ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 05 No. 01. Jan-March 2026.Page#.280-289
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems
https://doi.org/10.5281/zenodo.18288462

Understanding Cyber Victimization: Risk Patterns Among University Students in Pakistan

Husnain Hameed Awan
Lecturer, Department of Criminology
Faculty of Social Sciences, The University of Lahore-Pakistan
Muhammad Atif Nazir
Assistant Professor- M A Raoof College of LAW
Faculty of Law, The University of Lahore-Pakistan
Sobia Sifarish
Assistant Professor- M A Raoof College of LAW
Faculty of Law, The University of Lahore-Pakistan
Maleeha Amjad
Lecturer, Department of Criminology
Faculty of Social Sciences, The University of Lahore-Pakistan
Corresponding Author: maleeha.amjad@crim.uol.edu.pk

Abstract:

This study investigates the prevalence, patterns and consequences of cybercrime victimization among university students in Lahore, Pakistan, emphasizing the psychological impact and systemic barriers to reporting. Drawing on data from 150 students across four major universities, the study employs a mixed-methods approach grounded in Routine Activity Theory, Victim Facilitation Theory and Broken Windows Theory. Findings reveal that 45.3% of students have experienced cybercrime, yet 59.8% did not report it, primarily due to institutional mistrust and cultural stigma. Emotional consequences such as anxiety, anger and fear were common, while gender disparities highlighted the heightened vulnerability of female students. Instagram and WhatsApp emerged as the riskiest platforms due to algorithmic exposure and encryption loopholes. The study concludes with policy recommendations for universities, law enforcement and digital platforms, emphasizing workshops, anonymous reporting channels and identity verification protocols. The research underscores the need for comprehensive cyber safety frameworks in developing nations.

Keywords: *Cybercrime, Social Media, University Students, Lahore, Victimization, Routine Activity Theory, Psychological Impact, Institutional Barriers, Cybersecurity, Gender*

1. Introduction

The rise of social media has revolutionized communication, particularly among youth populations, fostering unprecedented levels of interaction, expression and connectivity. However, this digital revolution has also given rise to a corresponding increase in cybercrime, including harassment, impersonation, fraud and privacy violations. In Pakistan, where digital literacy remains inconsistent and cultural norms often stigmatize victims—particularly women—the consequences of cybercrime are both severe and underreported (Ahmad, Khan, & Zia, 2020; Amnesty International, 2023).

University students represent a particularly vulnerable demographic due to their high engagement with social media, exploratory online behavior and limited access to institutional support mechanisms (Bidgoli, Knijnenburg, & Grossklags, 2016; Kraus et al., 2023). According to a recent survey by the Higher Education Commission of Pakistan (2023), more than 70% of university students in urban centers like Lahore spend over three hours daily on platforms such as Instagram, WhatsApp and Facebook. This aligns with the global findings of Vishwanath (2015) and Smith and Lee (2024), who identified excessive social media use as a predictor of increased exposure to cyber threats.

Despite increasing awareness, effective prevention and reporting mechanisms remain inadequate. The enforcement of Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 has been criticized for bureaucratic delays and a lack of gender-sensitive protocols (Amnesty International, 2023; Punjab Cyber Crime Wing, 2024). Moreover, the existing cultural fabric further deters victims—especially women—from coming forward due to fears of stigma and familial repercussions (Ahmad et al., 2020). In this context, it becomes imperative to examine not only the types and frequencies of cybercrime affecting university students but also the psychological consequences and structural barriers to justice.

Theoretical frameworks such as Routine Activity Theory (Holt & Bossler, 2008; Leukfeldt & Yar, 2016), Victim Facilitation Theory (Yar, 2005) and Broken Windows Theory (Smith & Lee, 2024) provide robust lenses for understanding how user behavior, platform design and institutional neglect converge to exacerbate victimization. This study seeks to bridge the existing gap in empirical literature by focusing on Lahore's university students—a population situated at the intersection of digital exposure, institutional failure and cultural conservatism.

2. Literature Review

Cybercrime, especially when facilitated through social media platforms, has become a significant public safety issue worldwide. University students are among the most vulnerable groups due to their frequent use of social media, limited experience in digital risk assessment and often weak institutional support (Marcum, Higgins, & Ricketts, 2010; Mwiraria, Ngetich, & Mwaeke, 2022). Bidgoli et al. (2016) highlight that undergraduate students are frequently targeted for online scams and harassment, often due to their oversharing behavior and reliance on unsecured networks. In the Pakistani context, the problem is compounded by societal norms that discourage open discussions around online victimization, especially among women (Ahmad et al., 2020).

