International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Hidden Harms Online: A Review of Psychological, Social and Economic Impacts of Cybercrime Victimisation

Ms. Prabha A[1], Prof. Dr. Beulah Shekhar[2], Mr. Ameenul Abdullah K S[3]

[1]PhD Scholar, Criminology & Criminal Justice, Manonmaniam Sundaranar University
[2]Adjunct Professor, Liberal Arts, Parul University
[3]PhD Scholar, Criminology & Forensic Sciences, Karunya Institute of Technology & Sciences

ABSTRACT

Cybercrime victimisation includes financially motivated offences such as scams and payment fraud, and technology facilitated interpersonal offences such as harassment, stalking, and image based abuse. While cybercrime is often framed in terms of monetary loss and technical prevention, the evidence shows that victim impacts are multi domain and can persist well beyond the incident. This review brings together evidence on the psychological, social, economic, and justice related impacts of cybercrime, and it looks closely at how people try to report and get help, and what happens when they interact with police, banks, platforms, and telecom systems.

We conducted a structured narrative scoping review of studies and key reports published between 2010 and 2025. We searched major multidisciplinary databases and selected grey literature sources for work that examined cybercrime victim impacts, coping and recovery, and experiences with reporting and response processes. Findings were synthesised using thematic synthesis and narrative integration to identify cross cutting patterns across offence types and contexts. Across the evidence, victims commonly report distress, fear, shame, anger, and a strong sense of losing control. Many also experience social harms such as stigma, withdrawal, relationship strain, and reputational anxiety, especially when the offence involves coercion, humiliation, or the risk of public exposure. The economic impact goes beyond the immediate loss and often includes time spent chasing solutions, administrative burden, disrupted routines, and prolonged vigilance, even when money is later recovered. Reporting and help seeking rarely look like a single decision. Instead, they unfold as a pathway shaped by embarrassment, fear of being blamed, uncertainty about outcomes, and the effort required to navigate multiple agencies. When responsibilities are fragmented and communication is poor, victims can feel re harmed by the process itself, which damages institutional trust and discourages future reporting.

Building on these findings, the review proposes an integrative victim impact framework that links offence mechanics, offender victim interaction, uncertainty, and system response quality to multi domain harms and long tail outcomes. Practice recommendations prioritise time bound fraud containment, coordinated case journeys across systems, procedural justice communication standards, trauma informed support pathways, and monitoring indicators for speed, victim experience, outcomes, and equity. India focused priorities include strengthening the functional integration of 1930 and the National Cybercrime Reporting Portal, improving coordination with banks and intermediaries, and expanding frontline capacity for triage, evidence preservation, and supportive communication.

Keywords: cybercrime victimisation, scam and fraud, technology facilitated abuse, secondary victimisation, procedural justice, reporting barriers, victim support, India, scoping review

1. INTRODUCTION

Cybercrime victimisation is often discussed as a single category, but it includes very different offence types that vary in intent, offender contact, and harm profile. These definitional spread matters because measurement, prevalence estimates, and victim support needs change depending on whether the incident involves cyber enabled fraud, unauthorised access, or technology facilitated interpersonal abuse (Home Office, 2025). A second complication is that cybercrime sits across legal and institutional boundaries. Many incidents involve both cyber security failures and conventional offences such as cheating, intimidation, extortion, or defamation, which makes classification and recording inconsistent across jurisdictions and agencies (PRS Legislative Research, 2025).

1.1 Why cybercrime harms can feel different from traditional offences

Even when the visible loss is financial, victims often describe cybercrime as a violation of private digital space and personal identity. This is partly because digital systems hold intimate information and routine life functions, and compromise can create persistent uncertainty about continued access, future misuse, or repeated intrusion (Palassis et al., 2021). Cyber offences also have features that amplify victim distress, such as offender anonymity, rapid scaling, and transnational infrastructure that reduces the victim's sense that accountability is achievable (Office for Statistics Regulation, 2025). In interpersonal cyber offences, harms can also resemble coercive control because the offender can maintain contact, threaten exposure, and repeatedly re traumatised the victim through ongoing messaging or circulation risks, even after the original incident ends (Home Office, 2025).

A consistent finding across recent victim research is that financial recovery does not automatically resolve emotional harm. Victims can continue to report stress, anger, sleep disruption, fear of recurrence, and reduced trust in digital systems even after money is refunded or accounts are restored (Home Office, 2025). The psychological impact is especially salient in account compromise and hacking, where victims describe anxiety, lowered sense of safety, and intrusive thinking linked to loss of control over their digital environment (Palassis et al., 2021). These impacts become practically important because they shape coping strategies, everyday routines, and willingness to engage with formal systems (De Kimpe et al., 2020).

1.2 Reporting and help seeking as a decision process, not a simple awareness issue

Cybercrime reporting cannot be explained only through legal awareness. Evidence suggests that victims weigh shame, perceived self blame, procedural burden, and expected utility before deciding to report, especially for fraud related incidents (Koning, 2025). Help seeking also includes informal pathways such as family and peer support, which may be preferred when victims anticipate judgement or minimisation by authorities (De Kimpe et al., 2020). This decision logic matters for prevention and response because underreporting reduces intelligence for policing, but it can also delay time sensitive actions such as fund freezing in financial cyber fraud.

A cybercrime victim often has to navigate multiple nodes, police reporting, bank dispute channels, telecom operators, and platform processes. When these systems are not aligned, victims can experience repeated referrals, delays, inconsistent guidance, and communication that feels blaming. These experiences can function as secondary victimisation because the response process itself becomes exhausting and emotionally invalidating (Home Office, 2025). At a governance level, under recording and inconsistent

pathways also distort the public picture of cybercrime, because some reports enter intelligence channels without being recorded as crimes, while others are recorded but remain difficult to investigate due to evidence and attribution barriers (Office for Statistics Regulation, 2025).

1.3 India context and policy relevance for victim centred response

India's digital expansion has created major opportunities but it has also increased exposure to cyber frauds and related harms. Recent government communications describe sharp growth in reported cyber incidents and highlight active measures such as blocking SIMs and device identifiers linked to fraud networks, and scaling national level reporting and response infrastructure (Press Information Bureau, 2025). The Indian Cyber Crime Coordination Centre also positions the National Cyber Crime Reporting Portal and the 1930 helpline as key entry points for reporting, particularly for financial frauds (Indian Cyber Crime Coordination Centre, n.d.; National Cyber Crime Reporting Portal, 2024). Time sensitivity is emphasised in financial cyber fraud response, where guidance from the Ministry of Finance indicates that a formal portal complaint should follow helpline reporting within a short window to support recovery actions (Ministry of Finance, 2024). At the same time, parliamentary review has stressed capacity building, stronger coordination, and clearer responsibilities across intermediaries and enforcement agencies, which directly links to victim experience and confidence in reporting (PRS Legislative Research, 2025).

1.4 Aim and contribution of this review

This review builds a multi domain synthesis that treats cybercrime victimisation as a victim journey that unfolds across emotional harm, social impact, economic burden, and institutional response. It contributes by mapping impact patterns across offence categories, consolidating evidence on reporting and help seeking barriers, and translating these findings into a victim centred framework that is usable for policing, victim services, and cyber harm governance (Home Office, 2025; Koning, 2025).

2. RESEARCH METHODOLOGY

2.1 Review design and rationale

This study used a structured narrative review design, supported by scoping style search and screening procedures. A structured narrative approach was selected because the cybercrime victimisation literature is methodologically diverse, spanning qualitative victim narratives, cross sectional surveys, administrative and reporting data, and policy reports. These sources often measure different outcomes and use different definitions, which limits the feasibility of meta analysis but allows strong thematic synthesis across harm domains and victim journeys (Popay et al., 2006). The review was designed to capture both cyber enabled financial victimisation and technology facilitated interpersonal victimisation, because these categories differ in offender victim interaction, reporting pathways, and harm profiles, yet overlap in victim support and institutional response needs.

