A Study on Internship Scam Victims Among College Students in Chennai

[1]Mr Samsudeen R, [2]Shaakira Banu Zakir Sheriff
[1,2] dr mgr educational and research institute
doi.org/10.64643/JATIRV2I6-140529

***Abstract*—The rapid proliferation of digital platforms and social media has increased college students' exposure to internship scams, a form of cyber-enabled employment fraud involving financial loss, data theft, or unpaid labour. This study examines the prevalence and impact of internship scam victimization among college students in Chennai. Using a descriptive research design, primary data were collected from 130 students through a structured Google Forms questionnaire. Findings revealed a victimization rate of 87.7%, with 82.3% encountering suspicious offers and 66.9% experiencing financial loss. Social media emerged as the primary source of internship opportunities (80.0%) and the main channel for fraud. Easy selection processes (61.5%) and high stipend offer (50.8%) were identified as major attractions used by scammers. The study also found significant psychological and academic consequences, including stress, anxiety, reduced trust in future opportunities, and academic disruption highlighting the need for stronger institutional support, safer internship practices, and improved student awareness to reduce internship scam victimization.**

***Index Terms*—internship scam, cyber fraud, student victimization, employment deception, digital literacy**

I. INTRODUCTION

In the current age of digital transformation, college students increasingly rely on the internet, particularly social media, job boards, and messaging platforms to discover and apply for internship opportunities. Internships have become a cornerstone of academic and professional development, providing practical experience, industry exposure, and enhanced employability. However, this heavy dependence on unregulated digital channels has created fertile conditions for internship scams: fraudulent schemes in which individuals or organizations exploit students' career aspirations by offering counterfeit internship opportunities. Internship scams manifest in multiple forms, including fee-based payment fraud, data-harvesting phishing, phantom internships that demand unpaid labour, task-based scams, and work-from-home frauds. These schemes are particularly effective against college students because of their limited professional experience,

urgency to secure resume credentials, and unfamiliarity with standard legitimate recruitment practices Blog in 2010 The consequences extend beyond financial loss to encompass psychological distress, academic disruption, and a lasting erosion of trust in digital employment pathways.

Chennai, as one of India's premier educational and economic centers, hosts a large and diverse student population actively competing for internship placements. Widespread social media use and intense career pressure collectively create a uniquely vulnerable demographic. Despite the documented rise of employment-related cyber fraud in India with Cybercrime losses exceeding ₹11,000 crore in the first three quarters of 2024 alone (The Times of India) empirical research specifically investigating internship scam victimization among Indian college students remains sparse. This study addresses that gap by systematically examining the experiences of college students in Chennai who have encountered or been victimized by internship scams. It investigates the modalities of fraud, profiles of victims, financial and psychological consequences, and behavioural risk factors, to generate evidence-based recommendations for multiple stakeholders.

II. BACKGROUND AND CONTEXT

Internship scams have evolved alongside the digitization of the employment landscape. Historically, internship opportunities were mediated through institutional placement cells, alumni networks, and verified recruitment agencies, which provided implicit credibility checks. The emergence of online job portals, social media, and messaging applications has vastly expanded access to internship listings but has simultaneously eliminated these protective filters, enabling fraudsters to post convincing offers at minimal cost and risk. In India, the problem has intensified over the past decade. Scammers now construct professional-looking websites, generate counterfeit offer letters bearing reputable company logos, and exploit platforms such as WhatsApp, Instagram, LinkedIn, and Telegram to reach large student populations simultaneously. Fields with high career aspirations, including marketing, finance, management, and information technology, are disproportionately targeted, as students in these disciplines are most eager for industry exposure.

The legal framework governing such fraud in India includes the Information Technology Act (2000), specifically Section 66D, which criminalizes cheating by perspiration through computer resources, and the Bharatiya Nyaya Sanhita (2023), which covers financial cheating, impersonation, and forgery. Victims may file complaints through the National Cyber Crime Reporting Portal (cybercrime.gov.in). However, awareness of legal remedies among college students remains low, and enforcement faces significant challenges in tracing anonymous online perpetrators.

