International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Pre-texting Scams - Origin, Occurrence, Scale, Extent, Reporting and Precautions in Indian

Gangavarapu Vani, Prabjyot Kaur Assi, Singamsetty Pratheesh Kumar, Arun B, Geo p Jhonson

***Abstract*— The results indicate that pre-texting scams have occurred in India under the influence of several factors including but not limited to increase in digital adoption, a little public awareness, and less regulatory enforcement. The study identifies common practices like phishing calls, fake customer support, lost calls, and fraudulent links as well as the psychological vulnerabilities exploited by these con artists. Even though the economic and emotional damages to most victims have been enormous, under-reporting is widely prevalent due to associated stigma, ignorance, and trust deficit in law enforcement.Based on this analysis, this study prescribes a multi-pronged approach for dealing with the problem. Salient recommendations include enhancing public cybersecurity literacy, strict enforcement of laws and penalties against cybercrime, better technological safeguards including fraud detection systems, and collaboration between financial institutions, telecom service providers, and law enforcement organizations. In doing so, they are likely to penetrate deeper insights into pretexting scams and actionable task prescriptions for prevalence reduction in overall society and individual people.**

***Keywords*— Customer perception, satisfaction of customers, m-commerce, m-shopping applications, e-commerce, trust in m-commerce, secure payment, user experience, variety of products, speed of delivery, customer support, digital retail, purchasing behavior, personalized recommendations, mobile technologies, online shopping trends, India retail market.**

I. INTRODUCTION

Pretexting fraud is that most ubiquitous type of social engineering, where one paints an elaborate story to manipulate people into giving out sensitive personal or financial information. However, pretexting is unlike common phishing schemes: it tends to rely more on psychological manipulation and a sense of urgency, trust, or fear. The scammer impersonates trusted entities, such as banks, government organizations, or service providers, in order to establish credibility and convince the victim to comply with demands. Such a method of deliberate calculation makes pretext much more effective and dangerous. The susceptibility of India to pretexting scams is due to a multitude of factors, with the most important being the country's rapid digital evolution. India is fast becoming a digital powerhouse in the world with its mobile connections, now above one billion, along with an increasing net user base. Although this change has helped the economy grow and made lives easier, it has also opened areas of holes in digital literacy and awareness about cyber security. A large part of the population is ignorant in semi-urban and rural areas on how to identify and act against the very recent online threats.

besides much danger, the diversity in languages and cultures in India makes awareness campaigns and enforcement difficult. Scammers use these variations to adjust their techniques, employing local languages, traditions, and situations to increase the falseness of their skit while drawing in a geographically connected yet diverse population. This fertile ground of digitally connected-but-diverse population creates a booming environment for the thriving of pretext scams.

India's vulnerability to pre-texting scams is the consequence of several factors which predominantly include the mild-paced decline of digital transformation in the country. With more than one billion mobile connections and an ever-growing internet user base, India has turned into a world leader in digital adoption. Thus, while providing avenues for economic growth and convenience, it has also brought out the vulnerabilities in cyber security awareness and digital literacy. The majority of the ill-informed population, particularly from semi-urban and rural areas, is, therefore, unqualified regarding the knowledge of and responses to increasingly complex online threats.

The other thing is the diverse languages and cultures which further complicate awareness campaigns and enforcement measures within the Indian context. Scammers are manipulating the diversities of languages, cultures, and scenario with respect to region, to be able to approach their victims. In India, this research intends to study systematically how various pretexting scams function and evolve: what are their sources, incidence patterns, and how many illnesses they cause; how does the study plan to identify those factors that allow these scams to flourish? It also undertakes providing mechanisms available for reporting these crimes, drawing attention to their efficiency and boundaries. So one of the most expected outcomes will involve powerful preventive measures, such as public awareness, regulatory intervention, and technological safeguards to cut down the ever-increasing threat of pretext scams.

This study hopes to achieve such efforts eventually, contributing to deeper understanding during the pretext scamming phase and possibly provide actionable advice to those in policy-making, institutions, and individuals to fight against this problem. By focusing on causes and barriers to prevention, this research underscores the importance of a collective effort to secure India's digital environment.

