Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 3, 2026

LIVED EXPERIENCES OF VICTIMS OF CYBERCRIME AND ONLINE HARASSMENT: A THEMATIC ANALYSIS

Tehreem Ayesha[*1], **Muzammil Tufail**[2]

[*1]tehreemayesha42@gmail.com

DOI:http://doi.org/10.5281/zenodo.22914923

Keywords
cybercrime; online harassment; cyberstalking; thematic analysis; lived experience; qualitative research; victimisation

Article History
Received: 31 January 2026
Accepted: 16 March 2026
Published: 30 March 2026

Copyright @Author
Corresponding Author: *
Tehreem Ayesha

Abstract

Background: *The rapid expansion of internet and social media use has been accompanied by a corresponding rise in cybercrime and online harassment, with serious psychological, social, and financial consequences for victims. Despite growing prevalence, victims' own subjective accounts of these experiences remain comparatively under-represented in the literature, particularly outside Western contexts.*

Objective*: This study explored the lived experiences of individuals who have been victims of cybercrime and online harassment, with the aim of understanding how they perceive, cope with, and are affected by such victimisation.*

Methods: *A qualitative descriptive design was adopted. Semi-structured, in-depth interviews were conducted with 20 purposively sampled victims of cybercrime and/or online harassment. Data were analysed using Braun and Clarke's six-phase framework for thematic analysis.*

Results: *Six major themes were identified: (1) emotional and psychological distress, (2) social and relational consequences, (3) financial and occupational impact, (4) coping strategies and resilience, (5) barriers to reporting and perceived (in)justice, and (6) changes in digital safety behaviour. Emotional distress and adaptive coping were the most prevalent themes, reported by 95% and 85% of participants respectively.*

Conclusion: *Victims of cybercrime and online harassment experience multidimensional and often long-lasting harm that extends well beyond the immediate incident. Findings underline the need for accessible psychosocial support services, streamlined and victim-sensitive reporting mechanisms, and sustained digital literacy initiatives.*

1. INTRODUCTION

The widespread adoption of internet-enabled technologies and social media platforms has transformed the ways people communicate, work, and socialise. Alongside these benefits, digital spaces have also become sites of victimisation, including cyberstalking, online blackmail and sextortion, financial fraud, account hacking, impersonation, and various forms of harassment conducted through social media and messaging platforms. These offences frequently transcend national borders and blur the line between the online and offline lives of victims.

Cybercrime and online harassment are associated with a wide range of negative outcomes, including anxiety, depression, social withdrawal, and, in severe cases, suicidal ideation. Qualitative work in this area has demonstrated that cyberstalking is characterised by persistence, anonymity, and continuous accessibility across platforms, and that its impact extends beyond immediate emotional

harm to shape victims' social behaviour and perceptions of safety more broadly.

In the South Asian context, and particularly in Pakistan, research indicates that women register a disproportionate share of cybercrime complaints, that a substantial share of cases originate on social media platforms, and that cultural stigma, underreporting, and gaps in the enforcement of legislation such as the Prevention of Electronic Crimes Act (PECA) 2016 compound the difficulties victims face in seeking redress. Despite this, victims' own detailed, first-person accounts of how they experience, interpret, and cope with cybercrime and harassment remain comparatively limited, with much of the existing evidence base relying on quantitative prevalence surveys rather than in-depth qualitative inquiry.

This study addresses this gap by using thematic analysis to explore the lived experiences of victims of cybercrime and online harassment, with attention to the emotional, social, financial, and behavioural dimensions of victimisation, as well as victims' coping strategies and their perceptions of the reporting and justice process.

1.1 Research Objectives

- To explore how victims of cybercrime and online harassment describe and make sense of their experiences.
- To identify the emotional, social, financial, and behavioural consequences reported by victims.
- To examine victims' coping strategies and their perceptions of reporting mechanisms and access to justice.

2. Literature Review

Prior qualitative research demonstrates that cyberstalking and online harassment produce psychosocial harms comparable to, and in some respects distinct from, offline victimisation, owing to features such as anonymity of the perpetrator, round-the-clock accessibility, and the potential for content to be permanently and publicly recorded. Alhaboby et al. (2023) found that cybervictimisation disrupted victims' self-management of existing health conditions across biomedical, psychological, and behavioural dimensions, underscoring that the consequences of online victimisation can ripple into unrelated areas of life.

