Research Article

From Impersonation to Sextortion: A Thematic Case Study of Cyber Enabled Sexual Harassment in Tamil Nadu

Ms. Prabha A[1]*, Prof. Dr. Beulah Shekhar[2]

Abstract

Cyber enabled sexual harassment and blackmail are often discussed as online nuisance or moral risk, yet victim narratives show a patterned escalation that produces intense psychological and social harm. This paper presents a qualitative single case study from a district in Tamil Nadu, drawn from a larger mixed methods doctoral study of cybercrime victimisation in three southern districts. Using a semi structured interview and thematic analysis, the case is analysed as an escalation pathway. The findings show seven linked stages, trust entry through impersonation cues, boundary testing and forced intimacy demands, escalation to sexual harassment and demands for explicit reciprocity, persistence through anonymity and repeated identity switching, evidence fragility linked to disappearing chats and restricted capture, coercion through reputational threat and blackmail, and coping through evidence workarounds and formal reporting. The case highlights how platform conditions can amplify harm by limiting evidence preservation at the point of crisis, and how low feedback during early complaint processing can prolong distress. The paper argues for a victim centred first response model that combines rapid evidence preservation guidance, platform cooperation for traceability and secure export, and trauma informed communication in cybercrime reporting pathways.

Keywords: *cyber victimisation, sextortion, image based sexual abuse, online sexual harassment, coercive control, thematic analysis*

Introduction

Digital communication platforms have become central to everyday life, but they have also created a high frequency setting where cyber enabled victimisation can occur through routine social interactions. Importantly, cybercrime harms are not limited to direct monetary loss. Evidence reviews and victim studies show that many victims experience psychological distress, behavioural change, and longer term vigilance even when financial recovery is possible (Jansen & Leukfeldt, 2018; Wright et al., 2023). Recent public health oriented research on scam and fraud victimisation similarly documents emotional sequelae such as shame, guilt, anger, helplessness, and fear, alongside anxiety and depressive symptoms (Balcombe et al., 2025).

Within this broader harm landscape, image related offences and sexualised online coercion represent a particularly damaging category because the threat mechanism targets dignity, reputation, and social belonging. Image based sexual abuse refers to the creation, taking, sharing, or threatening to share intimate images without consent, and is widely recognised as a form of psychological abuse that can be used to induce shame, humiliation, and control (Umbach & Henry, 2025). Sextortion, which is often nested within this broader umbrella, is commonly defined by three core elements: a threat to distribute intimate images, a demand attached to that threat, and a coercive intent that may involve money, sexual acts, additional images, or other compliance (Ray et al., 2025). These offences operate

[1] PhD Scholar, Reg. No. 18214012042057, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, India
[2] Adjunct Professor, Parul Institute of Liberal Arts, Parul University, India

through stigma and social risk. The victim's primary fear may be exposure to family, peers, employers, or community networks, which can produce silence, delayed disclosure, and constrained help seeking. A second factor that can intensify harm is evidence fragility. Platform affordances such as ephemeral messaging, limited identifiers, and rapid account switching can complicate documentation and slow containment, particularly during the first hours when victims are trying to preserve proof and decide whether to report (Umbach & Henry, 2025). When evidence capture is obstructed, victims may resort to improvised workarounds, and the perceived gap between lived victimisation and actionable evidence can heighten helplessness and uncertainty. This matters because victim coping and recovery are shaped not only by the offence itself, but also by the practical ability to stop contact, preserve evidence, and navigate reporting pathways (Jansen & Leukfeldt, 2018).

Although scholarship on cyber victimisation has expanded, many studies still prioritise prevalence, typologies, and broad risk correlates, with less attention to process level escalation in sexualised coercion cases, meaning how contact begins, how boundary testing progresses into harassment, and how threats are introduced to extract compliance. Scoping work on sextortion highlights the diversity of offender contexts and the centrality of coercive control dynamics, but also points to definitional inconsistency and the need for clearer mechanism focused analyses that support prevention and response design (Ray et al., 2025). In parallel, ongoing international cybercrime governance emphasises the central challenge of electronic evidence and cross platform investigative needs, reinforcing the operational importance of early evidence preservation and coordinated response (Council of Europe, 2001).

This paper addresses these gaps through an in depth qualitative case study from a district, Tamil Nadu. The case is analysed as an escalation pathway, from initial entry and forced intimacy demands, to sexual harassment, persistence through renewed identities, and coercion through reputational threats. By centring the victim's account and the evidence barriers encountered, the study aims to generate actionable insights for victim centred first response guidance, platform level evidence support, and trauma informed reporting communication.