Routine Activity Theory postulates that crime occurs when a motivated offender encounters a suitable target in the absence of capable guardianship (Holt & Bossler, 2008). This model is particularly relevant in digital environments where constant connectivity, lax privacy settings and a lack of cybersecurity education create ideal conditions for victimization (Leukfeldt & Yar, 2016). Victim Facilitation Theory further emphasizes that certain user behaviors—such as oversharing personal information or clicking unverified links—may inadvertently increase the risk of becoming a victim (Yar, 2005; Wang et al., 2022). According to Abbas et al. (2019), Pakistani students often use social media without adequate awareness of digital threats, making them easy targets for various cyber offenses.

Broken Windows Theory suggests that the failure to address minor offenses signals a broader tolerance for deviant behavior, encouraging escalation (Smith & Lee, 2024). This is particularly applicable in Pakistan where reports of fake accounts, identity theft and online harassment often go unaddressed by both platforms and law enforcement agencies (Dawn, 2023; UNODC, 2023). Powell and Henry (2019) argue that unchecked technology-facilitated violence contributes to a normalization of abuse, especially when institutions fail to act. Uche

and Uche (2023) also note that students' perceptions of ineffective institutional responses lead to resignation and non-reporting.

In terms of psychological impact, cybercrime can lead to severe emotional distress, including anxiety, depression and social withdrawal (Metzger & Suh, 2017; Zheng et al., 2020). Hadlington and Chivers (2018) found that personality traits, such as impulsivity and openness, coupled with poor cybersecurity awareness, further heighten the risk of victimization. In Pakistan, these effects are often intensified by cultural stigma and victim-blaming, leading to long-term trauma and academic disengagement (Ahmad et al., 2020).

Despite the availability of legal frameworks such as PECA 2016, implementation remains weak. Amnesty International (2023) and the Punjab Cyber Crime Wing (2024) report systemic delays and a lack of specialized training among law enforcement personnel. Chagas and Da-Costa (2023) emphasize that the opaque nature of platform algorithms and encryption, particularly on WhatsApp, further complicates detection and accountability. Lee, Kang and Kim (2023) underline the necessity of understanding offender psychology to develop more effective deterrents.

Overall, while existing literature offers valuable theoretical and empirical insights, there remains a critical gap in localized, context-sensitive studies that explore the confluence of user behavior, platform risks and institutional failure in developing countries like Pakistan. This study aims to fill that gap by focusing on Lahore's university students.

3. Methodology

This study adopted a quantitative-dominant mixed-methods research design to investigate the patterns of cybercrime victimization among university students in Lahore, alongside its emotional and institutional consequences. Data was collected using an online survey distributed to undergraduate students aged 18–25 from four major universities. The questionnaire consisted of structured closed-ended questions and a few open-ended prompts that allowed participants to elaborate on their experiences.

The survey focused on three domains: social media usage, experiences with cybercrime and awareness or use of cybersecurity practices. The questionnaire was disseminated via student forums, university groups and social media channels, ensuring anonymity to minimize social desirability bias. A total of 150 valid responses were collected, providing a statistically adequate sample for exploratory analysis.

The instrument was reviewed and validated by two academic experts in criminology and pilot-tested with a group of 10 students. The demographic composition of the sample closely mirrored that of Lahore's general university student population in terms of age, gender and academic discipline. Quantitative data were analyzed using SPSS and Excel for frequencies, percentages and visual representations. Thematic analysis was conducted on the open-ended responses to enrich the findings with qualitative insights.

4. Results and Discussion

Survey data from 150 university students in Lahore was analyzed to examine the prevalence, nature and impact of cybercrime victimization on social media. Drawing upon theoretical frameworks such as Routine Activity Theory, Victim Facilitation Theory and Broken Windows Theory, the results are interpreted through both statistical insights and cultural contexts. The discussion integrates visual representations and literature-based comparisons to explore key themes, including gendered vulnerabilities, emotional consequences, underreporting and institutional gaps in prevention and response.