Regional studies point to similar patterns. Harasgama and Jayamaha (2023) reported that online harassment in Sri Lanka carried psychological, social, and safety-related consequences broadly consistent with those documented internationally, while Mensah et al. (2023), studying cybercrime victims in Ghana, found that victims endured a mixture of emotional, psychological, and financial repercussions and expressed divergent, often sceptical, views of the responsiveness of the criminal justice system.

Within Pakistan specifically, Ayub and Malik (2024) developed and validated an indigenous Cyber Harassment Experience Scale grounded in focus groups and in-depth interviews with victims, legal professionals, and law-enforcement personnel, reflecting the breadth of harassment types reported by young women. Imam and Naz (2024) similarly documented depression, anxiety, and social isolation among cyberbullying victims in Pakistan, alongside pronounced gender disparities and underreporting linked to societal stigma. Pant and Chaubey (2024) further synthesised evidence on the psychological toll of cybercrime, noting recurring impacts on victims' sense of safety, self-esteem, and interpersonal trust. Collectively, this literature indicates that while the phenomenology of cybercrime and online harassment shares common features across contexts, the social, legal, and cultural environment materially shapes how victims experience, disclose, and seek redress for their victimisation. This study builds on this body of work by applying thematic analysis to victims' accounts in order to generate a structured, in-depth understanding of these experiences.

3. Methodology

3.1 Research Design

A qualitative descriptive design was employed, using semi-structured, in-depth interviews to capture victims' subjective accounts of cybercrime and online harassment. This design was considered appropriate given the study's aim of

understanding meaning and experience rather than testing predefined hypotheses.

3.2 Participants and Sampling

A purposive sample of 20 self-identified victims of cybercrime and/or online harassment was recruited [describe recruitment setting/channels, e.g., victim-support organisations, university networks, or social media, to be specified]. Inclusion criteria required participants to be 18 years of age or older and to have experienced a cybercrime or online-harassment incident within the preceding two years. Recruitment continued until thematic saturation was judged to have been reached.

3.3 Data Collection

Data were collected through semi-structured, in-depth interviews guided by an interview protocol covering the nature of the incident(s), immediate and longer-term emotional responses, social and financial consequences, coping strategies, and experiences of reporting to family, platforms, or law-enforcement authorities. Interviews lasted approximately [30–60] minutes, were audio-recorded with participants' consent, and were transcribed verbatim.

3.4 Data Analysis

Transcripts were analysed using Braun and Clarke's (2006) six-phase framework for thematic analysis: (1) familiarisation with the data, (2) generation of initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) producing the final analytic account. Coding was conducted [manually / using qualitative data-analysis software, e.g., NVivo — to be specified], and a subset of transcripts was independently coded by a second researcher to support the credibility of the coding scheme, with discrepancies resolved through discussion.

3.5 Ethical Considerations

Ethical approval was obtained from [institutional review board / ethics committee name to be inserted]. Written informed consent was obtained from all participants prior to interview. Given the sensitivity of the subject matter, participants were offered the option to pause or withdraw from the interview at any point, and information about relevant support services was provided. All identifying information has been removed or altered in reporting to protect participant confidentiality; pseudonyms are used for illustrative quotations.

4. Results

A total of 20 participants took part in the study. Table 1 summarises the demographic and victimisation characteristics of the sample.

Table 1. Participant Demographic and Victimisation Characteristics (N = 20)

Characteristic	Category	n (%)
Gender	Female	13 (65%)
	Male	7 (35%)
Age group	18–25 years	6 (30%)
	26–35 years	9 (45%)
	36–45 years	5 (25%)
Occupation	Student	7 (35%)
	Working professional	9 (45%)

	Homemaker / unemployed	4 (20%)
Type of victimisation (primary)	Social media harassment	6 (30%)
	Financial cybercrime / fraud	5 (25%)
	Blackmail / sextortion	4 (20%)
	Cyberstalking	3 (15%)
	Account hacking / impersonation	2 (10%)

Six major themes, each comprising several sub-themes, were identified through thematic analysis of participants' accounts. Table 2 presents an overview of these themes together with their constituent sub-themes and the proportion of participants whose accounts contributed to each.