In the sections that follow, the methodology outlines the case study design and thematic analysis approach. The findings present the sequential themes that map escalation and coping. The discussion then interprets the case in relation to cyber harm scholarship and outlines practical implications for cybercrime reporting systems and victim support protocols.

Review of Literature

Cybercrime victimisation research shows that harm extends beyond direct monetary loss and can include sustained emotional, cognitive, and behavioural impacts. Qualitative work on online banking fraud victims found that impacts range from minimal disruption to severe distress, and that some victims report lasting changes such as reduced trust in others and reduced confidence in their own abilities (Jansen & Leukfeldt, 2018). Complementing this, recent research synthesising evidence on cybercrime victimisation highlights that psychological impact is shaped by both personal factors and incident circumstances, and that victims may experience continuing fear, stress, and altered routines even after the incident ends (Borwell et al., 2024).

A closely related stream focuses on technology facilitated sexual violence, especially image based sexual abuse and sextortion. Image based sexual abuse is widely conceptualised as nonconsensual creation, distribution, or threat of distribution of intimate images, and is consistently associated with shame, fear, reputational anxiety, and social withdrawal. Large scale cross national evidence indicates that such victimisation is common, and that victims report substantial negative impacts and often do not disclose or formally report their experiences (Umbach et al., 2025). Sextortion research further clarifies that the defining mechanism is coercion through threats of exposure linked to a compliance demand, and that cases can involve demands for additional sexual content, sexual acts, money, or ongoing access, often coupled with persistent intimidation (Ray & Henry, 2025).

Studies of online pursuit and harassment help explain why many victims struggle to stop contact. Cyberstalking scholarship using lifestyle and routine activity approaches shows that everyday online routines, exposure, and weak guardianship conditions can increase victimisation risk, while offender anonymity and low cost identity changes support persistence after blocking (Reyns et al., 2011). In sexualised coercion cases, persistence can be understood through coercive control dynamics, where repeated boundary violations and intimidation operate as strategies of domination rather than communication, and where the threat of social harm is used to compel compliance (Stark, 2007). This lens is particularly relevant in contexts where stigma and reputational consequences are severe, since perceived social fallout can become the core vulnerability exploited by offenders (Ray & Henry, 2025; Umbach et al., 2025).

Another practical issue highlighted across cyber harm literature is the role of electronic evidence and how its fragility shapes reporting and response. Cyber incidents often produce evidence that is volatile, distributed across platforms, and dependent on timely preservation, which creates barriers for victims at the very stage when they are trying to document abuse and seek help (Council of Europe, 2001). When victims cannot reliably preserve messages, identifiers, or interaction history, they may delay disclosure, feel helpless, or anticipate disbelief. This is consistent with victim coping research, where perceived controllability influences whether people use problem focused actions, emotion focused coping, or avoidance (Lazarus & Folkman, 1984). In cyber contexts, coping frequently includes attempts to block, document, and seek institutional assistance, but these efforts depend heavily on platform affordances and the clarity of reporting pathways (Jansen & Leukfeldt, 2018).

Taken together, the literature supports a process oriented understanding of cyber enabled sexual harassment and blackmail, where incidents unfold through stages of access, boundary testing, persistence, and coercion, and where harm is intensified by stigma, evidence barriers, and uncertainty in early institutional response. However, there remains limited case based work that integrates escalation dynamics, evidence fragility, coping, and early reporting experience into a single analytic narrative, particularly within district level Indian contexts. This article addresses that gap by presenting a detailed case as an escalation pathway and linking it to victim centred response needs.

Methodology

Study design

This paper uses a qualitative case study design, focusing on one detailed victim narrative from a district in Tamil Nadu. The case is drawn from a larger convergent mixed methods doctoral study in which quantitative survey data and qualitative case interviews were collected in the same period, analysed separately, and integrated during interpretation. The present article isolates the case to generate process level insight into escalation, harm, coping, and reporting.

Case study methodology is appropriate when the aim is to understand a contemporary phenomenon within its real world context and to explain how and why experiences unfold over time (Yin, 1994). The design also aligns with interview based case enquiry commonly used to capture sequence, meaning, and institutional interaction (Fowler & Mangione, 1990).

Study setting

The parent study was conducted in three southern districts of Tamil Nadu, namely. For this article, the single focal case is from one of the district, selected to provide an in depth account of cyber enabled harassment and coercion within the local socio cultural and policing context.