4.1 Prevalence of Cybercrime and Platform-Specific Risks

Findings reveal that 45.3% of students had experienced some form of cybercrime, a rate notably higher than global averages (Zalaquett & Chatters, 2014). Instagram (36.4%), WhatsApp (20.3%) and Facebook (30.5%) were the platforms most implicated. Common offenses included impersonation (37.8%), scams (26.1%), harassment (16.8%) and hacking (9.2%). WhatsApp's encryption and Instagram's algorithmic amplification of unknown contacts facilitated these crimes.

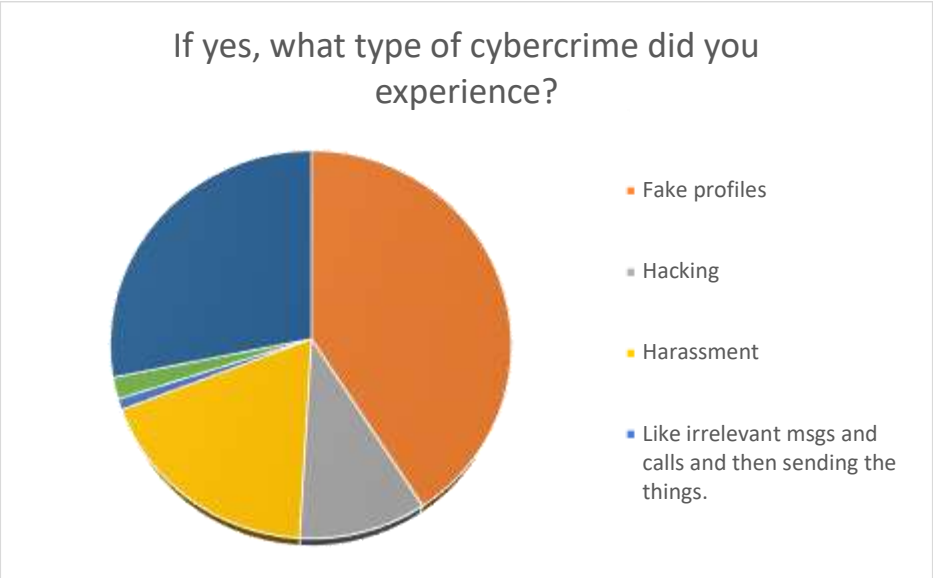

Figure 1. What type of cybercrime did you experience?

4.2 Social Media Engagement and Risk Exposure

Respondents showed intense platform engagement: 60.3% spent more than 3 hours daily online, mostly on Instagram (58.7%) and WhatsApp (28%).

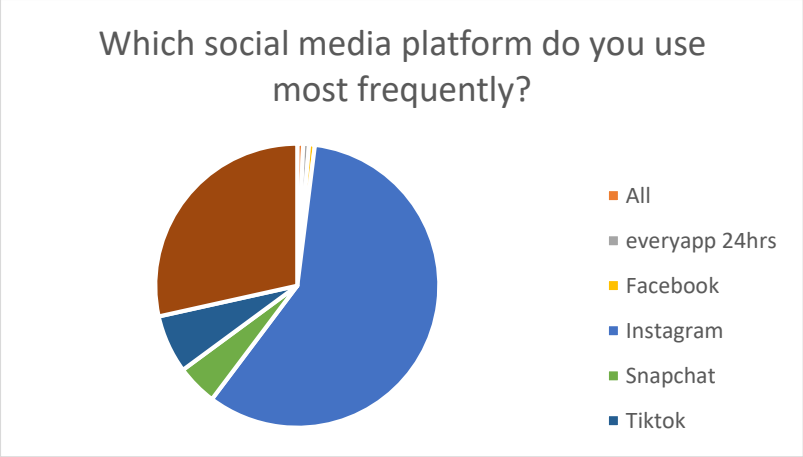

Figure 2. Frequently used social media platform

Personal data sharing was common, with 43.3% regularly or occasionally sharing private information. These behaviors align with Routine Activity Theory, which posits that increased exposure without adequate guardianship elevates victimization risks (Leukfeldt & Yar, 2016).