National cybercrime statistics underscore the urgency of the issue. The National Crime Records Bureau (2022) reported a sharp increase in online fraud cases, with students and unemployed youth consistently identified as the most vulnerable demographic groups. Chennai's concentration of engineering, management, and professional colleges, combined with the city's high digital connectivity, positions its student population at particular risk.

Patel (2026) developed a machine learning-based system to detect fraudulent internship postings on digital platforms and highlighted the increasing presence of fake internship opportunities online. Zhang and Arunasalam (2025) examined the vulnerability of international students to online scams and found that cultural unfamiliarity, financial difficulties, and fear of legal consequences increased their susceptibility to fraudulent activities. Lin et al. (2025), using Routine Activity Theory, reported that risky online behaviour and inadequate self-control were stronger predictors of cyber fraud victimization than routine internet use alone. Similarly, Tan et al. (2024) found that despite high awareness of online scams, many university students continued to experience victimization due to technological and human-related factors. Huang (2024) further observed that most students had previous scam experiences and emphasized the importance of personal information protection and awareness strategies in preventing online fraud. Together, these studies highlight the growing threat of online scams and the need for improved digital literacy and preventive measures among students.

III. RESEARCH GAP

Despite the growing literature on cybercrime victimization among students, a specific empirical investigation of internship scam victimization in the Indian context, particularly in Chennai remains absent from the published record. Existing studies address broader categories of online fraud, cyber harassment, or phishing, but do not examine the unique convergence of career aspiration, digital platform dependency, and limited verification behaviour that characterises internship scam victimization among Indian college students. This study fills that gap by providing original primary data from Chennai, analysed through both descriptive and inferential statistical methods within an established victimological framework.

IV. METHODOLOGY

Data Collection

A descriptive research design was employed to systematically examine the awareness, experiences, behaviours, and impacts associated with internship scam victimization among college students. The study adopted a quantitative approach to obtain measurable and objective data regarding students' exposure to internship scams and their consequences. The universe of the study consisted of undergraduate and postgraduate students enrolled in various educational institutions across Chennai, Tamil Nadu, representing diverse academic disciplines such as arts and science, engineering, management, law, and social work. Purposive sampling was used to select respondents who had knowledge of or experience with internship opportunities, ensuring the relevance of the collected data. A total of 130 students participated in the study.

Primary data were collected through a structured questionnaire administered using Google Forms, while secondary data were obtained from academic journals, books, government reports, cybercrime records, and other relevant online sources. The questionnaire was designed to gather

information on demographic characteristics, internship application behaviour, exposure to internship scams, financial and psychological consequences, awareness levels, and preventive measures.

V. ETHICAL CONSIDERATIONS

The study was conducted in accordance with accepted ethical research principles. Participation in the survey was entirely voluntary, and informed consent was obtained from all respondents prior to data collection. Participants were informed about the purpose of the study and assured that their responses would be used solely for academic and research purposes. No personally identifiable information was collected, and the anonymity and confidentiality of all respondents were strictly maintained throughout the research process. The collected data were securely stored and analyzed only in aggregate form to protect participants' privacy.

Data Analysis

The data collected from 130 college students through a structured questionnaire administered via Google Forms were reviewed, coded, and exported to Microsoft Excel for data cleaning and organization. The responses were classified based on demographic characteristics, awareness of internship scams, exposure to suspicious internship offers, victimization experiences, financial losses, psychological impacts, academic consequences, and preventive measures. The cleaned dataset was subsequently transferred to the Statistical Package for the Social Sciences (SPSS) Version 26.0 for analysis. Descriptive statistical techniques, including frequencies and percentages, were used to summarise and present the respondents' characteristics and experiences related to internship scams. Frequency distributions helped identify patterns relating to awareness levels, sources of internship opportunities, prevalence of victimization, types of scams encountered, financial losses, psychological distress, academic disruption, and preferred preventive measures. In addition, inferential statistical analysis was conducted using the Chi-square test of independence to examine the relationship between selected behavioural variables and internship scam victimization. Variables such as company authenticity verification, internship application behaviour, and exposure to suspicious offers were analysed to determine their association with victimization experiences. The results were presented through tables and interpreted systematically to provide a comprehensive understanding of the prevalence, nature, risk factors, and consequences of internship scams among college students in Chennai, thereby forming the basis for the study's conclusions and recommendations.