Population and eligibility

The target population for the parent study comprised adult cybercrime victims residing in the selected districts. Inclusion criteria included age eighteen years or above, residence in the study district at the time of the incident, self identification as a direct victim of a cybercrime incident, ability to understand Tamil or English, and willingness to provide informed consent. Individuals below eighteen, indirect victims, and persons in acute psychological crisis where participation could intensify distress were excluded.

Case selection for the present paper

The qualitative strand of the thesis used three case interviews drawn from the same victim pool to capture depth and variation. The case was purposively selected for the present article because it illustrates an escalation pathway involving persistent contact, sexual harassment, coercive threats, and practical difficulties in evidence preservation. This made it analytically suitable for examining mechanisms rather than prevalence.

Data collection

Data for the case study were generated using a semi structured interview schedule. The interview guide covered the following domains:

1. Personal background and digital habits before the incident
2. Detailed narrative of the cyber incident and its sequence
3. Immediate emotional and behavioural reactions
4. Disclosure patterns and responses from family or peers
5. Decision making regarding reporting or non reporting
6. Experiences with police, cyber cells, banks, or digital platforms
7. Longer term psychological, social, and economic consequences
8. Coping strategies and protective actions
9. Reflections, advice to other victims, and expectations from institutions

Interviews were conducted in Tamil or English based on participant preference. With consent, interviews were audio recorded. Where recording was not feasible, detailed notes were taken. Recordings were transcribed verbatim. Tamil interviews were translated into English with attention to meaning preservation. All transcripts were anonymised by removing names and identifying details.

Data analysis

The analysis followed a staged qualitative procedure that moves from organising the narrative to coding, pattern building, and interpretive theme development. The approach is consistent with case study analytic logic where empirical material is linked to propositions and interpreted through patterned meaning, rather than treated as isolated statements (Miles & Huberman, 1994; Yin, 1994). Coding proceeded iteratively, beginning with descriptive codes for incident stages, offender tactics, victim reactions, coping actions, and institutional interaction, followed by clustering into higher order themes that represent the escalation pathway. The final write up reports themes in a sequential structure to preserve process, and uses selected anonymised extracts to illustrate meaning. Practical guidance on staged case analysis for interview based case sets also informed the analytic workflow (Atkinson, 2002).

Trustworthiness and rigour

The credibility was supported through cautious transcription, keeping the field notes, and cross checking of interpretations with academic supervision. Where possible, the participant was invited to check whether a brief summary of their narrative resonated with their experience. Dependability was maintained by keeping a clear audit trail of coding decisions, theme refinement, and excerpt selection. Transferability was maintained provided that contextual details about setting, event features, and reporting context so that readers can judge relevance to similar cases.

Ethical considerations

For the parent study, ethical approval was obtained from the researcher’s university, Institutional Ethics Committee. Participation was voluntary and based on informed consent. The participant was informed about their rights to withdraw at any time, and the researcher remained attentive to distress during interviewing, pausing or stopping when and wherever required. Confidentiality was kept through total anonymisation of the subject.

Findings and Analysis

Case overview

The case demonstrates a distinct escalation process in which initial contact progressively developed into ongoing harassment, followed by compulsion through reputational harm. The victim narrative demonstrates how platform-level evidentiary hurdles and perpetrator anonymity influenced the victim's decision to seek treatment as well as the severity of their pain. Research on image-based sexual abuse and sextortion, where threats of social exposure and intimidation serve as the primary control mechanism, has extensively examined similar escalation logics (Ray et al., 2025; Umbach & Henry, 2025).

Theme 1: Trust entry through impersonation and plausibility cues

The contact strategy used in the first stage seemed credible enough to hold the victim's attention for a short period of time. This phase is important because it reduces suspicion at once and creates space for further interactions. When motivated criminals take benefit of common communication patterns and the apparent security of mediated contact, routine online engagement may turn into a gateway for victimization (Cohen & Felson, 1979; Reyns et al., 2011). In this case, the offender's primary approach resulted in uncertainty and confusion rather than an instant refusal, allowing access to continue.

Theme 2: Boundary testing and forced intimacy demands

The perpetrator started testing boundaries and forcing relational expectations after entering. According to the victim, there was continuous pressure that viewed refusal as negotiable. This is like the dynamics of coercive control, where resistance is gradually worn and intrusion regularized by persistence and common boundary violations (Stark, 2007; Umbach & Henry, 2025). The victim's emotional reaction quickly shifted from confusion to anger and frustration, but the perpetrator continued despite the victim's refusal, suggesting that dominance rather than engagement was the intended outcome.