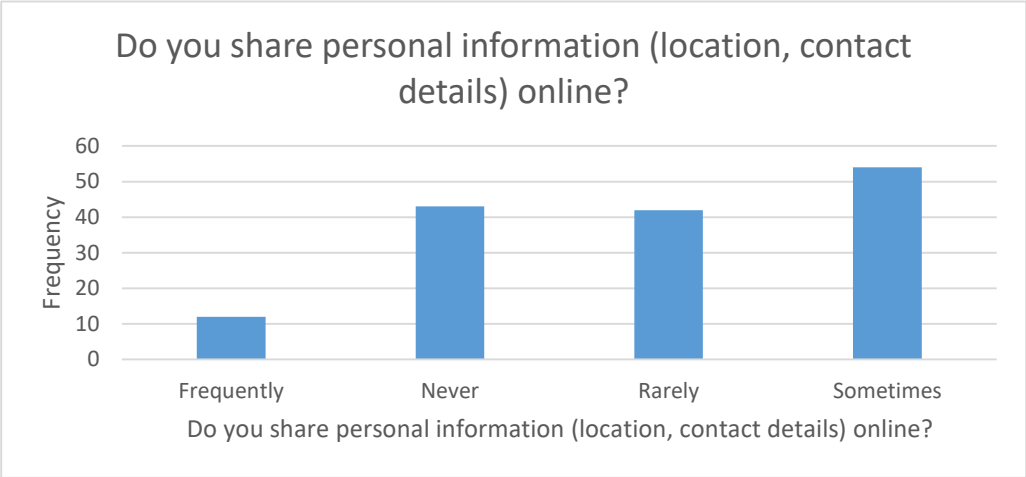

Figure 3: Personal data sharing

4.3 Demographic Characteristics of Victims

The demographic analysis of victims highlighted important trends in vulnerability. Female students were disproportionately targeted, especially for harassment, with a 23.7% victimization rate compared to 9.5% among males.

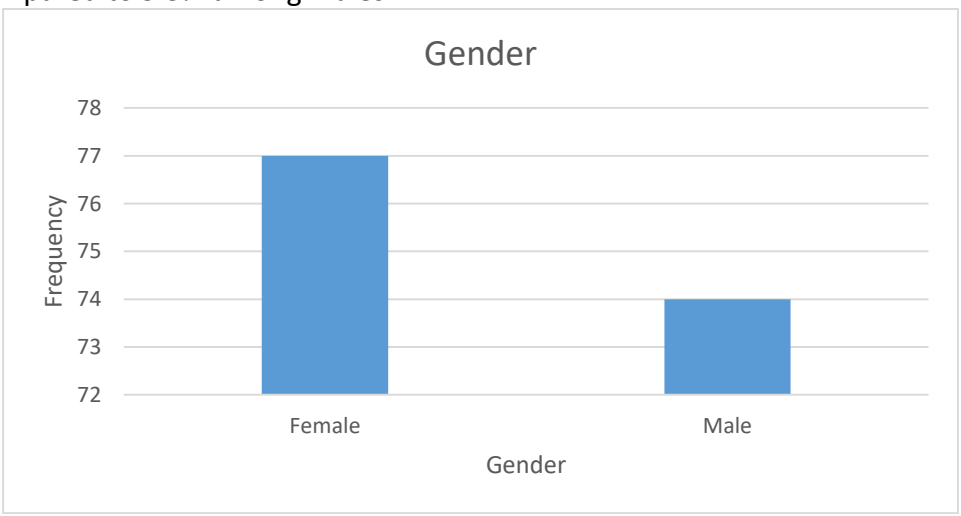

Figure 4. Gender of Respondents

The majority of victims were aged 21–25 (61.3%) and enrolled in senior semesters (56.3%). These characteristics suggest that more digitally engaged and socially active students are at greater risk.

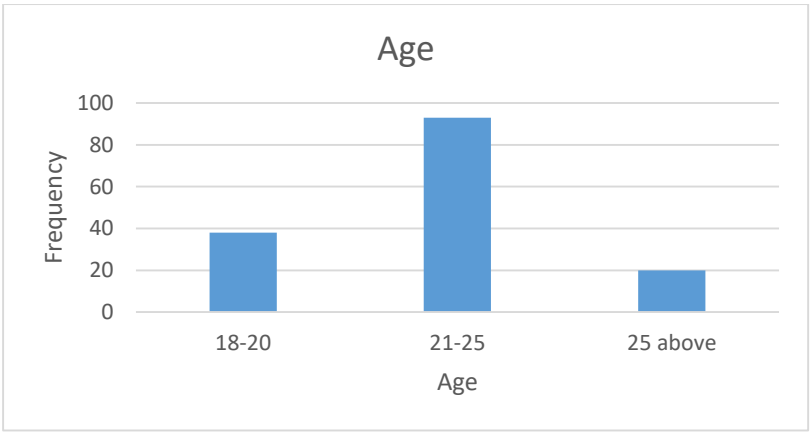

Figure 5. Age Distribution of Respondents

4.4 Gendered Norms and Cultural Stigma in Underreporting

Gendered victimization patterns were stark. Female students reported a 23.7% harassment rate compared to 9.5% among males. Underlying cultural taboos, such as "family honor," heavily influenced underreporting. Many female respondents feared blame or social consequences (Ahmad et al., 2020). This confirms the first research question on how sociocultural norms shape victim silence.