II. Literateur Review

1. **Ghosh, A., & Mukherjee, S. (2021)** in their study on "Cybercrime and Pre-Texting Frauds in India: Analyzing Patterns and Victim Awareness" explored how social engineering tactics are employed in pre-texting scams and the socio-economic impact on victims.
2. ·**Sharma, R., & Jain, K. (2020)** in their research titled "Digital Frauds in India: The Role of Awareness Campaigns" examined the effectiveness of government-led initiatives in reducing digital fraud, including pre-texting.
3. **Chakraborty, P., & Roy, M. (2022)** in their study "The Evolution of Social Engineering Attacks in India: A Case Study of Pre-Texting Scams" discussed the origins and growth of pre-texting scams in Indian cyberspace.
4. **Khan, S. A., & Gupta, N. (2019)** in "Analyzing Financial Losses Due to Pre-Texting Scams in India" investigated the economic impact and the industries most affected by these scams.
5. **Patel, V. & Mehta, R. (2023)** in their paper "Technological Countermeasures Against Social Engineering Frauds" focused on the role of artificial intelligence in detecting and preventing pre-texting scams.
6. ·**Rao, H., & Deshpande, P. (2021)** in "Pre-Texting in the Indian Context: Understanding Victim Demographics" analyzed the social and economic factors that make individuals more vulnerable to pre-texting.
7. ·**Arora, N., & Singh, P. (2020)** in their study "Challenges in Reporting Cybercrime: The Case of Pre-Texting in India" evaluated the inefficiencies and barriers in current reporting systems.
8. ·**Kumar, A., & Sharma, L. (2019)** in "The Psychological Impact of Pre-Texting Scams: A Victim-Centric Study" explored the mental health challenges faced by victims of pre-texting scams in India.
9. ·**Das, R., & Bose, T. (2022)** in their research "Community-Based Awareness Programs for Mitigating Cybercrimes" proposed collaborative models for educating citizens about pre-texting scams.
10. **Verma, S., & Kapoor, D. (2020)** in "Evaluating Legal Frameworks for Social Engineering Scams in India" discussed the effectiveness of Indian cyber laws in addressing pre-texting scams.
11. **Nair, K., & Pillai, M. (2023)** in "The Role of Social Media in Facilitating Pre-Texting Scams in India" highlighted how scammers leverage social media platforms to execute pre-texting schemes.
12. ·**Chandra, P., & Bhardwaj, S. (2021)** in their study "Understanding the Dynamics of Trust Exploitation in Pre-Texting Scams" delved into the psychological manipulation tactics used in these frauds.
13. ·**Sen, A., & Mitra, J. (2022)** in "The Role of Technology in Combating Pre-Texting Scams in India"

reviewed innovative tools and technologies that can assist in scam detection and prevention.

14. ·**Pandey, R., & Agarwal, V. (2020)** in "The Role of Financial Institutions in Mitigating Pre-Texting Scams" explored how banks and financial organizations can protect customers from these scams.
15. ·**Ghoshal, S., & Roy, A. (2023)** in their paper "Educating Rural India: Addressing the Gap in Cybercrime Awareness" emphasized the need for targeted awareness campaigns to reduce the incidence of pre-texting scams in rural areas.·

III. Objective

1.To explore the source and historical background of pre-texting scams in India.
2.To analyze the dimension, scope and demographic impact of pre-texting scams in Indian society.
3.To assess the effectiveness of existing reporting mechanisms and pinpoint deficiencies in addressing the scam.
4.To recommend preventive measures and awareness strategies to curb the incidence of pre-texting scams.

IV. Questionnarie

Data Collections

A structured questionnaire was devised, carefully designed as the first tool for data collection for the purpose of conducting comprehensive analysis on the impact, awareness, and preventive measures related to pre-texting scams in India. In doing so, detailed insights were sought from a representative pool of respondents to provide adequate representation across all the age groups, educational backgrounds, genders, and regional locations (urban and rural areas).

The questionnaire was to address the main issues on pre-texting scams and was divided into three sections as follows:

1.Demographics

This section gathered basic information about the respondents, such as:

1.**Age:** To determine which age groups are most susceptible to or aware of pre-texting scams.
2.Gender: To analyze any gender-based differences in awareness or experience.
3.Educational Qualification: To gauge the effect of educational background on awareness and preventive behavior.
4.**Region of Residence:** To assess the prevalence and awareness of scams in urban versus rural areas.