Theme 3: Escalation to sexual harassment and demands for explicit reciprocity

Unwelcome sexualised conversation and the sharing of obscene images were among the indicators of harassment that emerged as the interaction continued. The perpetrator also insisted that the victim send similar content. Offenders commonly use explicit content in sextortion pathways to pressure victims into exchanging images, which later serves as leverage for further threats (Ray et al., 2025). According to the victim narrative, the attacker was not deterred by even firm opposition. This shows how online sexual harassment can operate as a phased process, progressing from harassment to the creation of leverage material and ultimately to coercion.

Theme 4: Persistence through anonymity and identity switching

Persistence was an important part of the case. Because the offender reappeared using various different identities or accounts, blocking did not stop the communication. This goes hand in hand with research on cyberstalking and harassment showing that anonymity and low cost identity switching allow perpetrators to sustain contact, escalate intrusion, and drain victim coping resources (Reyns et al., 2011; Sheridan & Grant, 2007). Repeated re-entry heightened the victim's sense of powerlessness and continuing threat.

Theme 5: Evidence fragility and the growth of helplessness

The victim reported difficulty capturing evidence, which includes restrictions on screenshots or screen recordings and the disappearance of chats. Evidence fragility is a recognized challenge in digital sexual harassment cases, and it can discourage reporting because victims expect that authorities will request proof that is hard to preserve (Council of Europe, 2001; Umbach & Henry, 2025). In this case, the inability to preserve evidences operated like a second layer of harm. It increased anxiety and also forced the victim to adopt improvised documentation strategies.

Theme 6: Coercion through reputational threat and blackmail

When the culprit threatened to share the chats and photos public if the victim did not comply, the case reached a key point. This combination, a threat of exposure, a demand for compliance, and coercive intent, is what describes sextortion (Ray et al., 2025). The victim's fear is largely reputational and social, which aligns with image based abuse literature where stigma and shame are used as the offender's most effective weapon (Umbach & Henry, 2025). This stage produced the highest psychological strain because the victim had to weigh safety, dignity, and family consequences.

Theme 7: Coping actions, leverage strategies, and reporting experience

The victim tried to preserve documentation by recording the interaction on another device despite evidentiary hurdles. The victim sought practical solutions while constrained, which reflects a problem focused coping response (Lazarus & Folkman, 1984). By mentioning a police connection, the victim also used deterrence leverage, which immediately reduced communication with the offender. The victim later filed a complaint, but the early experience was marked by low feedback and uncertainty, with the status remaining under processing. Research on cybercrime victims indicates that lack of timely communication and unclear progress updates can prolong distress and reduce trust, even when cases remain under investigation (Jansen & Leukfeldt, 2018; Wright et al., 2023).

Summary of the escalation pathway

Entry and plausibility, boundary testing, sexual harassment and reciprocity demands, persistence through identity switching, disruption of evidence, coercion through exposure threats, and victim coping through reporting and evidence workaround are some of the themes that demonstrate a sequential escalation pattern in this case. This pathway demonstrates that cyber enabled sexual harassment is best understood as a process of control, not a single incident. It also shows how platform conditions and early institutional communication can amplify or reduce harm.

Discussion

This case shows cyber enabled sexual harassment as a staged process of access, boundary erosion, persistence, and coercion. The sequence matters because it explains why victims often describe the incident as escalating rather than sudden. It also clarifies where prevention and institutional intervention can interrupt harm.

First, the entry and boundary testing stages demonstrate how everyday online routines can become risk contexts. Routine Activity Theory helps explain this pattern, since victimisation becomes more likely when a motivated offender encounters a suitable target in a setting with weak guardianship, here meaning limited platform traceability and limited immediate support around the victim (Cohen & Felson, 1979). The offender's repeated disregard for refusal also aligns with coercive control logic, where persistence and domination are the goal, not mutual interaction (Stark, 2007). This framing shifts the emphasis from individual blame to offender tactics and situational risk.

Second, the fundamental process of sextortion and image based sexual abuse is seen in the shift from harassment to overt coercion. The primary weapon used by the offender is the threat of exposure, which exploits stigma, social sanctions, and humiliation. This aligns with research showing that reputational threat and shame are key drivers in sextortion pathways that shape compliance (Ray et al., 2025; Umbach & Henry, 2025). Because the victim perceives the risk as socially catastrophic, the case also shows that the threat alone can produce substantial psychological strain even without verified image possession.