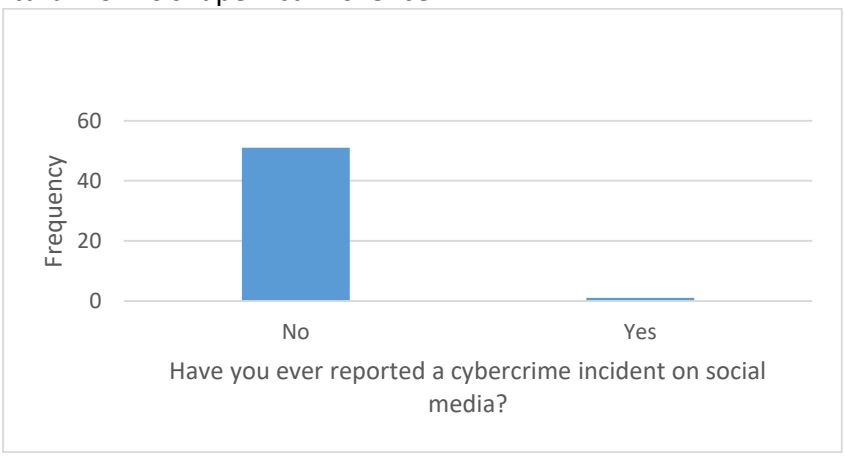

Figure 6. Have you ever reported a cybercrime incident on social media?

4.5 Emotional and Psychological Impact

Victims experienced anxiety (27.4%), anger (24.8%) and fear (11.1%). Some faced long-term academic disruption, including reduced class participation and social media withdrawal. 17% decreased educational use of social media post-victimization, confirming the broader academic costs (Zheng et al., 2020; Smith & Lee, 2024).

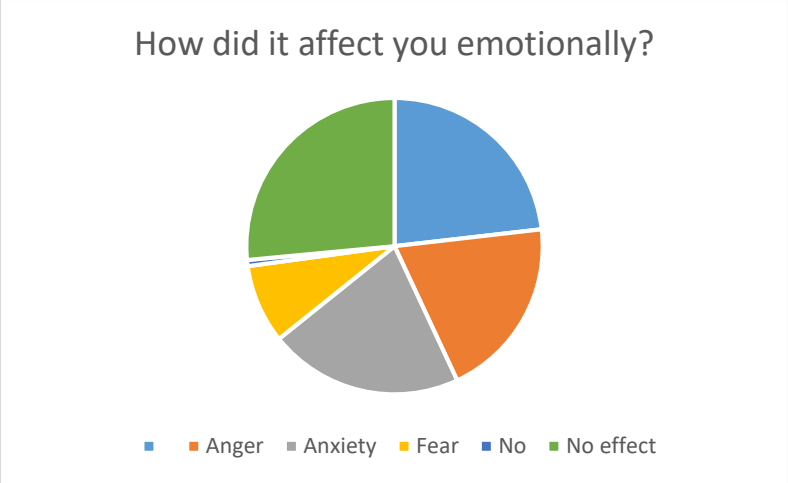

Figure 7. Emotional and psychological impacts

4.6 Underreporting and Institutional Gaps

Despite the emotional toll, 59.8% did not report incidents. Primary reasons included mistrust in institutional capacity (42.5%) and fear of social backlash (35%). Respondents noted FIA's delayed responses, echoing criticism of PECA 2016's flawed enforcement (Amnesty International, 2023). Female students cited cultural barriers, such as "family shame," reinforcing Ahmad et al.'s (2020) findings.