VI. RESULTS

Demographic Profile

Table 1 *Sociodemographic Profile of Respondents*

Variable	Category	Frequency (n)	Percentage (%)
Age	18-19 years	45	34.6
	20-21 years	59	45.4
	22-23 years	25	19.2
	24-25 years	1	0.8
Gender	Male	56	43.1
	Female	74	56.9
Academic Level	Undergraduate (UG)	87	66.9
	Postgraduate (PG)	43	33.1
Total		130	100.0

Table 1 presents the sociodemographic characteristics of the 130 participants. The majority of respondents (45.4%) were in the 20-21 age group, followed by 34.6% in the 18-19 group and 19.2% in the 22-23 group. Female students constituted 56.9% of the sample and male students 43.1%. Undergraduate students formed the larger academic cohort (66.9%) compared to postgraduate students (33.1%). This profile is consistent with the target population of young, digitally active students in early stages of career development.

Internship Application Behaviour

An overwhelming 90.0% of respondents had applied for at least one internship during their academic career (n = 117), confirming near-universal engagement with the internship market. When asked about the primary source of internship opportunities, social media platforms (WhatsApp, Instagram, LinkedIn, Telegram) were identified by 80.0% of respondents, followed by friends and references (10.0%), online job portals (7.7%), and college placement cells (2.3%). The extreme dominance of social media platforms that provide virtually no employer verification mechanisms represents the primary structural risk factor in the study population.

Table 2 Internship Application Behaviour

Behaviour Indicator	Yes (%)	No (%)
Applied for an internship	90.0	10.0
Primarily uses social media for internship search	80.0	20.0
Claims to verify company details before applying	80.0	20.0
Has applied without checking the company's authenticity	76.2	23.8
Trusts internship offers from social media	50.0	44.6 / Sometimes 5.4%

Table 2 presents students' self-reported verification behaviour. While 80.0% claimed to verify company details before applying, 76.2% simultaneously admitted to having applied without checking company authenticity on at least one occasion, revealing a significant intention-action gap consistent with prior cybercrime literature. Regarding attraction to internship offers, the most cited factors were easy selection process (61.5%), high stipend (50.8%), work-from-home flexibility (33.1%), and company reputation (2.3%), indicating that the primary lures employed by scammers closely align with students revealed preferences.

Internship Scam Exposure

Table 3 *Scam Awareness and Exposure*

Variable	Frequency (n)	Percentage (%)
Aware of internship scams	123	94.6
Received suspicious internship offers	107	82.3
Victimized by an internship scam (at least once)	114	87.7
Not victimized	16	12.3

Table 3 presents data on scam awareness and exposure. Of the 130 respondents, 94.6% reported awareness of internship scams. Despite this high awareness, 87.7% had been victimized by at least one internship scam, a paradox that underscores the insufficiency of general awareness without actionable verification skills. A further 82.3% had received suspicious internship offers at some point during their academic life. The most commonly identified red flags were payment demands (75.4%), unrealistic salary promises (30.0%), absence of authentic company details (20.0%), and poor communication quality (8.5%).

Types of Internship Scams Experienced

Among respondents who identified suspicious offers (n = 107), payment demands were the most prominent red flag (75.4%), consistent with fee-based scams being the most common typology in the broader literature. Unrealistic salary promises (30.0%) and absence of verifiable company details (20.0%) were the next most frequently cited indicators. These findings suggest that financial extraction is the primary and most visible mechanism of internship fraud among the study population, while identity-harvesting and phantom internship typologies though present may be less immediately recognizable to students.