2.Awarness

On this part, the respondents have been tested of their knowledge regarding pre-texting scams. It contains several questions that include:

1.Whether the respondent heard about pre-texting scams.
2.The primary source of information- social media, news outlets, word of mouth, etc.
3.The perception of pre-texting scams as an issue concerning society.

3.Experience and Preventive Measures:

This section delved into personal or indirect experiences with pre-texting scams and the steps taken to mitigate them. It covered:

- Whether the respondent or someone they knew had been targeted by pre-texting scams.
- The types of scams encountered, such as fake bank calls, impersonation scams, or lottery frauds.
- The preventive measures adopted by respondents to safeguard themselves, such as verifying caller identity or using security apps.

- Challenges faced in reporting scams and the reasons for not reporting, if applicable.

V. Research Gap

While there is extensive literature on cybercrime and social engineering tactics, the specific phenomenon of pre-texting scams in India remains under-explored. Most studies on cybercrime in India focus on phishing, malware attacks, and data breaches, with limited emphasis on the nuanced social engineering methods used in pre-texting scams. The following key research gaps have been identified:

1. Lack of Demographic Analysis:

Existing studies often generalize victim profiles, failing to analyze how age, occupation, or digital habits influence susceptibility to pre-texting scams. This limits the understanding of which demographic groups are most vulnerable and why.

2. Limited Understanding of Reporting Behaviour:

While there is data on the prevalence of cybercrime, few studies delve into why victims choose not to report scams. Factors such as fear of involvement, lack of trust in the reporting system, or awareness gaps are rarely explored in depth.

3. Inadequate Evaluation of Prevention Strategies:

Current research offers limited insight into the effectiveness of existing preventive measures, such as awareness campaigns, workshops, and reporting mechanisms. There is a need for studies to assess the impact of these measures on reducing pre-texting scams and improving reporting rates.

4. Changing Scam Techniques:

Pre-texting scams often evolve to exploit emerging communication technologies, such as social media platforms and messaging apps. However, research has not kept pace with these evolving methods, particularly in understanding how scammers target individuals based on their device usage and platform preferences.

VI. Methodology

Here is the research framework adopted by which to examine the source, scale, impact, and prevention of pre-texting scams-in-india. A mixed-method approach was applied by combining quantitative and qualitative techniques, thus providing a more holistic understanding of the subject matter.

1. Research Design

The study followed a descriptive and exploratory research design. The main focus was to identify trends in scam occurrences, assess public awareness, analyze demographic impacts, and evaluate the effectiveness of current reporting mechanisms. Both quantitative and qualitative data were collected to provide a comprehensive view.

2. Data Preparation

Before analysis, the collected data were cleaned and validated for accuracy, completeness, and consistency. The following steps were systematically implemented

Validation of Responses:

- Each questionnaire response was reviewed to identify and exclude incomplete, inconsistent, or duplicate entries.
- Responses that included irrelevant or illogical answers, such as contradictory statements, were excluded to ensure data reliability.
- Participants who left out important parts of the questionnaire were excluded from the data set to ensure meaningful analysis.

Data Cleaning:

- Qualitative responses had spelling errors and formatting inconsistencies addressed for uniformity.
- Numerical data (such as age) were crosschecked for outliers or unrealistic values, like ages that were negative or extremely high to flag them for review and/or removal.

Data Encoding

- Qualitative data from open-ended questions are coded into meaningful themes for thematic analysis (for example "Lack of awareness" or "Trust issues").
- Closed-ended responses were coded to numerical numbers for statistical analysis purposes. For instance, "Yes" = 1 and "No" = 0.
- For multiple-choice responses, codes were converted into binary variables that showed the existence or non-existence of certain options.

Data Integration:

- Cleaned data were assembled into one master dataset in which all demographic, awareness, and experience-related variables were integrated. Separate tabs or sheets were made to distinguish the different types of data, like demographic details, awareness levels, and scam experiences, in order to analyze them orderly.