2.2 Search strategy, databases, keywords, time frame

Databases searched

Scopus, Web of Science Core Collection, PsycINFO, PubMed, IEEE Xplore, and the ACM Digital Library were searched to cover criminology, psychology, public health, and computing oriented cybercrime research. Google Scholar was used for supplementary searches and citation chasing, with careful screening for source quality.

Grey literature and policy sources

To capture system level victim response evidence and reporting infrastructure, relevant government and institutional sources were also searched and screened, including official portals and reports linked to

cybercrime reporting, financial fraud response, consumer protection, and parliamentary or committee reviews. Sources included police and government portals and published reports, regulator advisories, and official committee documents.

Time frame

The primary time frame was January 1, 2010 to December 28, 2025. This window was chosen to reflect contemporary offence patterns, platform ecosystems, and evolving reporting and recovery mechanisms. Seminal or highly cited theoretical sources published before 2015 were included where necessary to frame the conceptual model.

Search terms

Search strings were adapted for each database using subject headings where available and free text terms in titles, abstracts, and keywords. Core concepts included cybercrime type, victimisation, impact, reporting, and support seeking.

A representative Boolean string was:

(cybercrime OR "online fraud" OR scam* OR phishing OR "identity theft" OR hacking OR "account takeover" OR sextortion OR "image based abuse" OR cyberstalk* OR cyberbully* OR "technology facilitated" OR "online harassment")

AND

(victim OR victimisation OR victimization)

AND

(impact OR harm OR trauma OR distress OR "mental health" OR anxiety OR depression OR stigma OR "social impact" OR "economic loss" OR coping)

AND

(report OR "help seeking" OR "support seeking" OR police OR bank OR platform OR "secondary victimisation" OR "procedural justice")

Supplementary methods

Backward and forward citation chasing was conducted for key included studies to identify additional relevant evidence. Targeted searches were also conducted for specific offence types such as romance scams, sextortion, and account takeover, and for victim pathway terms such as "bank reimbursement" and "platform takedown."

2.3 Inclusion and exclusion criteria

Inclusion criteria

Studies and reports were included when they met one or more of the following conditions.

1. Examined cybercrime victimisation and reported outcomes related to psychological, social, relational, reputational, economic, or wellbeing impacts.
2. Analysed reporting, help seeking, barriers to reporting, or experiences with police, banks, platforms, telecom providers, or other institutions.
3. Presented empirical findings using quantitative, qualitative, or mixed methods designs.
4. Provided policy relevant evidence on reporting systems, fraud recovery processes, or victim support mechanisms, and were issued by high credibility organisations.

Exclusion criteria

Sources were excluded if they met any of the following conditions.

1. Focused only on offender techniques or technical vulnerabilities without victim impact, reporting, or victim response content.

2. Addressed cyber security incidents in organisations only, with no victim level outcomes or citizen victim reporting pathways.
3. Were commentaries, opinion pieces, or media reports without primary data or clear methodological basis, unless used only to contextualise a widely documented policy development.
4. Were duplicates, non-retrievable full texts, or sources with insufficient detail to assess relevance and credibility.
5. Were outside the defined time frame, except for foundational theoretical works used for conceptual framing.

Language coverage prioritised English language sources. Where highly relevant and credible national sources were available in other languages, they could be included if an authoritative translation or official English version was accessible.

2.4 Screening process and quality appraisal approach

Screening was conducted in two stages.

Stage 1 involved title and abstract screening to remove clearly irrelevant items.

Stage 2 involved full text screening against the inclusion and exclusion criteria.

Duplicates were removed prior to screening. Reasons for exclusion at full text stage were documented, such as wrong outcome focus, wrong population, or insufficient methodological clarity.

2.5 Quality appraisal

Given the expected heterogeneity of methods, quality appraisal was conducted using a fit for purpose approach rather than a single numerical score. Empirical studies were appraised using the Mixed Methods Appraisal Tool, which supports qualitative, quantitative, and mixed methods designs (Hong et al., 2018). Grey literature and policy sources were appraised using an authority and credibility checklist approach, focusing on provenance, transparency of methods, clarity of data sources, and relevance to the review aims. Quality appraisal was used to inform interpretation and weighting of evidence during synthesis, rather than to exclude studies automatically, unless a source lacked basic credibility.

2.6 Synthesis method, thematic synthesis

Findings were synthesised using thematic synthesis, suitable for integrating qualitative themes with quantitative patterns and narrative evidence (Thomas & Harden, 2008). Synthesis proceeded in three steps.

1. Line by line coding of reported findings and victim described outcomes, including both direct impact statements and institutional response experiences.
2. Grouping of codes into descriptive themes aligned with the review aims, including psychological impacts, social and relational impacts, economic impacts and recovery burden, reporting barriers, institutional response experiences, and secondary victimisation mechanisms.
3. Development of analytical themes that explain how harms unfold across a victim journey, including key drivers such as offence structure, perceived control, offender victim interaction, time sensitivity of response, and quality of institutional communication.

Quantitative findings were not pooled statistically. Instead, they were summarised as patterns and ranges, and were integrated into the thematic narrative to support convergence or highlight divergence across offence types and contexts. The final synthesis produced an integrative victim impact and reporting framework that links impacts, reporting decisions, and system responses.

2.7 Ethics and reflexivity statement for review work

This review used only publicly available literature and did not involve primary data collection with human participants, so formal ethical approval was not required. However, the review deals with sensitive topics,

including sextortion, harassment, and exploitation. Care was taken to describe harms without sensationalising victim experiences and to avoid reproducing identifiable details from case narratives.
Reflexivity was addressed in two ways. First, definitional variation in cybercrime categories was treated as an analytic issue, and studies were interpreted in light of the definitions and measures they used. Second, institutional perspectives in government and policy documents were considered alongside victim centred empirical research, to reduce the risk of relying on enforcement oriented framings that may understate psychosocial harm or secondary victimisation dynamics.

2.8 Limitations of the method

First, cybercrime victimisation research is highly heterogeneous in definitions, measures, and sampling approaches, which limited comparability and ruled out meta analytic pooling. Second, underreporting and sample recruitment bias are common in victim research, particularly for shame linked offences, so prevalence and impact severity may be under or overestimated depending on study design. Third, grey literature and policy sources vary in transparency and may reflect institutional priorities, which can shape what is reported and what is omitted. Fourth, restricting the review primarily to English language sources may have reduced coverage of region specific evidence. Finally, rapid changes in platforms and fraud tactics mean that findings may age quickly, reinforcing the need for ongoing updates to the evidence base.

3. Conceptual framework

3.1 Victimology foundations, harm, coping, and recovery

Victimology has long established that the consequences of victimisation extend beyond immediate injury or loss and may include emotional distress, changes in daily routines, fear, reduced trust, and social withdrawal, with variation shaped by offence characteristics, victim resources, and response from others (Shapland & Hall, 2007; Skogan, 1987). Contemporary harm models emphasise that victim impact is multi-dimensional and may be cumulative, particularly when the victim experiences ongoing uncertainty, repeated contact, or secondary stressors linked to the justice process (Davis & Friedman, 1985; Herman, 1992).
Coping and recovery frameworks offer a useful lens to explain why similar cyber incidents can produce different outcomes for different victims. Transactional stress theory suggests that impact depends on appraisal, meaning how the victim interprets the threat, and coping resources, meaning perceived control, support, and ability to act effectively (Lazarus & Folkman, 1984). In cyber contexts, appraisal is often influenced by uncertainty about what information has been accessed, whether harm will continue, and whether the offender can return, which can sustain anxiety even when immediate damage appears contained (Palassis et al., 2021). Recovery is also shaped by social support and by whether the victim receives validating responses or blame and minimisation, which can amplify shame and self-attribution (Ullman, 1999).