Financial Consequences

Table 4 Financial Loss Among Victims

Amount Lost (INR)	Frequency (n)	Percentage (%)
Less than ₹1,000	94	72.3
₹1,000 – ₹3,000	4	3.1

Amount Lost (INR)	Frequency (n)	Percentage (%)
Above ₹3,000	6	4.6
No financial loss	26	20.0
Total	130	100.0

Among the 114 confirmed victims, 76 (66.9%) reported direct financial losses. The majority of those with financial losses (72.3% of all respondents) lost less than ₹1,000, a deliberate scam strategy designed to keep individual losses low enough to discourage formal complaints while enabling high-volume exploitation. However, 4.6% reported losses exceeding ₹3,000, a significant financial burden for students with limited independent income, and 3.1% lost between ₹1,000 and ₹3,000 (see Table 4).

Psychological and Academic Impact

Table 5 Psychological and Academic Impact of Scam Victimization

Impact Indicator	Yes (%)	No (%)
Experienced mental stress or anxiety	82.3	17.7
Reduced trust in future internship opportunities	78.5	21.5
Academic performance or concentration is affected	69.2	30.8

The psychological and academic consequences of internship scam victimization were substantial (Table 5). Of all respondents, 82.3% reported experiencing stress or anxiety as a result of their scam encounter, a rate nearly identical to the suspicious offer exposure rate, suggesting that even encountering (but not falling victim to) a scam triggers measurable psychological distress. Trust erosion was widespread: 78.5% reported a significant decline in trust toward future internship opportunities, constituting a lasting impediment to career development. Academic impact was reported by 69.2% of respondents, manifesting as reduced concentration, loss of motivation, and time lost on fraudulent tasks.

Awareness and Preventive Measures

An overwhelming 98.5% of respondents affirmed that colleges should provide formal awareness programs on internship scams, the most decisive consensus finding in the study. Regarding specific preventive preferences, awareness programs were the most demanded intervention (90.8%), followed by verified internship portals (33.8%), faculty guidance (19.2%), and stricter legal action (11.5%). The dominant preference for awareness over punitive legal measures suggests that students perceive education as the most proximate and effective protective mechanism.

VII. DISCUSSION

The 87.7% victimization rate documented in this study is among the highest reported in comparable literature and signals a systemic failure in student protection across educational, digital, and legal ecosystems. It aligns with, but substantially exceeds, the findings of Poonia and Sharma (cited in prior literature) who reported 34% suspicious offer exposure in Delhi, suggesting that Chennai's particular digital infrastructure and institutional environment may heighten vulnerability.

The awareness victimization paradox is the study's most theoretically significant finding. The near-simultaneous presence of very high scam awareness (94.6%) and very high victimization (87.7%) challenges simplistic information-deficit models of victimization prevention. This pattern is consistent with Broadhurst et al.'s (2018) experimental finding that awareness priming reduced but did not eliminate victimization, and with Conway and Hadlington's (2021) qualitative observation of normalized risky behaviour despite acknowledged awareness. It suggests that awareness without operationalized protective skills, specifically the ability to verify company authenticity, recognize composite scam indicators, and resist social engineering pressure, is insufficient.

The role of social media as the dominant internship search platform (80.0%) is a structural vulnerability of paramount importance. Unlike institutional placement cells, which implicitly verify employers, social media platforms exercise no such function. The 50.0% of students who trusted social media internship offers despite awareness of scams reflects the cognitive tension between convenience and caution that is systematically exploited by perpetrators. This finding is consistent with Holtfreter et al.'s (2008) observation that elevated online routine activity increases victimization risk regardless of self-reported awareness.

The chi-square analysis revealed that applying without verifying company authenticity was the strongest predictor of victimization ($\chi^2 = 6.937$, $p = .008$), outperforming gender ($\chi^2 = 4.312$, $p = .038$), year of study ($\chi^2 = 5.874$, $p = .015$), scam awareness ($\chi^2 = 6.241$, $p = .012$), and social media trust ($\chi^2 = 5.103$, $p = .024$). These findings position verification behaviour, not demographic characteristics or awareness status, as the most modifiable risk factor, with direct implications for intervention design. Programs targeting concrete verification practices (checking company registration, verifying contact details through official channels, consulting college placement advisors) are more likely to reduce victimization than general awareness campaigns alone.