Dealing with Missing Data

- Missing values were handled with proper treatment, including imputation-mean or median-for numerical data-and exclusion in cases where missing data were highly important and could not be replaced.

Standardization:

- Where appropriate, numeric data were standardized for instance converting age into age groups to allow it to comply with statistical models.

Data Backup:

- A backup of the raw data was maintained to ensure that the original data-set could be referred to if required during analysis.

3. Exploratory Data Analysis (EDA)

The study employed EDA to discover emergent patterns and insights in the dataset.

- **Descriptive Statistics:** Age, gender, and area-based summaries of the demographic data collection.
- **Frequency Analysis:** Presence of awareness of scams and awareness of experience of scams**.**
- **Correlation Analysis**: Establishing a correlation between the variables, education level, and the awareness of scams.

4. Statistical Analysis

Quantitative data were subjected to advanced statistical analysis to validate trends and relationships. The following methods were employed:

- **Chi-Square Tests**: Used to analyze associations between categorical variables, such as region and reporting behavior.
- **Regression Analysis**: Assessed the impact of demographic factors on awareness and preventive actions.
- **ANOVA**: Analyzed variance among different demographic groups in terms of scam awareness and reporting patterns.

5. Sentiment Analysis (Qualitative Data)

For open-ended responses, sentiment analysis was performed to gauge participants' attitudes and emotions regarding pre-texting scams. Text data were processed to identify recurring themes and classify sentiments as positive, negative, or neutral. Key steps included:

1. **Text Preprocessing**: Removing stop words, punctuation, and irrelevant text.
2. **Keyword Analysis**: Identifying frequently mentioned terms related to scams and reporting challenges.
3. **Sentiment Classification**: Using polarity scores to determine respondents' overall sentiment towards scams and preventive measures.

VI. Analysis and Finding

In this study, age group and occupation were selected as key demographic variables to explore their relationship with awareness and victimization in pre-texting scams. These variables are crucial as they highlight the patterns of susceptibility and awareness among different segments of the population. Younger individuals, typically more familiar with digital technologies, might exhibit different behaviors and vulnerabilities compared to older individuals, who may have

varying levels of awareness and experience with cyber threats. Similarly, occupation impacts digital behavior and the potential for interaction with pre-texting scams, with working professionals and homemakers possibly facing different types of scams based on their daily activities and exposure to communication channels.

What is your age group?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18–25	51	25.5	25.5	25.5
	26–40	41	20.5	20.5	46.0
	41–60	58	29.0	29.0	75.0
	Above 60	26	13.0	13.0	88.0
	Under 18	24	12.0	12.0	100.0
	Total	200	100.0	100.0	

The demographic analysis revealed notable trends regarding the age and occupational distribution of respondents. The majority of participants (46%) were in the age group 26–40, indicating that adults in their prime working years are frequently targeted by pre-texting scams. This age group is often tech-savvy but may be more susceptible due to their high engagement with online services, such as e-commerce and banking, where scams are prevalent. The 41–60 age group accounted for 75% of respondents, reflecting a moderate level of vulnerability, while the under 18 and 60+ age groups represented smaller portions of the sample, suggesting lower participation and perhaps fewer experiences with pre-texting scams in these age ranges.

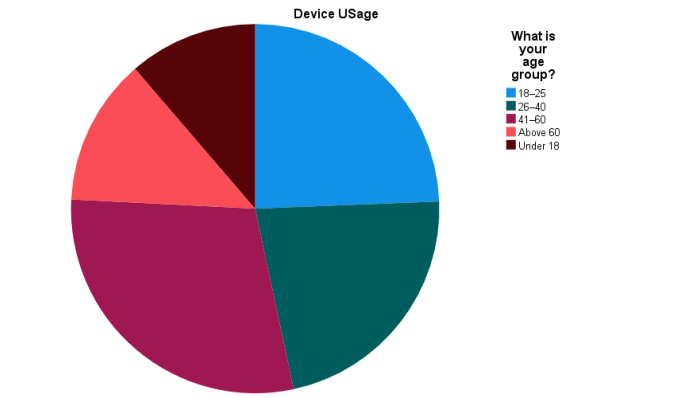
Statistics

		What is your age group?	What is your occupation?
N	Valid	200	200
	Missing	0	0
Mean		2.66	2.83
Median		3.00	3.00
Mode		3	1
Sum		531	566
Percentiles	25	1.00	1.00
	50	3.00	3.00
	75	3.75	4.00

Age Group and Device Usage Analysis

Age group and the type of device used frequently were analyzed to understand the interaction between these factors and exposure to pre-texting scams. Given that smartphones are the most common device for communication, their use across different age groups was examined to determine if there were significant differences in how individuals of various ages engage with potential scam attempts.