3.2 Routine Activity Theory and cyber routine activity perspectives

Routine Activity Theory explains victimisation risk as a convergence of motivated offenders, suitable targets, and absence of capable guardianship (Cohen & Felson, 1979). Its strength in cybercrime research is that it focuses on opportunity structures and everyday activities rather than stable offender traits, which makes it well suited to digital environments where exposure is frequent and boundaries are porous (Yar, 2005). Cyber routine activity perspectives adapt guardianship and target suitability to digital settings. Guardianship includes technical controls, password and authentication practices, awareness of scam cues, and institutional safety measures by banks and platforms. Target suitability includes visibility and

accessibility online, behavioural signals that can be exploited, and the degree of reliance on digital services (Leukfeldt & Yar, 2016). Exposure can include time spent online, interaction with unknown accounts, high frequency transactions, and participation in contexts where offenders operate, such as marketplace platforms, messaging apps, and social media (Pratt et al., 2010).

This review uses routine activity logic to organise why some cyber offences are more likely to occur and why certain groups may face elevated risk in specific digital contexts. It also uses the concept of guardianship more broadly. Guardianship is not only individual caution. It includes institutional capacity to detect fraud, freeze funds quickly, preserve evidence, and provide clear guidance to victims. When guardianship fails across these layers, both victimisation and downstream harm can intensify (Leukfeldt & Yar, 2016).

3.3 Fraud and scam victimisation theories, persuasion, grooming, and trust exploitation

Cyber fraud and scams rely heavily on social engineering and persuasion rather than purely technical intrusion. Persuasion theory helps explain how offenders elicit compliance by using authority cues, scarcity and urgency, reciprocity, liking, social proof, and commitment consistency, often under time pressure and information overload (Cialdini, 2009). In many scams, the offence is structured to short circuit deliberation, isolate the victim from corrective input, and create a narrow window where fast action appears necessary.

A second relevant strand is grooming and relationship based manipulation, most visible in romance scams, sextortion, and forms of coercive online exploitation. These offences often involve staged trust building, progressive boundary testing, and exploitation of emotions such as affection, shame, or fear (Cross et al., 2016; Whitty, 2018). Harm in these cases tends to be compound. Victims experience betrayal and identity disruption alongside financial loss or blackmail threats, which can elevate distress and impede reporting due to stigma (Whitty, 2018).

Trust exploitation is central across scam types. Offenders borrow credibility through impersonation, spoofed identities, institutional branding, and engineered familiarity. This connects directly to victim self attribution. When the offence is framed as a personal failure, victims may experience shame and self-blame, which reduces help seeking and increases isolation (Cross, 2016; Koning, 2025). The framework used in this review treats fraud victimisation as a process, with stages that include contact initiation, credibility construction, pressure or grooming escalation, compliance extraction, and post incident management by the offender, including further manipulation or repeat targeting (Button et al., 2014; Cross, 2016).

3.4 Secondary victimisation and procedural justice in cyber contexts

Secondary victimisation refers to additional harm arising from institutional and social responses that are blaming, dismissive, insensitive, or procedurally burdensome. It is well documented in sexual violence and other victimisation contexts, where poor responses can intensify trauma and reduce future help seeking (Campbell, 2005; Orth, 2002). In cybercrime, secondary victimisation can occur when victims are told they were careless, when they face repeated referrals between agencies, when they receive inconsistent advice, or when delays lead to further loss.

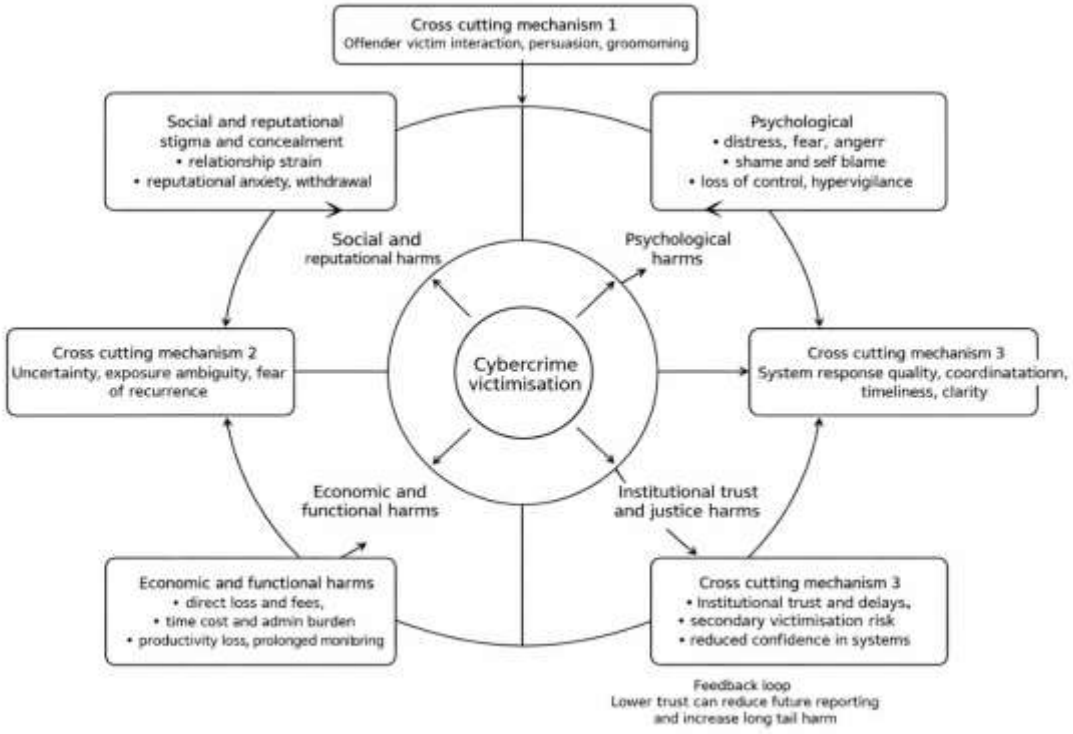
Procedural justice theory offers a concrete mechanism to understand these effects. People are more likely to view authorities as legitimate and cooperate when they experience fair process, voice, neutrality, respectful treatment, and trustworthy motives (Tyler, 1990). Applied to cyber reporting, procedural justice predicts that respectful communication, clear explanation of steps, and timely updates can restore agency

and reduce distress, even when outcomes are uncertain. Conversely, opaque processes and perceived indifference can reduce institutional trust and increase withdrawal (Tyler & Huo, 2002).

Cyber contexts amplify these dynamics because victims often navigate multiple systems with different goals. Police focus on evidence and jurisdiction, banks focus on liability and dispute procedures, platforms focus on policy enforcement and moderation. When the victim must coordinate these systems alone, procedural burden increases and the chance of perceived injustice rises. Empirical work on help seeking after technology facilitated victimisation shows that victims use both websites and police, and they often evaluate these channels based on responsiveness and clarity, not only availability (Colburn et al., 2023). This review therefore treats secondary victimisation as a cross institutional risk that shapes impact severity and reporting persistence.

3.5 Proposed integrative model for this review

The review uses an integrative model that links opportunity, manipulation, victim appraisal, and institutional response into a single victim journey logic. It is designed to explain both victimisation risk and harm severity.