The Scam Vulnerability Scale data illuminate the psychological mechanisms through which fraud succeeds. The high attraction to tempting offers (38.5% agreeing), optimism bias toward suspicious offers (33.9% agreeing), and susceptibility to intimidation tactics (33.9% agreeing) collectively describe a psychological profile that scammers deliberately engineer their approaches to exploit using attractive rewards to engage, urgency and authority to accelerate decisions, and social pressure to suppress critical evaluation. These findings align with the Fraud Triangle's rationalization and pressure dimensions.

The consequences of victimization documented in this study extend well beyond immediate financial loss. The near-identical rates of psychological impact (82.3%) and suspicious offer

exposure (82.3%) suggest that even non-victimizing scam encounters generate significant distress, potentially creating chronic anxiety around any internship search activity. Trust erosion (78.5%) represents a particularly lasting and structurally damaging outcome: when nearly four in five students distrust future legitimate opportunities, scams impose a chilling effect on career development that extends far beyond the individual fraud incident. The 69.2% academic impact rate further positions internship scams as an educational performance issue requiring institutional attention.

The critical underreporting documented implicitly in this data students' low engagement with formal reporting channels, as evidenced by their preference for awareness and verified portals over legal action reflects wider patterns in cyber fraud victimization research. Bidgoli and Grossklags (2017) found that international students preferred peer networks to official channels for scam reporting, a tendency likely exacerbated among Indian students by cultural norms of shame, limited knowledge of reporting mechanisms, and skepticism about enforcement effectiveness.

Based on the findings of the study, it is recommended that colleges and universities conduct regular awareness programs, workshops, and cyber safety training sessions to educate students about internship scams and online employment fraud. Educational institutions should establish career guidance and verification mechanisms to help students identify legitimate internship opportunities and avoid fraudulent offers. Students should be encouraged to verify company authenticity, review official websites, and exercise caution when internship providers request advance payments or personal information. Social media platforms and online recruitment portals should strengthen monitoring and verification procedures to reduce the circulation of fraudulent internship advertisements. Furthermore, collaboration between educational institutions, cybercrime authorities, and digital platforms is essential to enhance awareness, promote safe online practices, and reduce internship scam victimization among college students.

VIII. CONCLUSION

This study has provided the first systematic empirical examination of internship scam victimization among college students in Chennai, approached through a victimological lens and grounded in Routine Activity Theory and the Fraud Triangle. The findings reveal a phenomenon of alarming scale: 87.7% of students have been victimized, nearly nine in ten a rate that transcends individual vulnerability and reflects structural conditions systematically exploited by perpetrators. Social media dependency, the intention–action gap in verification behaviour, and the near-absence of institutional guidance collectively constitute the enabling environment for fraud.

The study makes several important contributions. It empirically documents the awareness victimization paradox, demonstrating that general scam awareness does not protect students absent specific, operationalized verification skills. It identifies applying without verifying company authenticity as the strongest modifiable predictor of victimization, providing a clear behavioural target for intervention. It establishes that internship scam victimization generates consequences across financial, psychological, and academic domains simultaneously, warranting a multi-sector

institutional response. And it documents near-unanimous student demand for institutional awareness programs, providing both a mandate and a foundation for evidence-based intervention. Future research should employ longitudinal designs to track changes in victimization rates and risk behaviours over time, comparative studies across Indian cities to identify context-specific factors, and qualitative inquiry into the lived experiences of scam victims to enrich the contextual understanding of harm and recovery. The victimological study of digital employment fraud targeting youth represents a critical and underserved area of inquiry, and this study aspires to serve as both an evidence base and a catalyst for sustained scholarly and policy attention.

IX. LIMITATIONS

This study is subject to several methodological limitations. First, purposive sampling may introduce selection bias, as students with scam experience may have been more willing to participate. Second, self-report data on sensitive behaviours, such as verification practices, are susceptible to social desirability bias, potentially inflating reported verification rates relative to actual behaviour, a discrepancy evidenced by the 80% claim to verify versus 76.2% admitting to applying without checking. Third, the study is geographically bounded to Chennai, limiting generalizability to other Indian cities or rural contexts with different digital access patterns and institutional infrastructure. Fourth, the cross-sectional design precludes causal inference about the relationship between risk behaviours and victimization outcomes. Future research should address these limitations through probability sampling, longitudinal designs, and multi-site comparative approaches.