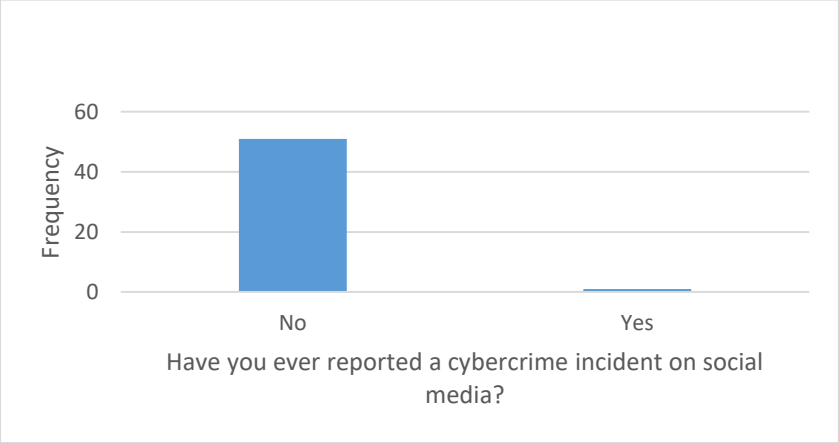

Figure 8. Reported cybercrime incident

4.7 Awareness, Platform Features and Preventive Behaviors

Only 38% used protective features like two-factor authentication and just 16.1% learned about cyber safety via university channels. Awareness largely came through media (37.7%) or personal experience (34%) (HEC, 2023; Kraus et al., 2023). Nonetheless, 65.6% of students endorsed stricter platform verification to reduce impersonation and scams, supporting the need for platform reform.

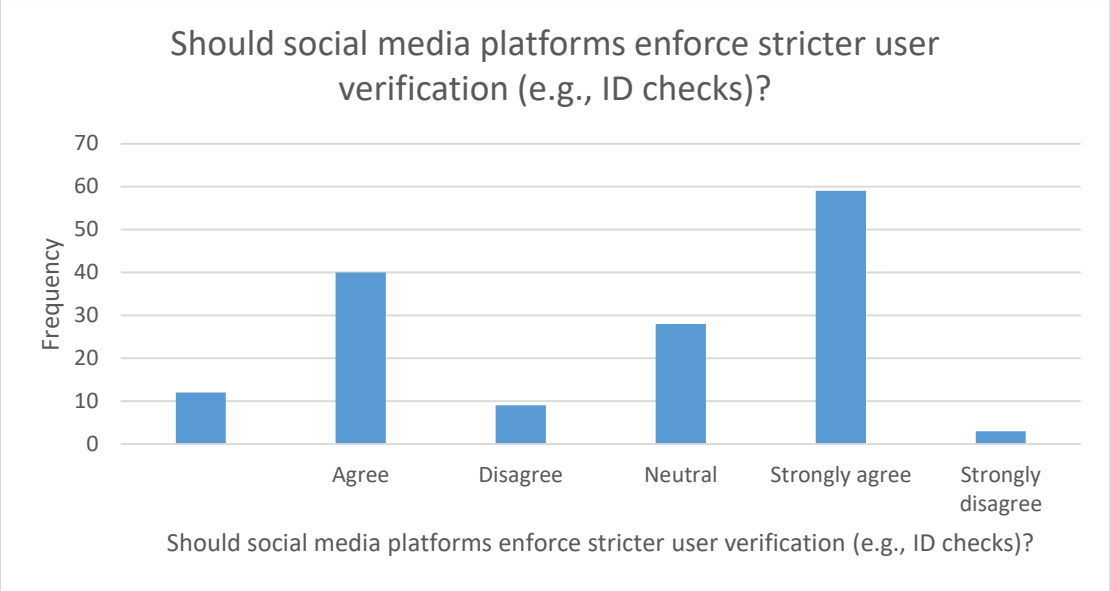

Figure 9. Should social media platforms enforce stricter user verification?

4.8 Theoretical Reflections, Legal and Institutional Effectiveness

Routine Activity Theory explains how excessive time online and weak digital safeguards increase risks (Leukfeldt & Yar, 2016). Victim Facilitation Theory reveals how oversharing, driven by social media reward systems, makes users easier targets (Abbas et al., 2019). Broken Windows Theory helps explain the escalation of minor, unchecked offenses into more serious crimes, facilitated by institutional inaction (Yar, 2005).

These findings answer the third research question by revealing that institutional responses such as PECA enforcement and university workshops are currently insufficient to reduce cybercrime or encourage reporting. For these responses to be effective, culturally aware outreach, faster response mechanisms and platform collaboration are urgently needed.

These integrated results and theoretical reflections underscore the urgent need for reforms tailored to cultural, institutional and digital realities faced by students in Pakistan.