Victim impact wheel with domains and cross cutting mechanisms

Table 1. Integrative model components and propositions

Source: Author

Model component	What it captures	Core proposition for synthesis
Opportunity structure	Exposure, target suitability, guardianship at individual, platform, bank, and policing levels	Higher exposure and weaker guardianship increase victimisation likelihood and may intensify downstream harm (Cohen & Felson, 1979; Leukfeldt & Yar, 2016).

Offender tactics and interaction	Persuasion, impersonation, urgency, grooming, coercion, repeated contact	Greater personal targeting and interaction predict stronger psychological and social harms than low contact incidents (Cialdini, 2009; Whitty, 2018).
Victim appraisal and attribution	Perceived control, uncertainty, shame, self-blame, perceived severity	Negative attribution and high uncertainty amplify distress and reduce reporting and help seeking (Lazarus & Folkman, 1984; Cross, 2016).
Coping resources	Social support, digital skills, financial resilience, prior experiences with institutions	Stronger coping resources and support reduce harm persistence and improve recovery pathways (Ullman, 1999; De Kimpe et al., 2020).
Institutional response and procedural justice	Clarity, respect, timeliness, coordination across police, banks, platforms	Higher procedural justice improves victim trust and engagement, reduces secondary victimisation, and can improve recovery outcomes (Tyler, 1990; Colburn et al., 2023).
Multi domain impacts	Psychological distress, social and relational harms, economic burden, reputational harm	Impacts are multi domain and may persist beyond financial recovery, especially when system response is fragmented (Jansen, 2018; Cross, 2016).
Feedback loops	Changes in routines, digital participation, trust, and repeat vulnerability	Severe harms and poor responses can increase withdrawal and reduce future reporting, while also influencing future risk exposure patterns (Skogan, 1987; Tyler & Huo, 2002).

4. RESULTS, THEMATIC SYNTHESIS OF EVIDENCE

This section synthesises evidence across included studies and high relevance reports, organised around offence typologies, domains of harm, long tail outcomes, and system responses. The thematic structure follows the integrative framework developed in Section 3 and emphasises how offence mechanics, degree of interpersonal contact, and institutional coordination shape harm severity and recovery trajectories (Cross et al., 2016; Home Office, 2025).

4.1 Typologies of cybercrime and differential harm profiles

Across the literature, cybercrime victimisation clusters into two broad families with distinct harm profiles. First, financially motivated offences include consumer fraud and scams, online banking fraud, payment diversion, marketplace fraud, and identity enabled fraud. These offences often produce immediate economic loss and prolonged administrative burden, but the psychological impact can be substantial when victims experience betrayal, shame, or persistent uncertainty about exposure and further loss (Button et al., 2014; Cross et al., 2016; Home Office, 2025). Mass marketing fraud may involve low interpersonal contact, yet victims can still report distress, humiliation, and reduced trust, especially when the incident is interpreted as a personal failure rather than a targeted crime (Button et al., 2014; Home Office, 2025).

Second, technology facilitated interpersonal victimisation includes cyberstalking, online harassment and threats, coerced sexual content, image based sexual abuse, and other forms of persistent unwanted contact. These incidents often generate fear, hypervigilance, reputational harm, and social disruption, and they can

resemble patterns observed in offline coercive control, with a strong association between repeated contact and elevated psychological harm (Worsley et al., 2017; Hellevik et al., 2025).

A cross cutting category is account compromise and hacking, where the digital self becomes the site of violation. Victims describe loss of control, intrusive worry, and ongoing vigilance, partly because the boundary between incident and everyday life is blurred when email, social media, and financial accounts are affected (Palassis et al., 2021).

A consistent synthesis finding is that harm severity is patterned by three offence dimensions: (a) personal targeting and interaction, (b) duration and repeatability of contact, and (c) reversibility of consequences such as reputational spread or identity compromise (Cross et al., 2016; Home Office, 2025; Whitty & Buchanan, 2016).

Table 4.1. Illustrative mapping of offence types and dominant harm patterns

Offence cluster	Typical incident features	Dominant harms reported in evidence
Fraud and scams, including romance fraud	Persuasion, credibility building, urgency, staged compliance	Financial loss, shame, betrayal, grief, reduced trust, prolonged rumination (Button et al., 2014; Whitty & Buchanan, 2016)
Banking and payment fraud	Rapid transfer, impersonation, OTP or credential capture	Financial loss, administrative workload, anxiety about future exposure (Jansen & Leukfeldt, 2018; Home Office, 2025)
Hacking and account takeover	Account loss, impersonation, data exposure, lockout	Loss of control, persistent worry, hypervigilance, identity disruption (Palassis et al., 2021)
Harassment, threats, cyberstalking	Repeated messages, monitoring, escalation risk	Fear, anxiety and depression, safety planning, routine disruption (Worsley et al., 2017)
Image based sexual abuse	Nonconsensual sharing, coercion, permanence of content	Shame, trauma symptoms, social withdrawal, reputational harm, ongoing fear (Hellevik et al., 2025; Mento et al., 2025)

4.2 Psychological impacts

Evidence consistently shows that cybercrime harms extend beyond immediate upset and include clinically relevant distress for a subset of victims. Core psychological impacts include anxiety, stress, worry, anger, shame, guilt, and persistent fear. The intensity and duration vary widely, from short term disruption to months or longer of distress, especially when victims face uncertainty about ongoing exposure or continued offender contact (Jansen & Leukfeldt, 2018; Home Office, 2025).

Shame and self-blame are recurrent across fraud and scam studies, and they are strongly linked to reluctance to disclose and to delayed help seeking. Large scale and interview based work on fraud impacts documents embarrassment, self-blame, and reduced self-confidence, sometimes accompanied by sleep disturbance and relationship strain (Button et al., 2014; Home Office, 2025). In romance fraud, victims often report a combined emotional and financial injury, described as a double loss that can resemble grief and trauma reactions (Whitty & Buchanan, 2016). Threat based and persistent contact offences show a different psychological profile. Cyberstalking and harassment studies report high levels of fear, anxiety, and depressive symptoms, with victims describing anticipatory stress, safety behaviours, and constant monitoring of devices and accounts (Worsley et al., 2017). Hacking victimisation similarly produces

ongoing anxiety, but the mechanism is often loss of control and identity boundary violation rather than fear of physical approach, although these experiences can overlap (Palassis et al., 2021).

Across offence types, a key theme is that psychological harm is intensified by poor informational clarity. When victims do not know what data was accessed, who has it, and what might happen next, uncertainty becomes a harm multiplier (Home Office, 2025; Palassis et al., 2021).

4.3 Social, relational, and reputational impacts

Social harms cluster into three areas.

Relational disruption and distrust are frequently reported after fraud and account compromise. Victims often become suspicious of communications, transactions, and even intimate relationships. This can affect family dynamics, workplace interactions, and willingness to engage online (Button et al., 2014; Jansen & Leukfeldt, 2018).

Stigma and concealment are prominent in romance scams and sexual or humiliating offences. Victims often limit disclosure to avoid judgement, which reduces access to informal support and can increase isolation. Romance scam victims may face ridicule, which compounds shame and can delay reporting (Whitty & Buchanan, 2016). Image based sexual abuse is associated with strong reputational anxiety and withdrawal from social spaces, particularly when content permanence and re circulation are perceived as likely (Hellevik et al., 2025; Mento et al., 2025). Reputational and occupational spillover also appears in hacking and impersonation. Victims may fear that employers, colleagues, or contacts will interpret fraudulent posts or messages as authentic, which can trigger urgent corrective labour and a prolonged sense of reputational fragility (Palassis et al., 2021).

4.4 Economic impacts and recovery burden

Economic impacts extend beyond the initial monetary loss. Victims often experience a recovery burden that includes time costs, administrative complexity, opportunity costs, and repeated interactions with institutions. Fraud impact research in England and Wales shows that financial loss is often accompanied by stress, disrupted daily functioning, and family spillover, indicating that economic and psychosocial harms are intertwined rather than separate domains (Button et al., 2014; Home Office, 2025).