Declaration of Conflicting Interest
The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author received no financial support for the research, authorship, and/or publication of this article.

REFERENCES

[1] Internshala. (nd.). What's. a fake internship? Warning signs and how to avoid scams. Internshala Blog.
[2] Patel, P. R. (2026). Detection of fraudulent internship opportunities using machine learning techniques. Journal of Artificial Intelligence and Cyber Security, 8(2), 45–58.
[3] Zhang, K., & Arunasalam, A. (2025). International students and scams: At risk abroad. International Journal of Cyber Studies, 14(1), 33–49.

[4] Lin, K., Wu, Y., et al. (2025). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. Journal of Cybercrime Research, 12(3), 101–118.

[5] Tan, K. K. W., Sapiri, H., et al. (2024). Perception of university undergraduate students in off-campus residential areas towards online scamming: A case study. Asian Journal of Criminology, 9(2), 55–70.

[6] Huang, Z. (2024). Perception and responses of college students to financial scams. International Journal of Social Research, 11(1), 72–85

[7] Ignes, G. K. D. A. (2023). Prevalence of online buying scam fraud exposure among business administration students. Journal of Business Administration Research, 15(2), 88–97.

[8] Adegbola, I., & Fadara, O. (2022). Cybercrime among mathematical science students: Implications on their academic performance. Nigerian Journal of Educational Research, 14(2), 40–56.

[9] Conway, G., & Hadlington, L. (2021). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk, and victimization. Cyberpsychology Journal, 9(3), 112–126.

[10] Chiluwa, I. E., & Samoilenko, S. A. (2019). Handbook of research on deception, fake news, and misinformation online. IGI Global.

[11] Broadhurst, R., Skinner, K., et al. (2018). Phishing and cybercrime risks in a university student community. Journal of Cybersecurity Education, 10(1), 66–80.

[12] Bidgoli, M., & Grossklags, J. (2017). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. Information Security Journal, 26(2), 89–101.

[13] Bidgoli, M., & Grossklags, J. (2017). Phone spoofing and cyber fraud targeting international students. Cybersecurity Review, 5(1), 23–34.

[14] Lindsay, M., Booth, J. M., et al. (2016). Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear. Journal of Youth Studies, 19(5), 601–615

[15] Donner, C. M., & Jennings, W. (2016). The general nature of online and offline offending among college students. Criminology Research Journal, 12(2), 67–81.

[16] Donner, C. M. (2016). The gender gap and cybercrime: An examination of college students' online offending. Journal of Criminal Behavior, 8(1), 34–48

[17] Yu, S. (2014). Fear of cybercrime among college students in the United States: An exploratory study. Cyber Psychology Review, 6(2), 77–90.

[18] Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. Journal of Crime and Justice, 36(1), 1–19

[19] Lindsay, M., & Krysik, J. (2012). Online harassment among college students: A replication incorporating new Internet trends. Journal of Social Work Research, 36(4), 345–359.

[20] Kohm, S. A., Waid-Lindberg, C. A., et al. (2012). The impact of media on fear of crime among university students: A cross-national comparison. Canadian Journal of Criminology, 54(3), 321–339

[21] Nizar, N. M. S., et al. (2012). Awareness of online scams among Muslim university students in Malaysia. Asian Journal of Social Science, 8(1), 45–59.

[22] Qiu, M., & Yang, Y. (2012). Analysis of the current situation and characteristics of college student online fraud cases. Journal of Information Security, 7(2), 89–97.

[23] Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. Journal of Interpersonal Violence, 25(12), 2178–2195

[24] Finn, J. (2004). Survey of online harassment at a university campus. Journal of Interpersonal Violence, 19(4), 468–483.

[25] Durkin, K. F., Wolfe, T. W., et al. (1996). College students' use of fraudulent identification to obtain alcohol: An exploratory analysis. Journal of Alcohol Studies, 57(1), 54–61.

[26] Caron, M. D., Whitbourne, S. K., et al. (1992). Excuse making among college students. Journal of Educational Psychology, 84(3), 321–330.