5. Conclusion

This study highlights the alarming prevalence and impact of cybercrime among university students in Lahore, revealing a critical intersection between behavioral risks, technological vulnerabilities and institutional inefficiencies. With nearly half of the respondents reporting victimization and a majority choosing not to report, the findings underscore the urgent need for policy intervention.

Theoretical insights from Routine Activity Theory, Victim Facilitation Theory and Broken Windows Theory help explain the systemic nature of this issue. Students' routine online activities, poor digital hygiene and the unresponsiveness of institutions collectively create an environment ripe for cybercrime. Gendered cultural norms further complicate reporting and recovery, especially for female students.

Policy recommendations include integrating cybersecurity education into university curricula, establishing anonymous reporting mechanisms, enhancing the implementation of PECA 2016 and fostering collaboration between social media platforms and academic institutions. Future research should employ longitudinal designs and incorporate offender perspectives to develop more comprehensive prevention strategies. Ultimately, addressing cybercrime requires a multidimensional approach that accounts for cultural, institutional and technological factors unique to the Global South.

References

Ahmad, S., Khan, R., & Zia, A. (2020). Cyber harassment and cultural stigma: A study of Pakistani women. *Asian Journal of Social Science*, 48(3), 301–318.

Amnesty International. (2023). *PECA 2016: Failures in implementation*. Retrieved from https://www.amnesty.org

Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016). When cybercrimes strike undergraduates. In *2016 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–10). IEEE. https://doi.org/10.1109/ECRIME.2016.7487948

Chagas, V., & Da-Costa, G. (2023). WhatsApp and transparency: An analysis on the effects of digital platforms' opacity in political communication research agendas in Brazil. https://doi.org/10.3145/epi.2023.mar.23

Dawn. (2023, May 12). *PU students blackmailed through fake profiles*. Retrieved from https://www.dawn.com

Hadlington, L., & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice*, 12(1), 1–15. https://doi.org/10.1093/police/pay027

Higher Education Commission (HEC) Pakistan. (2023). *Digital Literacy Survey of Pakistani Universities*. Islamabad: HEC.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1–25. https://doi.org/10.1080/01639620701876577

Kraus, L., Švábenský, V., Horák, M., Matyáš, V., Vykopal, J., & Čeleda, P. (2023). Want to raise cybersecurity awareness? Start with future professionals. In *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1*. https://doi.org/10.1145/3587102.3588862

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, 72, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 31(5), 381–410. https://doi.org/10.1080/01639620903004903

Metzger, M. J., & Suh, J. Y. (2017). Comparative optimism about privacy risks on Facebook. *Journal of Communication*, 67(2), 203–232. https://doi.org/10.1111/jcom.12290

Mwiraria, D., Ngetich, K., & Mwaeke, P. (2022). Factors associated with cybercrime awareness among university students in Egerton University, Njoro Campus, Nakuru County, Kenya. *European Journal of Humanities and Social Sciences*, 2(3). https://doi.org/10.24018/ejsocial.2022.2.3.256

Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, 34(17), 3637–3665.

Punjab Cyber Crime Wing (PCCW). (2024). *Annual Cybercrime Report*. Lahore: Punjab Police.

Smith, J., & Lee, K. (2024). The hidden costs of cyber victimization: Academic and mental health outcomes among university students. *Journal of Interpersonal Violence*, 39(1–2), 112–134.

Uche, I., & Uche, O. (2023). Perceptions of undergraduates towards cybercrimes at the University of Nigeria, Nsukka. *International Journal of Social Sciences and Humanities Invention*, 10(5). https://doi.org/10.18535/ijsshi/v10i05.01

United Nations Office on Drugs and Crime (UNODC). (2023). *Cybercrime in developing nations*. Vienna: UNODC.

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1), 83–98. https://doi.org/10.1111/jcc4.12100

Wang, N., Zhao, Y., Zhou, R., & Li, Y. (2022). Factors influencing users' online information disclosure intention and the moderating effect of cultural background and platform type. *Aslib Journal of Information Management*, 75(6), 1178–1208. https://doi.org/10.1108/AJIM-04-2022-0218

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407–427.

Zalaquett, C. P., & Chatters, S. J. (2014). Cyberbullying in college: Frequency, characteristics and practical implications. *SAGE Open*, 4(1), 1–8.

Zheng, Y., et al. (2020). Cyberbullying and academic outcomes. *Journal of Cybersecurity*, 6(1), 45–60.