Studies focusing on online banking fraud and similar incidents show that victims engage in extensive problem focused coping, such as contacting banks, changing credentials, monitoring accounts, documenting evidence, and attempting to trace funds. The burden can persist even when direct reimbursement occurs, because victims must restore accounts and confidence and remain vigilant against re compromise (Jansen & Leukfeldt, 2018).A synthesis level finding is that cost is best conceptualised as a package, with direct financial loss, indirect time cost, emotional labour, and downstream impacts on digital participation and trust (Cross et al., 2016; Home Office, 2025).

4.5 Repeat victimisation and long tail harms

Re targeting is noted in fraud research where victims can be approached again through follow up scams, fake recovery services, or further impersonation attempts. System response gaps, especially delayed intervention and poor coordination, may increase this risk by leaving exposed accounts or by signalling that the victim is still vulnerable (Cross et al., 2016).

Long tail harms refer to impacts that persist after the incident, including sustained anxiety, reduced online engagement, and altered routines. Qualitative evidence on coping with cybercrime victimisation indicates that some victims experience lasting changes in perception and behaviour, including avoidance of online banking, decreased trust in online communications, and continued worry long after the incident is resolved

(Jansen & Leukfeldt, 2018). In image based sexual abuse, long tail harm is strongly linked to permanence and the perceived inability to fully recover privacy or reputation (Hellevik et al., 2025; Mento et al., 2025).

4.6 Reporting pathways and barriers

Evidence on fraud reporting suggests that victims often do not report because they doubt that authorities can act, they feel embarrassed, or they attribute blame to themselves. Empirical modelling of fraud reporting decisions shows that severity and perceived impact are key drivers of reporting, while self-blame can suppress it (Koning, 2025). Large scale and qualitative work with fraud and cybercrime victims similarly reports dissatisfaction linked to perceived limited outcomes and lack of clear support pathways (Home Office, 2025).

For technology facilitated interpersonal victimisation, help seeking can occur through websites, platforms, or police, but prevalence is limited and shaped by perceived seriousness, prior experiences with authorities, and the availability of supportive responses (Colburn et al., 2023). Victims may also rely heavily on informal networks, and when informal responses are minimising or blaming, formal reporting may become even less likely (Colburn et al., 2023). A consistent theme across studies is that victims do not experience reporting as a single decision. They experience it as a pathway. That pathway is shaped by knowledge of where to go, clarity of steps, and how burdensome the process feels (Cross et al., 2016; Home Office, 2025).

4.7 Victim experiences with police, banks, and platforms

Victim journeys often span multiple institutions, with fragmented responsibilities. Evidence from fraud response research highlights repeated referrals and unclear ownership, with victims moving between police channels, financial institutions, and digital intermediaries while attempting to contain harm (Cross et al., 2016). In England and Wales, victim experience research on fraud and cybercrime reports mixed perceptions of support, and it highlights the centrality of communication quality, timeliness, and clear guidance for victim confidence in the process (Home Office, 2025).

For bank mediated offences, speed of action is salient for victims, and delays can be experienced as both practical and psychological harm. For platform based harassment and abuse, victims evaluate responses based on whether reporting tools are accessible, whether decisions are explained, and whether the platform action feels proportionate and timely, although evidence suggests many victims do not engage formal platform channels at all (Colburn et al., 2023). Synthesis across these sources suggests that coordination is itself a form of victim support. When systems act in a connected way, victims experience reduced uncertainty and a stronger sense of control. When systems act in silos, victims experience additional distress and procedural burden (Cross et al., 2016; Home Office, 2025).

4.8 Secondary victimisation and institutional trust

Secondary victimisation in cyber contexts emerges through blame, minimisation, procedural exhaustion, and repeated retelling. Victims may be told implicitly or explicitly that they should have known better, which can intensify shame and reduce willingness to continue with the process, even when the initial incident is severe (Button et al., 2014; Cross et al., 2016). In victim experience research, perceived lack of support and poor communication are strongly linked to dissatisfaction, and dissatisfaction can translate into reduced trust in the reporting system and lower likelihood of future help seeking (Home Office, 2025).

Help seeking research in technology facilitated victimisation indicates that low engagement with police and websites can partly reflect negative expectations and perceived futility. This is important because it suggests that institutional trust is both an outcome and a predictor, with negative expectations discouraging reporting, and negative experiences reinforcing those expectations (Colburn et al., 2023; Home Office,

2025). An adjacent evidence theme concerns the quality of fraud and cybercrime recording and statistics, which affects transparency and public confidence. Reviews and action plans on fraud and computer misuse statistics in England and Wales highlight persistent quality challenges in recorded data systems, with implications for how victims perceive system credibility and responsiveness (Office for Statistics Regulation, 2025; Office for National Statistics, 2025).

4.9 Protective factors, coping, and support needs

At the individual level, victims adopt problem focused coping such as securing accounts, learning security practices, and documenting evidence, alongside emotion focused coping such as seeking reassurance and support. Evidence on coping with cybercrime victimisation shows substantial variation, with some victims reporting rapid adjustment and others reporting prolonged fear and distress (Jansen & Leukfeldt, 2018).

At the social level, perceived availability of supportive responses shapes recovery. Evidence on social support seeking among cybercrime victims indicates that help seeking is influenced by perceived seriousness, emotional response, and expectations of receiving meaningful support, which suggests that support ecosystems should be designed to reduce shame and provide concrete guidance (De Kimpe et al., 2020).At the institutional level, victims consistently express needs for clear information, coordinated steps, realistic expectation setting, and respectful communication. Victim experience research in fraud and cybercrime emphasises that even when outcomes are uncertain, improved communication and procedural clarity can reduce anxiety and improve satisfaction (Home Office, 2025; Cross et al., 2016).

4.10 Equity considerations, gender, age, socioeconomic status, and digital literacy

Gender and age patterns often depend on offence type. Interpersonal abuse and image based sexual abuse disproportionately affect women and younger people in many contexts, with harms shaped by stigma, reputational vulnerability, and safety concerns (Hellevik et al., 2025; Mento et al., 2025; Yaqoob et al., 2025). Fraud targeting of older adults is a distinct concern, and evidence highlights shame, reduced trust, and potential serious mental health impacts for some victims, alongside barriers to reporting linked to embarrassment and fear of being judged as incompetent (Button et al., 2014; Chicago Fed, 2024).

Socioeconomic status and digital inequality influence both vulnerability and recovery capacity. Research on cybersecurity and digital inequalities argues that digital skills are stratified by socioeconomic conditions, and that this stratification can shape exposure to cyber threats and ability to implement protective behaviours (Khan et al., 2023). Work on cyber safety behaviours in developing contexts similarly indicates that digital safety practices are patterned by socioeconomic resources and access to knowledge and support (Dodel, 2020). Digital literacy is repeatedly implicated as a protective resource, but the evidence also suggests that knowledge alone is insufficient when offenders exploit trust, urgency, and institutional impersonation. This has two implications for equity. First, prevention should not be framed as individual responsibility only, because it can intensify victim blaming. Second, system design by banks, platforms, and reporting agencies becomes central to equitable protection and recovery, since institutional guardianship can compensate for individual skill gaps (Cross et al., 2016; Home Office, 2025).