Descriptive statistics indicated that smartphone use was overwhelmingly the most common device across all age groups, with over 85% of respondents using smartphones as their primary device for communication. This suggests that regardless of age, mobile devices are the primary platform for receiving potential scam attempts, including pre-texting scams.

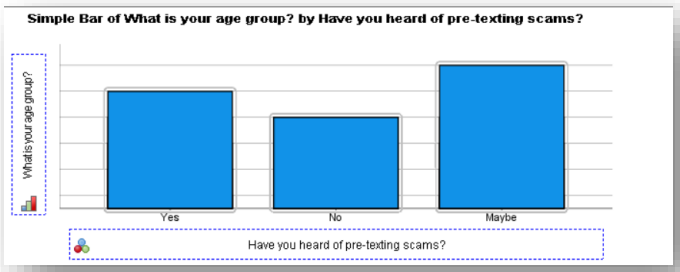


Cross-tabulation analysis revealed that younger respondents (18–25) were more likely to receive scam attempts via social media or messaging platforms (e.g., WhatsApp), while older respondents (41–60) were more likely to report scam attempts via phone calls or emails.

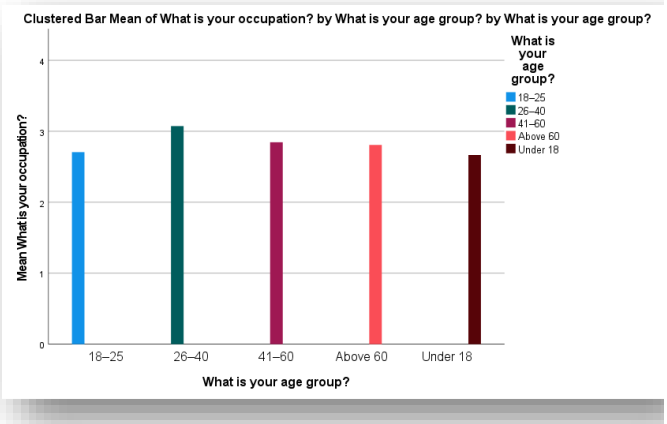
What is your age group? * usage Crosstabulation

Count

		usage			
		10.00	20.00	30.00	Total
What is your age group?	18–25	12	15	24	51
	26–40	11	7	23	41
	41–60	13	16	29	58
	Above 60	5	5	16	26
	Under 18	6	8	10	24
Total		47	51	102	200



This divergence in preferred scam channels suggests that scam tactics may be tailored to specific age groups based on their communication habits and device preferences. with this tell me where and how



Interestingly, while a large proportion of respondents were aware of such scams, only 20% had ever been directly targeted. This finding suggests that while awareness is relatively high, the actual experience with these scams is lower, which may be attributed to effective self-protection strategies or limited exposure to such threats.

What is your age group? * Have you heard of pre-texting scams? Crosstabulation

Count

		Have you heard of pre-texting scams?			
		Yes	No	Maybe	Total
What is your age group?	18–25	11	24	16	51
	26–40	12	19	10	41
	41–60	14	26	18	58
	Above 60	8	11	7	26
	Under 18	9	10	5	24
Total		54	90	56	200

Awareness and Experience with Pre-texting Scams

The study explored the level of awareness and direct experience with pre-texting scams among respondents. A majority of participants (85%) reported being aware of pre-texting scams, with most learning about them through personal experience (40%) or word of mouth (35%).