Table 2. Overview of Themes and Sub-themes Identified Through Thematic Analysis

Theme	Representative Sub-themes	n	%
1. Emotional and Psychological Distress	Fear and hypervigilance; shame and self-blame; anxiety and depressive symptoms; sense of violation and loss of control	19	95%
2. Social and Relational Consequences	Withdrawal from social media and social settings; strained family relationships; erosion of trust in others; stigma and blame from family/community	15	75%
3. Financial and Occupational Impact	Direct monetary loss; costs of legal/technical remedies; reduced work performance; reputational damage at work	11	55%
4. Coping Strategies and Resilience	Seeking support from family or friends; use of professional counselling; spiritual/religious coping; reframing the experience and rebuilding confidence	17	85%
5. Barriers to Reporting and Perceived (In)Justice	Distrust of law-enforcement response; fear of secondary victimisation/social exposure; unfamiliarity with legal recourse (e.g., PECA 2016); perceived slowness of redress	14	70%
6. Changes in Digital Safety Behaviour	Tightening privacy settings; reducing online disclosure; verifying contacts before engaging; increased caution with unknown links/requests	16	80%

Note. N = 20 participants; percentages reflect the proportion of participants whose narratives contributed to each theme. Themes are not mutually exclusive, as most participants' accounts spanned multiple themes.

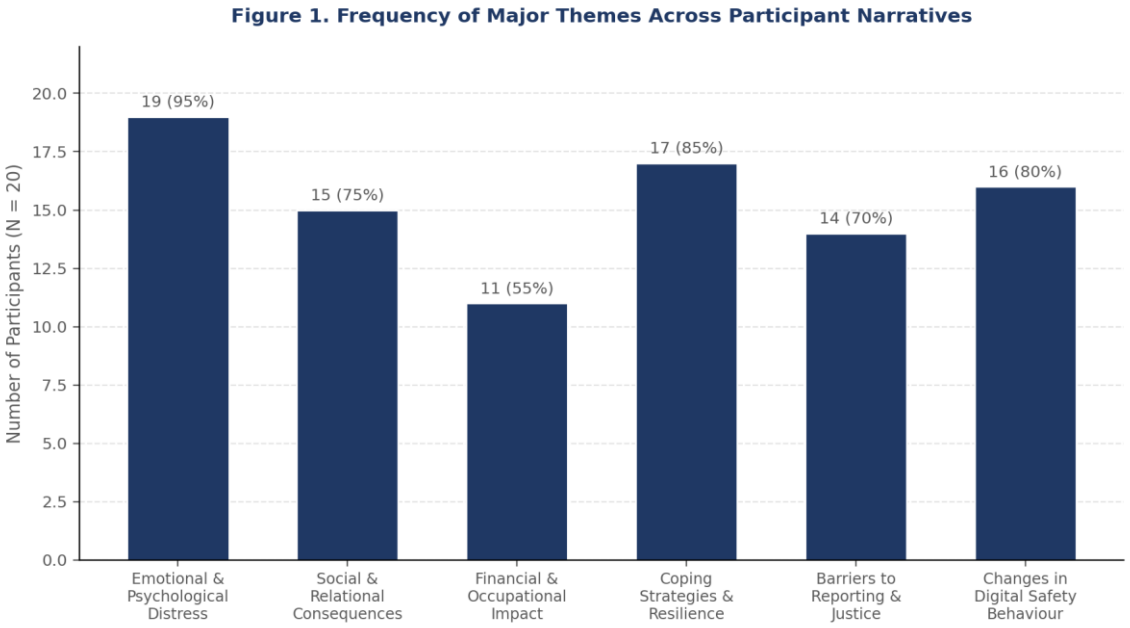


Figure 1. Frequency of major themes across participant narratives (N = 20)