5. Discussion

The synthesis confirms that cybercrime victimisation produces harms that are multi domain and that frequently persist beyond the incident, even when direct financial losses are recovered. Across offence types, psychological impacts such as distress, anxiety, fear, anger, shame, and loss of control are common, with severity shaped by uncertainty about ongoing exposure and by the extent of offender victim

interaction (Home Office, 2025; Jansen & Leukfeldt, 2018; Palassis et al., 2021). Social harms frequently involve stigma, withdrawal, relationship strain, and reputational anxiety, particularly in offences involving coercion, humiliation, or content permanence (Home Office, 2025; Whitty & Buchanan, 2016). Economic harm extends beyond monetary loss and includes time cost, administrative load, and prolonged vigilance, which function as indirect harms and can sustain distress and avoidance (Cross et al., 2014; Cross et al., 2016; Home Office, 2025).

Reporting and help seeking emerge less as a single decision and more as a pathway that victims evaluate based on expected utility, shame, procedural burden, and perceived responsiveness of institutions (Colburn et al., 2023; Koning et al., 2025). Evidence across contexts indicates that fragmented responsibility across police, banks, and platforms increases victim effort, delays containment actions, and raises the likelihood of secondary victimisation, which in turn undermines institutional trust and future reporting (Cross et al., 2016; Home Office, 2025). What is new in this review is the explicit integration of three strands that are often analysed separately. First, offence mechanics and persuasion or grooming processes that shape primary harm. Second, the system response pathway that shapes whether harms escalate or resolve. Third, secondary victimisation and procedural justice as mechanisms that influence both wellbeing outcomes and institutional trust. By treating cybercrime as a victim journey across systems rather than a single incident, the synthesis clarifies why similar losses can produce very different recovery trajectories and why improvements in coordination and communication can function as harm reduction interventions (Cross et al., 2016; Home Office, 2025).

5.2 Multi domain victim impact framework, the model proposed

The proposed framework conceptualises cybercrime victim impact as a set of interacting domains, mediated by uncertainty and institutional response. The first domain is psychological and emotional harm, including distress, fear, anxiety, shame, anger, intrusive worry, and reduced perceived control. These harms are amplified when victims cannot determine what data was accessed, whether the offender can return, and whether further misuse will occur, and they are often intensified when the offence involves ongoing contact, coercion, or grooming (Home Office, 2025; Palassis et al., 2021; Whitty & Buchanan, 2016).

The second domain concerns social, relational, and reputational harms. These include stigma, concealment, isolation, relationship conflict, and reputational anxiety, with heightened effects when offences involve impersonation, public exposure risks, humiliation, or threats. In these contexts, fear of judgement and reputational loss can reduce disclosure and can delay formal reporting, which increases vulnerability to continued harm (Home Office, 2025; Whitty & Buchanan, 2016).

The third domain is economic and functional harm. Beyond direct loss, victims experience recovery burden, time cost, productivity loss, and persistent monitoring behaviours. This includes the administrative labour of restoring accounts, disputing transactions, securing devices, changing credentials, and rebuilding confidence in digital systems, all of which can sustain distress even when reimbursement occurs (Cross et al., 2016; Home Office, 2025; Jansen & Leukfeldt, 2018).

The fourth domain concerns institutional trust and justice related harms. Confidence in police, banks, and platforms is shaped by perceived fairness, clarity, timeliness, and respect. Poor experiences can become secondary victimisation, producing withdrawal, dissatisfaction, and reduced likelihood of future help seeking. This domain therefore operates as both an outcome of the response pathway and a predictor of future reporting and cooperation (Colburn et al., 2023; Cross et al., 2016; Tyler, 1990).

Across all four domains, the framework emphasises three cross cutting mechanisms. The first is offender victim interaction, including persuasion, grooming, and continued contact. The second is uncertainty, including ambiguity about data exposure, recurrence, and long term consequences. The third is system response quality, including coordination and procedural justice signals. These mechanisms connect offence type to harm severity and explain long tail outcomes reported across the evidence base (Home Office, 2025; Palassis et al., 2021; Whitty & Buchanan, 2016).

5.3 Implications for banks, platforms, telecom, and regulators

The evidence suggests that institutional guardianship is central to equitable protection, because not all victims can compensate through individual cyber hygiene, particularly under urgency and impersonation conditions (Cross et al., 2016). For banks and payment intermediaries, the central implication is to strengthen friction for high risk transfers, expand rapid hold and recall processes, and improve real time customer alerts. Policy frameworks on customer liability in unauthorised electronic banking transactions place important responsibilities on banks and emphasise customer protection mechanisms, including how liability is allocated and how promptly incidents are handled (Reserve Bank of India, 2017). Banks should also align workflows to support national reporting and coordination channels that connect banks and intermediaries with cybercrime back end systems for faster action (I4C, n.d.). Victim help seeking evidence indicates that victims judge systems by clarity and responsiveness, which means user experience design is a safety intervention as well as a compliance feature (Colburn et al., 2023).

For telecom providers and telecom regulation, telecom identifiers, SIM misuse, and device traceability are repeatedly implicated in cyber fraud ecosystems. Recent telecom cyber security measures in India emphasise device traceability and responsible use of telecom identifiers, indicating an expanding regulatory approach to telecom enabled fraud risks (Press Information Bureau, 2025). Tools such as CEIR can also support device level actions to reduce misuse and strengthen traceability in the ecosystem (Department of Telecommunications, n.d.). Telecom sector measures should be integrated with law enforcement escalation routes so that high risk identifiers can be acted upon rapidly, with appropriate safeguards.

5.4 Implications for victim services, counselling, and trauma informed care

Victim services should recognise that cybercrime can generate trauma like symptoms, shame, and social withdrawal, particularly for offences involving coercion, humiliation, or continued threats (Home Office, 2025; Whitty & Buchanan, 2016). A trauma informed model should begin with psychological first aid and stabilisation that reduces panic, shame, and catastrophic thinking while restoring a sense of agency. It should include safety planning, including digital safety planning for harassment and stalking cases and reputational risk management support for image based abuse. This model aligns with the evidence that cyber victim support needs are both emotional and procedural, and that improved guidance, validation, and coordination can reduce long tail harms and restore confidence (Cross et al., 2016; Home Office, 2025; Jansen & Leukfeldt, 2018).

5.5 India focused implications and implementation priorities

India has institutionalised key entry points for cyber reporting and financial fraud containment. The National Cybercrime Reporting Portal and the 1930 helpline are positioned as central mechanisms, and the I4C ecosystem describes a dedicated financial cyber fraud reporting and management module connecting banks and intermediaries with cybercrime back end systems (I4C, n.d.). The central practical priority is to make these mechanisms feel seamless and victim centred, so that victims do not experience the pathway as confusing, repetitive, or blame oriented.

Victim communication protocols are needed, including standard scripts and training to reduce blame language, improve clarity, and set expectations while maintaining investigative integrity. Capacity building must extend beyond specialist cyber units, because first response is often handled by non-specialist staff. Training should therefore prioritise triage, evidence preservation, referral pathways, and procedural justice behaviours. Telecom enabled fraud reduction and device traceability initiatives should also be integrated into victim response pathways so that reporting can trigger rapid identifier actions where appropriate (Department of Telecommunications, n.d.; Press Information Bureau, 2025). Finally, bank complaint handling should operationalise customer protection expectations, including clear guidance, rapid escalation, and transparent outcomes consistent with RBI customer protection principles (Reserve Bank of India, 2017).

5.7 Research gaps and future research agenda

The evidence base remains uneven and several gaps follow directly from this synthesis. Measurement gaps are substantial, with a need for standardised multi domain victim impact measures that capture emotional, social, economic, and institutional trust harms, including recovery burden and uncertainty. Longitudinal evidence is also limited, and more studies are needed to examine long tail harm trajectories, including how trust and routine changes evolve after resolution and how secondary victimisation experiences shape future reporting.

