service as I got no help or feedback…” (Meera)

Table 3. System improvement expectations, themes

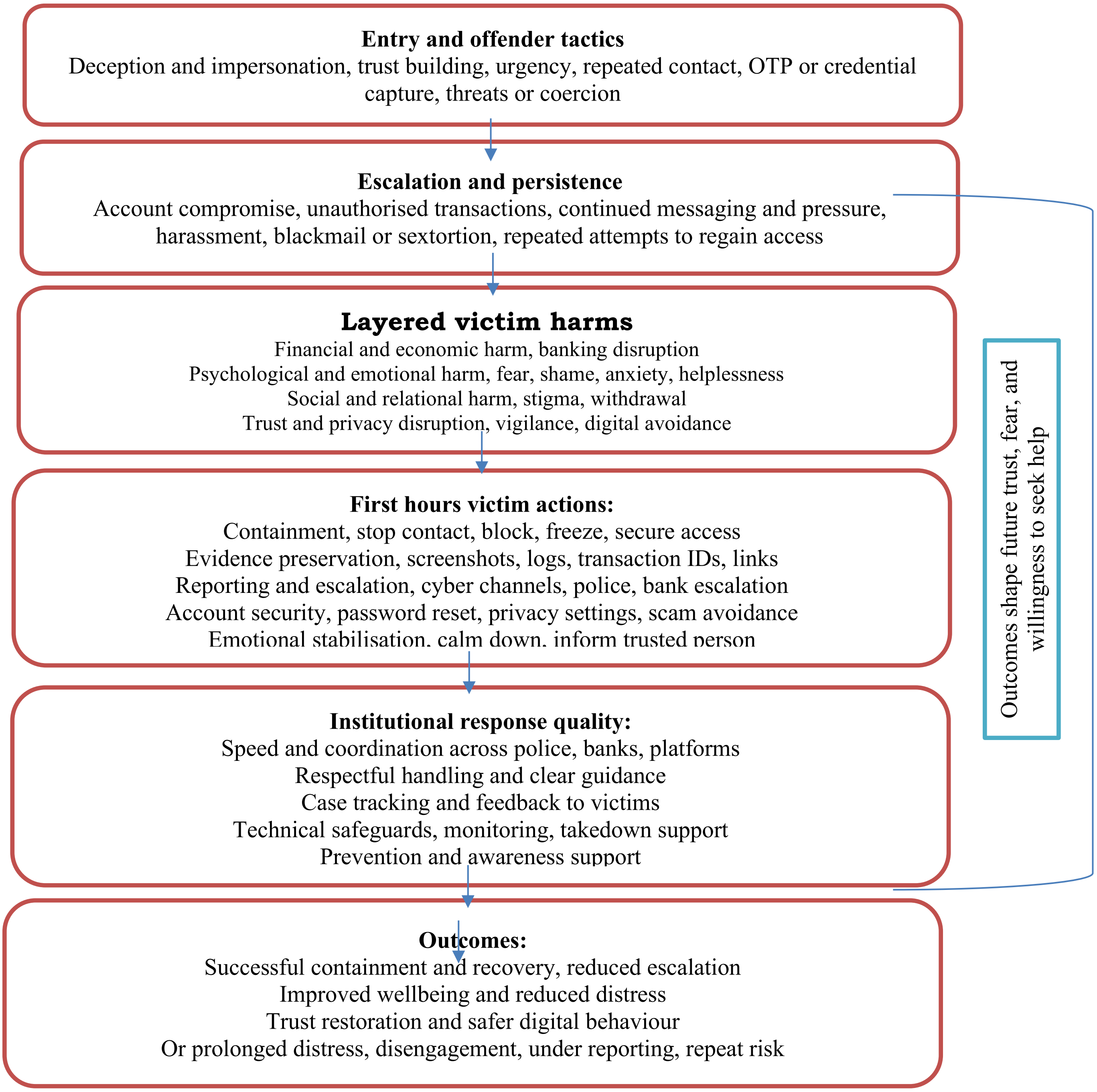
Theme	**What it captures**	**Representative quotation 1**	**Representative quotation 2**
Timely response and	Quick action, reduced delay,	“They should respond more	“In my view cybercrime unit

faster action	portal and follow up issues	quickly." (Karthik)	should respond within 24 hours." (Meera)
Respectful handling and better communication	Empathy, non-judgemental approach, clear guidance	"Provide more support to cyber victims." (Anjali)	"The response by Police, banks should be proper and respect to victims." (Suresh)
Stronger security systems and safeguards	Monitoring, verification, fraud detection, technical capacity	"Awareness programs and need of more technical improvement in cybercrime departments." (Divya)	"More security… monitor the fake apps and suspicious mails and spam ids." (Ramesh)
Platform control and takedown actions	Remove fake sites, regulate unsafe spaces, faster action	"Ban that illegal sites and remove that website." (Varun)	"Strict regulation should be done especially on social media to take immediate action on scams." (Latha)
Stronger rules and enforcement	Stricter laws, accountability, deterrence	"To implement strict laws and useful software to protect the users to make it safe." (Harish)	"Need stricter regulations and more awareness among people." (Harini)
Awareness and prevention initiatives	Public awareness, campaigns, prevention guidance	"Also make awareness to the people." (Kavitha)	"Launch Awareness Campaigns." (Priya)

4.9 Victim Pathway Model of Cybercrime Harm and Response

This model integrates themes derived from the open ended narratives across Tirunelveli, Tuticorin, and Kanyakumari. It conceptualises cybercrime victimisation as a staged pathway where offender tactics and escalation generate layered harms, victims respond through time sensitive first hours actions, and outcomes depend on institutional speed, coordination, and victim sensitive communication, which in turn influences longer term trust and future help seeking.