Third, the fragility of evidence becomes a separate source of harm. Powerlessness and the need to use improvised evidence solutions resulted from the victim's inability to preserve proof due to platform limitations and disappearing communications. This is significant because electronic evidence is vital for cybercrime action, yet it is often volatile, distributed, and platform dependent, which limits victim reporting and investigative response (Council of Europe, 2001). The case suggests that early evidence preservation guidance is not only an investigative necessity, it is also a victim support intervention because it helps restore a sense of control.

Fourth, the case shows how institutional response is felt through communication, not just through case outcomes. Consistent with a broader body of research on cybercrime victims linking emotional harm to post event uncertainty and perceived procedural opacity, a complaint status kept under processing with limited feedback can raise distress and reduce trust (Jansen & Leukfeldt, 2018; Wright et al., 2023). From a victim centred policing perspective, short but dependable updates can ease anxiety and strengthen reporting confidence even when investigations take time.

Finally, coping responses in the case show problem focused adaptation under constraint. The victim documented evidence using another phone and used deterrence leverage by invoking a police connection. These actions reflect coping theory, where individuals attempt to manage threat through practical control strategies when emotional processing alone is insufficient (Lazarus & Folkman, 1984). However, it is not reasonable to expect all victims to have such leverage or digital improvisation skills. This reinforces the need for standardised first response protocols and accessible victim guidance.

Conclusion

The case demonstrates that cyber enabled sexual harassment and blackmail should be understood as an escalation pathway driven by coercive control and reputational threat, rather than as a single incident. Platform level evidence fragility and offender persistence through identity switching intensified harm and constrained the victim's reporting readiness. The early reporting experience, marked by limited feedback, became part of the post incident distress.

Practical implications

1. Develop a simple first hour response protocol for victims that prioritises safety, blocking and reporting steps, and evidence preservation actions that work across common platforms.
2. Strengthen platform evidence support by promoting secure export options and clearer traceability for verified complaints, while protecting privacy.
3. Improve victim centred communication in cyber complaint processing through acknowledgement, realistic timelines, and brief periodic updates.
4. Train frontline responders in trauma informed handling for stigma sensitive cases involving sexual harassment, reputational threat, and blackmail.

Limitations and future scope

This article is based on a single case study, so findings are not statistically generalisable. The contribution is analytic generalisation, meaning the case clarifies mechanisms of escalation, coercion, and evidence barriers that can inform future multi case qualitative work and mixed methods designs. Future research should compare similar cases across districts and platforms, and should examine how reporting channels, response timelines, and platform cooperation shape harm reduction and recovery outcomes.

References

- Balcombe, L. (2025). *The mental health impacts of internet scams*. *International Journal of Environmental Research and Public Health, 22*(6), 938. https://doi.org/10.3390/ijerph22060938
- Borwell, J., Jansen, J., & Stol, W. (2024). The psychological impact of cybercrime victimization. *European Journal of Criminology*.
- Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). Council of Europe.
- Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization, an exploratory study into impact and change. *Qualitative Criminology, 6*(2).
- Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.
  Ray, A., & Henry, N. (2024). Sextortion: A Scoping Review. *Trauma, Violence, & Abuse*, *26*(1), 138-155. https://doi.org/10.1177/15248380241277271 (Original work published 2025)
- Stark, E. (2007). *Coercive control, how men entrap women in personal life*. Oxford University Press.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends, a routine activity approach. *American Sociological Review, 44*(4), 588–608.
- Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185, Budapest, 23.XI.2001). Council of Europe.
- Fonseca, C. C., Moreira, S., & Guedes, I. (2022). Online consumer fraud victimization and reporting, a quantitative study of the predictors and motives. *Victims & Offenders, 17*(5), 756–780. https://doi.org/10.1080/15564886.2021.2015031
- Fowler, F. J., Jr., & Mangione, T. W. (1990). *Standardized survey interviewing, minimizing interviewer related error*. Sage.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis, an expanded sourcebook* (2nd ed.). Sage Publications.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online, applying cyberlifestyle routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149–1169.
- Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13*, 627–640. https://doi.org/10.1080/10683160701340528
- Umbach, R., Henry, N., & Beard, G. (2025). Prevalence and impacts of image based sexual abuse victimization, a multinational study. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (CHI '25). Association for Computing Machinery. https://doi.org/10.1145/3706598.3713545
- Yin, R. K. (1994). *Case study research, design and methods* (2nd ed.). Sage Publications.