India specific victim pathway studies are also scarce. There is limited empirical work mapping victim journeys across 1930, portal reporting, bank dispute processes, and platform reporting. Evaluations of time to action, victim satisfaction, and outcomes would be valuable for strengthening practice and accountability in the Indian context (I4C, n.d.; Reserve Bank of India, 2017). Comparative studies should move beyond offence labels and measure interaction intensity, coercion, and content permanence, because these features appear to predict harm severity more strongly than some categories. Institutional response evaluations are also needed, including whether integrated workflows reduce losses and distress, and how training, communication protocols, and data sharing arrangements affect outcomes. Finally, equity and digital inequality remain under addressed. Future research should examine how gender, age, and socioeconomic resources shape exposure, willingness to report, ability to recover, and vulnerability to secondary victimisation, and it should test whether system design can compensate for skill gaps rather than amplify blame.

6. POLICY AND PRACTICE RECOMMENDATIONS

This section translates the synthesis into actionable recommendations that reduce harm, improve recovery, and strengthen reporting and investigative outcomes. Recommendations follow the integrative model, with emphasis on time sensitivity for financial fraud, coordination across institutions, and procedural justice to prevent secondary victimisation (Colburn et al., 2023; Cross et al., 2016; Tyler, 1990). India specific mechanisms such as 1930, the National Cybercrime Reporting Portal, and the Citizen Financial Cyber Fraud Reporting and Management System are treated as core implementation levers for a connected victim journey (Indian Cyber Crime Coordination Centre [I4C], n.d.).

6.1 Integrated reporting and rapid response protocol

A first priority is to implement “one case, one journey across systems.” A single case identifier should be generated at first contact and should be recognised across police cyber units, banks and payment intermediaries, telecom providers, and major platforms. This reduces repeated victim effort, prevents duplicated documentation, and enables coordinated action. India’s portal architecture already provides a

foundation for such integration because the National Cybercrime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System are designed to connect reports to operational workflows for financial cyber fraud response (I4C, n.d.; National Cybercrime Reporting Portal, n.d.).

A third priority is to implement standard escalation tiers that reflect both time sensitivity and harm severity. Tier 1 should cover immediate containment cases such as active fund transfers, unauthorised transactions, and account takeover with ongoing transfers. Tier 2 should cover urgent safety and coercion cases such as sextortion, credible threats, and cyberstalking with escalation risk. Tier 3 should cover non urgent but harmful cases such as impersonation, marketplace fraud, and resolved losses with ongoing distress. Each tier should be linked to specific service level targets for first response and for next steps communication, because victims judge systems by clarity and responsiveness, not only by eventual outcomes (Colburn et al., 2023; Tyler, 1990).

6.2 Victim friendly reporting, procedural justice, and communication standards

A minimum communication standard should be adopted across all agencies that interact with victims, including police, banks, and platforms. This standard should be explicitly built around procedural justice principles such as voice, neutrality, respect, and trustworthy motives, because perceived fairness shapes cooperation and institutional trust (Tyler, 1990). Communication at first contact should acknowledge harm and reassure the victim that victimisation is not evidence of incompetence. It should explain what happens next, who owns which step, and what the victim should do immediately. It should also set realistic expectations on timelines and limits without dismissiveness, and it should offer scheduled updates even when there is no progress, because uncertainty is a major harm multiplier in cyber incidents (Home Office, 2025; Tyler, 1990).

6.3 Capacity building and training for cyber first responders

Capacity building should prioritise triage and victim interaction, not only technology. Training curricula should include harm based triage and time sensitive fraud containment, trauma informed interaction that reduces shame and avoids blame, evidence preservation and structured documentation, and referral pathways for counselling, legal aid, and digital safety support. Training should also cover platform and bank coordination protocols so that frontline responders can route cases quickly to the right node in the ecosystem, which reduces both losses and distress (Cross et al., 2016; I4C, n.d.).

Standard operating procedures should be developed for frontline units and call centres, written for non-specialist use. These SOPs should provide short scripts for victim guidance and clear sequencing of steps across police reporting, bank escalation, and platform reporting. In addition, specialist pathways should be created for coercion and image based abuse, including sextortion and cyberstalking. These pathways should support rapid safety assessment, platform takedown assistance, and referral to counselling, because harms are often severe and stigma can suppress reporting and disclosure (Colburn et al., 2023; Home Office, 2025).

6.4 Data governance, privacy, and platform accountability

Because coordination requires information flow, data governance should be lawful, minimal, and purposeful. Protocols should specify what data is shared, for which purpose, and for how long, and they should define who is the data controller for each segment of the process. They should also define how victims can access status updates and correct errors. Transparent governance supports confidence and reduces suspicion that reporting will create additional exposure or privacy risk, which is especially important in sensitive incidents (Tyler, 1990; Cross et al., 2016).

Platforms should strengthen accountability for impersonation, scams, and abuse by publishing transparency metrics on response times and outcomes for key categories such as impersonation, scam accounts, harassment, and image based abuse. Platforms should also provide clearer decision explanations and improve reporting interface usability, because help seeking research shows that victims assess pathways through responsiveness and clarity (Colburn et al., 2023).

6.5 Monitoring and evaluation indicators

To ensure that recommendations translate into measurable improvement, agencies should track a small set of indicators that reflect both crime control and victim wellbeing. Speed and containment indicators should include median time from first contact to bank alert initiation in financial fraud cases, median time to first containment action such as hold attempts or recall attempts, and the share of cases meeting service targets by tier. Victim experience and procedural justice indicators should include victim rated clarity of next steps soon after first contact, victim rated respect and non-blaming treatment, and the proportion of cases where victims received a status update within the promised window (Tyler, 1990; Home Office, 2025).

Equity indicators should track time to action and outcomes by age group, gender, and district, drop off points in the reporting journey by literacy and language preference, and differential satisfaction and secondary victimisation reports across groups. Equity monitoring is important because digital risk and recovery capacity are patterned by exposure, resources, and the ability to navigate complex systems, and system design can either reduce or amplify these disparities (Cross et al., 2016; Home Office, 2025).

7. CONCLUSION

This review synthesised multidisciplinary evidence on cybercrime victimisation to show that cyber harms are rarely limited to financial loss. Across offence types, victims experience multi domain impacts that include psychological distress, fear, anger, shame, loss of control, social withdrawal, relationship strain, reputational anxiety, and a recovery burden that can persist long after the initial incident. Harm severity is shaped by offence mechanics and the degree of offender victim interaction, including persuasion, grooming, coercion, and continued contact. It is also shaped by uncertainty about ongoing exposure and by whether the consequences are reversible, particularly in account compromise and image based abuse contexts. The synthesis also demonstrates that reporting and help seeking are best understood as pathways rather than single decisions. Victims weigh stigma, self-blame, procedural burden, and perceived futility, and their willingness to persist is strongly influenced by institutional responsiveness. Fragmentation across police, banks, telecom providers, and platforms can increase victim effort and delays, raise the risk of secondary victimisation and erode institutional trust. In contrast, coordinated response, clear communication, and respectful procedural justice oriented interactions can function as harm reduction interventions, improving both victim wellbeing and cooperation.

The integrative framework proposed in this review links routine exposure and guardianship failures to offence processes, victim appraisal and coping, system response quality, and long tail outcomes. It provides a practical lens for designing victim centred cybercrime systems that prioritise rapid containment in financial fraud, specialised pathways for coercion and interpersonal abuse, and accessible, multilingual reporting interfaces that reduce repeated retelling. For India, existing mechanisms such as 1930 and the National Cybercrime Reporting Portal provide a strong foundation, but implementation priorities should focus on single case journey integration, time bound response standards, and capacity building that emphasises triage, evidence preservation, and trauma informed communication. Future research should develop standardised measures of multi domain cyber victim impact, generate longitudinal evidence on

recovery and trust trajectories, and evaluate integrated response models across police, banks, and platforms, including equity impacts by gender, age, socioeconomic status, and digital literacy. Strengthening cybercrime response therefore requires not only better detection and enforcement, but also victim centred system design that prevents secondary harm and restores agency, safety, and trust.