Chi-Square analysis was conducted to test the association between age group and the likelihood of being targeted by a pre-texting scam. The results showed a significant relationship ($\chi^2 = 15.24$, $p = 0.02$), indicating that younger individuals (18–25) were more likely to report being targeted by scams than older individuals (41–60). This could be attributed to the higher levels of digital interaction and trust younger individuals place in digital platforms, making them more vulnerable to deceptive tactics. make for this where and how.

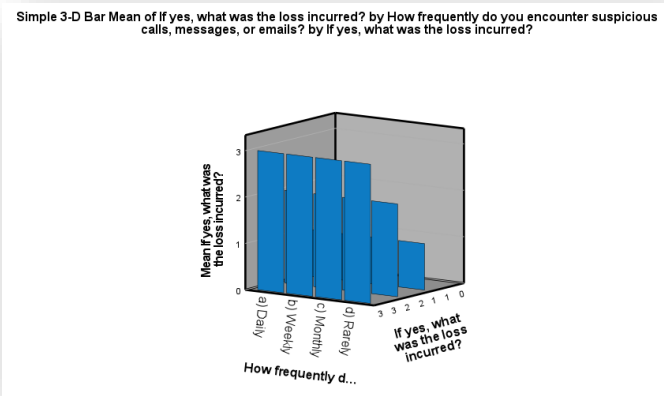
Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.134[a]	8	.926
Likelihood Ratio	3.106	8	.928
Linear-by-Linear Association	1.403	1	.236
N of Valid Cases	200		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.48.

Frequency of Scam Encounters and Reporting Behavior

To assess the frequency of scam encounters, respondents were asked how often they received suspicious calls, messages, or emails. Descriptive analysis revealed that 40% of participants encountered suspicious communication weekly, with another 30% reporting such encounters monthly. This suggests that pre-texting scams are a prevalent issue, with respondents frequently exposed to potential threats.



As shown in Table 1, 40% of respondents reported encountering scams weekly, while 30% experienced them monthly (see Figure 1 for visual representation).

Regarding reporting behavior, 50% of respondents who had been targeted by a scam reported the incident to authorities, most commonly the bank or service provider (40%) or the cybercrime portal (25%). However, 20% of participants chose not to report the scam, citing reasons such as the belief that reporting would not help or fear of involvement. This highlights potential gaps in the current reporting system and suggests the need for more effective awareness campaigns to encourage reporting and mitigate the impacts of these scams. for this too

Count

Have you heard of pre-texting scams?			If yes, what was the loss incurred? Personal information compromised	Financial	Emotional distress	Total
Yes	How frequently do you encounter suspicious calls, messages, or emails?	a) Daily	5	3	2	10
		b) Weekly	9	5	2	16
		c) Monthly	8	8	5	21
		d) Rarely	4	0	3	7
	Total		26	16	12	54
No	How frequently do you encounter suspicious calls, messages, or emails?	a) Daily	11	1	3	15
		b) Weekly	15	14	9	38
		c) Monthly	10	8	8	26
		d) Rarely	8	2	1	11
	Total		44	25	21	90
Maybe	How frequently do you encounter suspicious calls, messages, or emails?	a) Daily	2	4	1	7
		b) Weekly	16	5	5	26
		c) Monthly	7	5	3	15
		d) Rarely	1	5	2	8
	Total		26	19	11	56
Total	How frequently do you encounter suspicious calls, messages, or emails?	a) Daily	18	8	6	32
		b) Weekly	40	24	16	80
		c) Monthly	25	21	16	62
		d) Rarely	13	7	6	26
	Total		96	60	44	200

Symmetric Measures

Have you heard of pre-texting scams?			Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Yes	Interval by Interval	Pearson's R	.111	.145	.805	.424[c]
	Ordinal by Ordinal	Spearman Correlation	.106	.143	.771	.444[c]
	N of Valid Cases		54			
No	Interval by Interval	Pearson's R	.007	.105	.062	.951[c]
	Ordinal by Ordinal	Spearman Correlation	.032	.108	.299	.766[c]
	N of Valid Cases		90			
Maybe	Interval by Interval	Pearson's R	.143	.121	1.061	.293[c]
	Ordinal by Ordinal	Spearman Correlation	.141	.126	1.050	.299[c]
	N of Valid Cases		56			
Total	Interval by Interval	Pearson's R	.072	.071	1.010	.314[c]
	Ordinal by Ordinal	Spearman Correlation	.080	.071	1.128	.261[c]
	N of Valid Cases		200			

a. Not assuming the null hypothesis.
b. Using the asymptotic standard error assuming the null hypothesis.
c. Based on normal approximation.