Victim Pathway Model of Cybercrime Harm and Response



Entry and offender tactics
Deception and impersonation, trust building, urgency, repeated contact, OTP or credential capture, threats or coercion

Escalation and persistence
Account compromise, unauthorised transactions, continued messaging and pressure, harassment, blackmail or sextortion, repeated attempts to regain access

Layered victim harms
Financial and economic harm, banking disruption
Psychological and emotional harm, fear, shame, anxiety, helplessness
Social and relational harm, stigma, withdrawal
Trust and privacy disruption, vigilance, digital avoidance

First hours victim actions:
Containment, stop contact, block, freeze, secure access
Evidence preservation, screenshots, logs, transaction IDs, links
Reporting and escalation, cyber channels, police, bank escalation
Account security, password reset, privacy settings, scam avoidance
Emotional stabilisation, calm down, inform trusted person

Institutional response quality:
Speed and coordination across police, banks, platforms
Respectful handling and clear guidance
Case tracking and feedback to victims
Technical safeguards, monitoring, takedown support
Prevention and awareness support

Outcomes:
Successful containment and recovery, reduced escalation
Improved wellbeing and reduced distress
Trust restoration and safer digital behaviour
Or prolonged distress, disengagement, under reporting, repeat risk

Outcomes shape future trust, fear, and willingness to seek help

5. DISCUSSION

This study developed a victim centred account of cybercrime in three districts of southern Tamil Nadu, Tirunelveli, Tuticorin, and Kanyakumari, by analysing 80 open ended narratives drawn from a parent survey of 180 participants. The themes show that cybercrime is experienced as a pathway, not as a single transaction or isolated online event. Victim accounts repeatedly described staged deception and impersonation, escalation through pressure or threats, and continued harassment in some cases. This aligns with prior evidence that cybercrime victimisation often involves iterative interaction and decision making under uncertainty, which creates practical challenges for policing and response because offenders exploit time pressure and attention lapses (Curtis & Oxburgh, 2023). A major contribution of the findings is the consistent presence of psychological, social, and trust related harms alongside financial harm. Victims described shame, fear of judgement, anxiety, and helplessness, even when the incident did not centre on large monetary loss. This supports existing literature showing that online fraud and related cyber offences produce emotional burden, self-blame, disruption to relationships, and ongoing safety anxiety, rather than purely economic loss (Cross et al., 2016). The themes of trust and digital safety demonstrate how cybercrime alters people's daily internet usage. Numerous victims reported reducing their online activity, avoiding specific apps, remaining vigilant all the time, and withdrawing from regular digital engagement. These behavioral changes align with studies showing that cybervictimization may have long-term effects on online behavior and perceived safety (Reep van den Bergh & Junger, 2018).

The initial few hours are crucial for preventing injury, safeguarding evidence, and initiating institutional action, according to victim guidelines. The narratives' implied procedure is not merely technical, which is noteworthy. It also involves quick social assistance and emotional stabilization. This is important because early support can enhance decision quality and lessen isolation, whereas panic and guilt might postpone containment activities and decrease reporting. The strong emphasis on evidence captures, including screenshots, logs, links, and transaction identifiers, reflects a practical policing reality. Delays can weaken digital traces, reduce traceability, and complicate investigative workflows (Curtis & Oxburgh, 2023). The findings therefore support a first response model that combines containment, documentation, and reporting with psychologically supportive guidance that discourages self-blame and promotes help seeking. The narratives also suggest that willingness to report and follow up is shaped by perceived institutional effectiveness and victim facing communication. According to some experiences, reporting without apparent action might undermine trust because of the lack of assistance, lack of feedback, or unhappiness with the answer. This is consistent with research demonstrating that victim discontent might deter future reporting and that reporting decisions are influenced by expected outcomes, convenience, and past experiences (van de Weijer et al., 2020). Inadequate reactions may result in secondary victimization, which exacerbates misery and lowers system participation (Chatzisymeonidis & Pina, 2024).

Victims' recommendations for system improvement cluster around three operational priorities.

First, police, banks, and platforms should coordinate and move quickly. Victims frequently demanded quicker response, such as prompt feedback and early intervention. This makes sense given that early financial cyber fraud reporting systems are built on time-sensitive containment and tracing (National Cyber Crime Reporting Portal, n.d.).