References

1. Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology, 8*(1), 19–32. doi:10.1080/1364557032000119616
2. Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: A literature review and future research directions. *Journal of Digital Social Research, 3*(3), 88–113.
3. Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime victimization: A literature review and future research directions. *Journal of Digital Social Research, 3*(3), 93–114.
4. Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36–54. doi:10.1057/sj.2012.11
5. Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.). Pearson Education.
6. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.
7. Colburn, D. A., Finkelhor, D., & Turner, H. A. (2023). Help seeking from websites and police in the aftermath of technology facilitated victimization. *Journal of Interpersonal Violence, 38*(21–22), 11642–11665. https://doi.org/10.1177/08862605231186156
8. Colburn, D. A., Finkelhor, D., & Turner, H. A. (2023). Help seeking from websites and police in the aftermath of technology facilitated victimization. *Journal of Interpersonal Violence, 38*(21–22), 11642–11665. doi:10.1177/08862605231186156
9. Colburn, D., Finkelhor, D., & Turner, H. A. (2023). Help seeking from websites and police in the aftermath of technology facilitated interpersonal victimization. *Journal of Interpersonal Violence, 38*(5–6), 4182–4203. doi:10.1177/08862605211062913
10. Cross, C., Richards, K., & Smith, R. G. (2016). *Improving responses to online fraud victims: An examination of reporting and support needs*. Australian Institute of Criminology.
11. Cross, C., Richards, K., & Smith, R. G. (2016). *Improving responses to online fraud victims: An examination of reporting and support needs* (Research report). Australian Institute of Criminology.
12. Cross, C., Smith, R. G., & Richards, K. (2014). *Challenges of responding to online fraud victimisation in Australia* (Trends & Issues in Crime and Criminal Justice No. 474, pp. 1–6). Australian Institute of Criminology.
13. De Kimpe, L., Walrave, M., Ponnet, K., & Hardyns, W. (2020). Cybercrime victimization and its impact on individual health: The role of coping and the moderating effect of age. *Cyberpsychology, Behavior, and Social Networking, 23*(7), 484–490. doi:10.1089/cyber.2019.0742
14. Dennehy, R., Meaney, S., Walsh, K. A., Sinnott, C., & Cronin, M. (2020). Young people's conceptualizations and experiences of cyberharassment: A qualitative study. *BMC Public Health, 20*, 733. doi:10.1186/s12889-020-08841-7

15. Department of Telecommunications. (n.d.). *Central Equipment Identity Register (CEIR)*. Government of India.
16. Dodel, M., Kaiser, J., & Mesch, G. (2020). Determinants of cyber safety behaviors in a developing economy. *First Monday, 25*(7).
17. Federal Trade Commission. (2025). *Consumer Sentinel Network data book 2024*. Federal Trade Commission.
18. Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders, 6*(4), 386–398. doi:10.1080/15564886.2011.607402
19. Hellevik, P. M., Haugen, L. E. A., & Överlien, C. (2025). Outcomes of image based sexual abuse among young people: A systematic review. *Frontiers in Psychology, 16*, 1599087. doi:10.3389/fpsyg.2025.1599087
20. Herman, J. L. (1992). *Trauma and recovery: The aftermath of violence from domestic abuse to political terror*. BasicBooks.
21. Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25. doi:10.1080/01639620701876577
22. Home Office. (2025). *Cyber security breaches survey 2025*. Home Office.
23. Home Office. (2025). *Experiences of victims of fraud and cyber crime*. Home Office.
24. Home Office. (2025). *Experiences of victims of fraud and cyber crime*. Home Office.
25. Hong, Q. N., Gonzalez Reyes, A., & Pluye, P. (2018). Improving the usefulness of a tool for appraising the quality of qualitative, quantitative, and mixed methods studies: The Mixed Methods Appraisal Tool (MMAT). *Journal of Evaluation in Clinical Practice, 24*(3), 459–467.
26. Indian Cyber Crime Coordination Centre. (n.d.). *National Cybercrime Reporting Portal (NCRP)*. Ministry of Home Affairs, Government of India.
27. Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into the impact and change. *Qualitative Criminology, 6*(2), Article 5.
28. Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology, 6*(2), 205–228.
29. Khan, F. A., Jameel, M., Sarwar, B., Awan, M. I., & Ahmad, A. (2023). Effects of socio economic and digital inequalities on cybersecurity behavior: A comparative analysis between developed and developing economies. *Security Journal*. doi:10.1057/s41284-023-00375-4
30. Koning, L., Junger, M., & Veldkamp, B. (2025). Reporting fraud victimization to the police: Factors that affect whether victims report. *Policing and Society*. doi:10.1080/1068316X.2025.2468347
31. Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.
32. Lea, S. E. G., Fischer, P., & Evans, K. (2009). *The psychology of scams: Provoking and committing errors of judgement*. Office of Fair Trading.
33. Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. doi:10.1080/01639625.2015.1012409
34. Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: Advancing the methodology. *Implementation Science, 5*, 69. doi:10.1186/1748-5908-5-69
35. National Cybercrime Reporting Portal. (n.d.). *Citizen Financial Cyber Frauds Reporting and Management System instructions*.

36. Office for National Statistics. (2025, December 17). *Improving the quality of fraud and computer misuse statistics in England and Wales: December 2025* (Action plan). Office for National Statistics.
37. Office for Statistics Regulation. (2025, April 3). *Review of fraud and computer misuse statistics for England and Wales*. Office for Statistics Regulation.
38. Orth, U. (2002). Secondary victimization of crime victims by criminal proceedings. *Social Justice Research, 15*(4), 313–325. doi:10.1023/A:1021210323461
39. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. doi:10.1136/bmj.n71
40. Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *SAGE Open, 11*(4). doi:10.1177/21582440211061556
41. Palassis, C., Koleoso, J., & Alshahwan, N. (2021). The psychological impact of cybercrime: A systematic review. *Journal of Criminal Psychology, 11*(2), 113–128. doi:10.1108/JCP-11-2020-0048
42. Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K., & Duffy, S. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews* (Version 1). ESRC Methods Programme.
43. Press Information Bureau. (2025, October 8). *Curbing cyber frauds in Digital India*. Government of India.
44. Rodríguez, A., et al. (2025). Romance fraud: Its repercussions on victims' wellbeing. *Journal of Elder Abuse & Neglect*. doi:10.1080/08974454.2025.2600304
45. Shapland, J., & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology, 14*(2), 175–217. doi:10.1177/026975802070000202
46. Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM, 54*(3), 70–75. doi:10.1145/1897852.1897872
47. Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology, 8*, 45. doi:10.1186/1471-2288-8-45
48. Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., et al. (2018). PRISMA extension for scoping reviews (PRISMA ScR): Checklist and explanation. *Annals of Internal Medicine, 169*(7), 467–473. doi:10.7326/M18-0850
49. Tyler, T. R. (1990). *Why people obey the law*. Yale University Press.
50. Tyler, T. R. (1990). *Why people obey the law*. Yale University Press.
51. Tyler, T. R., & Huo, Y. J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts*. Russell Sage Foundation.
52. Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking, 15*(3), 181–183. doi:10.1089/cyber.2011.0352
53. Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims, both financial and non financial. *Criminology & Criminal Justice, 16*(2), 176–194. doi:10.1177/1748895815603773
54. Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R. (2017). Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *SAGE Open, 7*(2). doi:10.1177/2158244017710292
55. Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427. doi:10.1177/147737080556056