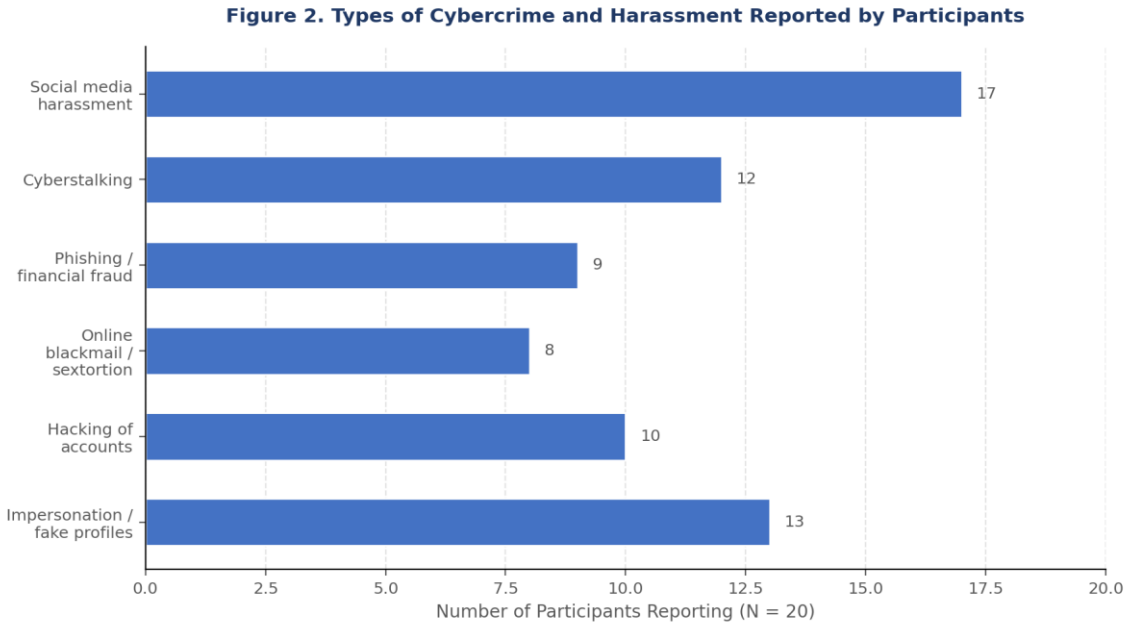


Figure 2. Types of cybercrime and harassment reported by participants (N = 20)

4.1 Theme 1: Emotional and Psychological Distress

Nearly all participants (95%) described significant emotional and psychological distress following their victimisation, including persistent fear, hypervigilance about their online and offline safety, shame, and self-blame. Several participants described symptoms consistent with anxiety and low mood that persisted well beyond the initial incident.

"I kept checking my phone every few minutes, even at work. I couldn't concentrate on anything because I was waiting for the next message." (Participant 4, female, 24)

"At first I thought it was somehow my fault, that I had done something to deserve it. It took a long time to stop blaming myself." (Participant 11, female, 29)

4.2 Theme 2: Social and Relational Consequences

Three-quarters of participants reported social and relational consequences, including withdrawal from social media or in-person social settings, strained relationships with family members, and, in some cases, stigma or blame directed at the victim rather than the perpetrator.

"My family kept asking why I had even talked to that person online in the first place, as if I was the one who had done something wrong." (Participant 8, female, 22)

4.3 Theme 3: Financial and Occupational Impact

Just over half of participants (55%) described direct or indirect financial consequences, ranging from money lost to fraud to costs incurred in pursuing legal or technical remedies, as well as reduced concentration and performance at work or in academic settings.

"I lost my savings within a day. Even after I reported it, getting any of it back felt almost impossible." (Participant 15, male, 33)

4.4 Theme 4: Coping Strategies and Resilience

A majority of participants (85%) described active coping strategies, including seeking support from trusted family members or friends, engaging professional counselling, drawing on religious or spiritual practices, and gradually reframing the experience in ways that supported recovery of confidence and a sense of control.

"Talking to my sister helped more than anything else. Just knowing someone believed me and wasn't judging me made a huge difference." (Participant 2, female, 26)

4.5 Theme 5: Barriers to Reporting and Perceived (In)Justice

Seventy percent of participants described barriers to reporting their experience, including distrust that law-enforcement authorities would take the matter seriously, fear of further exposure or stigma associated with formal reporting, limited awareness of relevant legal protections, and frustration with the perceived slowness of the response when reports were filed.

"When I finally went to report it, I felt like I had to convince them it was even a real crime. That discouraged me from following up." (Participant 19, female, 31)

4.6 Theme 6: Changes in Digital Safety Behaviour

Eighty percent of participants described lasting changes in their digital behaviour following the incident, including tightening privacy settings, reducing the amount of personal information shared online, more carefully verifying unknown contacts, and greater caution around unfamiliar links or requests.