Second, victim sensitive communication. Many narratives emphasised empathy, respect, non-judgemental handling, and clearer guidance. Practically, this points to simple communication protocols for first contact and follow up, using plain language steps for evidence preservation, bank escalation, and realistic timelines.

Third, technical safeguards and platform controls. Victims asked for stronger verification, monitoring, and takedown actions against fake websites, spam identities, and suspicious applications. This promotes a multi-stakeholder preventative strategy in which police units develop their ability for quick triage and digital evidence handling, banks improve anomaly detection and dispute resolution, and platforms lessen impersonation and the propagation of scams.

5.1 Limitations and future research

The findings are based on self-reported narratives and therefore reflect subjective accounts and recall. The qualitative dataset is drawn from three districts and may not generalise to other regions. Offence type variation could not be fully disaggregated within the qualitative sample. Future work should test the first hours checklist for usability and effectiveness, examine institutional response timelines using administrative data, and compare victim pathways across different offence categories such as financial fraud, account takeover, and technology facilitated harassment.

Overall, the thematic findings show that cybercrime victimisation produces layered harms and that early containment and evidence preservation are central victim priorities. However, recovery and trust depend not only on victim actions but also on institutional speed, coordination, and respectful victim facing communication. Embedding victim authored first hours guidance within police, bank, and platform response systems may improve help seeking, reduce escalation, and strengthen public confidence in cybercrime reporting pathways.

6. CONCLUSION

This study synthesised open ended narratives from Tirunelveli, Tuticorin, and Kanyakumari, drawn from a parent survey of 180 cybercrime victims, to develop a victim centred account of how cybercrime unfolds, how harm is experienced, and what victims prioritise in the first hours and from institutions. The findings show that cybercrime victimisation is commonly experienced as a staged process involving deception, impersonation, urgency, and coercive persistence, followed by multi layered harms that extend beyond financial loss to include psychological distress, stigma driven social withdrawal, and disruption of trust and perceived digital safety.

The initial few hours were frequently cited by victims as the crucial period. Rapid containment, evidence preservation, prompt reporting through appropriate channels, account security, and contacting reliable individuals for prompt assistance are the main points of their advice. Just as importantly, their stories show that recovery does not depend only on what victims do. Victims emphasised faster and coordinated action, respectful and non-judgemental communication, clear guidance and follow up, stronger technical safeguards, platform controls, and prevention oriented awareness initiatives.

These ideas are combined into a single framework by the Victim Pathway Model presented in this research. It maps the first-hour activities victims prioritize, connects perpetrator techniques to layered damages, and illustrates how institutional response influences healing and long-term trust in digital systems. A victim-informed first-hours checklist and a collection of institution-specific action items that can improve cybercrime triage, victim care, and public awareness are the two immediate outputs that the model practically supports. Future studies could test these results in diverse areas and with different kinds of offenses, and assess their efficacy using metrics like recovery indicators and institutional reaction times.

REFERENCES

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

Chatzisymeonidis, S., & Pina, A. (2024). Exploring police attitudes on victims' delayed reporting and victim blame in technology facilitated IPV. *Crime Science, 13*, Article 12.

Chatzisymeonidis, S., & Pina, A. (2024); Cross et al. (2016); Curtis & Oxburgh (2023); National Cyber Crime Reporting Portal (n.d.); Reep van den Bergh & Junger (2018); van de Weijer et al. (2020).

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, (518), 1–14.

Cross, C., Richards, K., & Smith, R. G. (2016). *The reporting experiences and support needs of victims of online fraud* (Trends & Issues in Crime and Criminal Justice No. 518). Australian Institute of Criminology. https://doi.org/10.52922/ti148355

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in "real world" policing and law enforcement. *The Police Journal, 96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in "real world" policing and law enforcement. *The Police Journal: Theory, Practice and Principles, 96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Indian Cyber Crime Coordination Centre. (n.d.). *Indian Cyber Crime Coordination Centre (I4C)*. Ministry of Home Affairs, Government of India.

Indian Cyber Crime Coordination Centre. (n.d.). *National Cybercrime Reporting Portal (NCRP) and 1930 helpline*. Ministry of Home Affairs, Government of India.

National Cyber Crime Reporting Portal. (n.d.). *Filing a complaint on the National Cyber Crime Reporting Portal*. Government of India.

National Cyber Crime Reporting Portal. (n.d.). *National cybercrime reporting portal* (includes reporting options for financial cyber fraud and helpline details). Government of India.

Reep van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*, Article 5. https://doi.org/10.1186/s40163-018-0079-3

Reep van den Bergh, J., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*, Article 5.

Sikra, J., Renaud, K. V., & Thomas, D. R. (2023). UK cybercrime, victims and reporting: A systematic review. *Commonwealth Cybercrime Journal, 1*(1), 28–59.

van de Weijer, S. G. A., Leukfeldt, E. R., & van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal, 43*(1), 17–34.

van de Weijer, S. G. A., Leukfeldt, E. R., & van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal, 43*(1), 17–34.