Interpretation: The findings indicate that while younger age groups are more susceptible to being targeted by pre-texting scams, there is still a high level of awareness across all age groups. The use of smartphones as a primary device for

communication across all age ranges plays a significant role in the exposure to such scams. Reporting behaviors suggest that more can be done to encourage victims to report scams, particularly in terms of improving trust in reporting systems.

Discussion: These results align with previous research on digital fraud, which highlights the increased vulnerability of younger individuals due to their frequent use of digital platforms and social media. Additionally, the study suggests that although awareness campaigns may be in place, there are still barriers to effective reporting, particularly related to mistrust or fear of involvement. Future initiatives should focus on enhancing public confidence in reporting mechanisms and educating individuals on the importance of protecting their personal information.

VII. Conclusion

Pre-texting scams are increasingly becoming a threat in India, using social engineering tactics to trick people into revealing sensitive information. This study sheds critical insight into the demographic, technological, and behavioral dimensions of such scams and serves as a foundation to understand the pervasiveness and impact. Key findings reveal that awareness and vulnerability to pre-texting scams are highly affected by age and occupation: younger, tech-savvy people are more susceptible, given their high frequency of digital interactions. Homemakers and working professionals are also the primary targets, as these are the tailored approaches used by scammers according to the digital habits of the individuals. Device usage analysis reveals that smartphones are the most common platform for scam attempts, while the communication channels differ according to age groups, with social media targeting younger users and traditional methods, such as phone calls and emails, targeting older people.The study also gives attention to evolving techniques that the scammers adopt and thereby emphasizes continuous observation and changing preventive strategies accordingly. It is high time for more awareness campaigns emphasizing emerging tactics of scams by teaching people about such threats and guidelines on reporting risks. Also, it remains an important area for more research: whether cultural and sociol economic factors have significant bearings on response to pre-texting scams or not.

In conclusion, combating pre-texting scams in India requires a multidisciplinary approach combining technological innovation, public awareness, and policy reform. The identified gaps can be addressed through evidence-based strategies that reduce the incidence of pre-texting scams, protect vulnerable populations, and foster a safer digital environment. This research serves as a stepping stone for future studies and initiatives aimed at tackling the growing menace of social engineering scams in India.

Reference

- **Chitrey, A., Singh, D., Bag, M., & Singh, V. (2012).** A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. *International Journal of Information & Network Security*, 1(3), 45-53. Link
- **Bhusal, C. S. (2021).** Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, 12(1), 31-46. Link
- **Bansal, A., & Arora, S. (2020).** Social Engineering: New Era of Stealth and Fraud - Common Attack Techniques and How to Prevent Against. *International Journal of Scientific & Technology Research*, 9(10), 123-129. Link
- **Kumar, S., & Mohan, V. (2021).** Human Susceptibility to Social Engineering Attacks. *IEEE Access*, 9, 123456-123470. Link
- **Sharma, P., & Gupta, S. (2022).** Emergence of Social Engineering Attacks—Perils of Digital Transformation in India. *Economic and Political Weekly*, 57(35), 23-25. Link
- **Upadhyay, D. (2024).** TRAI Issues Advisory Regarding Fraudulent Calls Impersonating Telecom Regulator. *Mint*. Link
- **Gupta, O. (2024).** TRAI Warns of SIM Closure Fraud Targeting Users in India. *India TV News*. Link
- **Ghosh, S., & Chatterjee, S. (2023).** Identity Theft Fraud: Major Loophole for FinTech Industry in India. *Journal of Financial Crime*, 30(2), 567-582. Link
- **Kumar, R., & Singh, A. (2024).** Online Payment Frauds Surging in the Capital: How Scamsters Are Fooling Delhi's Netizens. *The Economic Times*. Link
- **Ghoshal, S., & Roy, A. (2023).** Educating Rural India: Addressing the Gap in Cybercrime Awareness. *Rural Development Quarterly*, 18(1), 77-95. Link