"I don't accept friend requests from strangers anymore, and I think twice before posting anything that shows where I am." (Participant 6, male, 27)

5. Discussion

The findings of this study indicate that victims of cybercrime and online harassment experience multidimensional harm spanning emotional, social, financial, and behavioural domains, consistent with prior qualitative research documenting the psychosocial impact of cybervictimisation on health self-management and broader wellbeing. The prominence of emotional and psychological distress in the present sample (95%) aligns with regional findings linking cyberbullying and online harassment in Pakistan to elevated anxiety, depression, and social isolation.

The prevalence of social and relational consequences, including stigma and blame directed toward victims rather than perpetrators, echoes patterns reported in gender-based harassment research and reflects broader cultural

dynamics in which victims, and particularly women, may be held responsible for the harassment they experience. This is consistent with evidence that a substantial share of cybercrime complaints in Pakistan are filed by women and that family and societal attitudes can compound, rather than alleviate, the harm experienced.

Barriers to reporting identified in this study, including distrust of law-enforcement responsiveness and fear of secondary victimisation, mirror concerns raised in relation to the practical implementation of legislation such as the Prevention of Electronic Crimes Act (PECA) 2016, including low conviction rates and difficulties in gathering digital evidence. At the same time, the prominence of the coping and resilience theme (85%) suggests that, despite these structural barriers, victims actively draw on informal support networks, professional help, and adaptive reframing to manage the aftermath of victimisation.

Taken together, these findings suggest that interventions addressing cybercrime and online harassment should extend beyond legal and technical remedies to encompass accessible psychosocial support, family- and community-level awareness efforts to reduce victim-blaming, and simplified, victim-sensitive reporting pathways.

5.1 Implications for Practice and Policy

- Strengthening victim-support services, including accessible counselling and peer-support networks for individuals affected by cybercrime and online harassment.
- Simplifying reporting procedures and improving the sensitivity and training of personnel handling cybercrime complaints.
- Expanding digital literacy and online safety education, with attention to both preventive behaviour and reducing stigma associated with victimisation.
- Engaging families and communities in awareness efforts to shift responsibility away from victims and toward perpetrators and platform accountability.

5.2 Limitations

This study is subject to several limitations. The sample, while sufficient for thematic saturation, was drawn from a specific context and may not capture the full diversity of victims' experiences across different regions, age groups, or types of cybercrime. Reliance on retrospective self-report may be subject to recall bias, and the cross-sectional nature of the interviews does not allow conclusions about how experiences and coping evolve over longer periods of time.

6. Conclusion

This thematic analysis provides an in-depth account of the lived experiences of victims of cybercrime and online harassment, highlighting the emotional, social, financial, and behavioural dimensions of victimisation alongside the coping strategies victims employ and the barriers they face in seeking justice. The findings underscore that the harm caused by cybercrime and online harassment extends well beyond the immediate incident, and point to the need for coordinated psychosocial, legal, and educational responses that centre victims' experiences and reduce the stigma associated with reporting.

References

Alhaboby, Z. A., Evans, H., Barnes, J., & Short, E. (2023). The impact of cybervictimization on the self-management of chronic conditions: Lived experiences. Journal of Medical Internet Research, 25, e40227. https://doi.org/10.2196/40227

Ayub, S., & Malik, F. (2024). Construction and validation of Cyber Harassment Experience Scale (CHES). Pakistan Journal of Psychological Research, 39(4), 875–894. https://doi.org/10.33824/PJPR.2024.39.4.47

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Harasgama, K. S., & Jayamaha, S. (2023). Online harassment in Sri Lanka: A thematic analysis. Social Sciences, 12(3), Article 176. https://doi.org/10.3390/socsci12030176

Imam, S. K., & Naz, T. (2024). Cyberbullying: Legal challenges and societal impacts in the digital age. Pakistan Social Sciences Review, 8(4), 392–407. https://doi.org/10.35484/pssr.2024(8-IV)31

Mensah, R. O., Mensah, P., & Opoku, D. (2023). Experiences and perceptions of cybercrime victims in Ghana: The perspective of digital consumers of agricultural produce. Cogent Education, 10(2), Article 2285623. https://doi.org/10.1080/2331186X.2023.2285623

Pant, R., & Chaubey, U. (2024). Protecting minds in the digital age: A review-based study on psychological impact of cybercrime. International Journal of Indian Psychology, 12(3). https://doi.org/10.25215/1203.220

IEER
Institute for Excellence in Education & Research