iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** X **Month of publication:** October 2025

DOI: https://doi.org/10.22214/ijraset.2025.74467

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

Cybersecurity Awareness in Goa: A Descriptive and Inferential Study

Gaurav A. Naik
Info Tech Corporation of Goa Limited, India

Abstract: ***This study assesses cybersecurity awareness among internet users in Goa, focusing on young adults, students, and professionals. Using an online survey, data were analyzed through descriptive statistics and chi-square tests to evaluate awareness of online risks, reporting behaviors, and associations with demographic factors.***
Findings show that most respondents were young adults (18–25) and students, with high daily internet usage but limited knowledge of cyber risks. While 59.8% felt confident identifying scams, 40.7% lacked knowledge of reporting mechanisms. Willingness to report cybercrime (65.9%) was significantly associated with trust in Goa Police, while status correlated with internet use. However, no significant links were observed between age and reporting knowledge.
The results highlight partial and inconsistent cyber awareness, low exposure to safety campaigns, and mixed trust in law enforcement. Strengthening digital literacy, expanding outreach initiatives, and enhancing institutional trust are recommended to improve cyber resilience in Goa.

I. INTRODUCTION

In today's digital era, the internet has become an integral part of personal, professional, and governmental activities. Rapid technological adoption has not only created opportunities for growth and connectivity but also exposed individuals and institutions to a wide range of cybersecurity threats. Cybercrimes such as phishing, identity theft, financial fraud, ransomware attacks, and online harassment are growing at an alarming rate, threatening both individual safety and national security. According to recent studies, India ranks among the countries experiencing a sharp increase in cybercrime cases, with young internet users being the most vulnerable group. Cybersecurity awareness plays a critical role in reducing exposure to such risks. Awareness determines how effectively individuals recognize suspicious activities, protect their digital assets, and respond to threats. However, despite multiple national campaigns and policy measures, research consistently highlights that ordinary users often lack adequate knowledge of cyber risks and safe practices. This lack of awareness is especially concerning in regions with high internet penetration but limited structured digital literacy initiatives. In the state of Goa, which has a rapidly growing base of young internet users due to its educational institutions and expanding digital infrastructure, the issue of cybersecurity awareness takes on special significance. While internet access is widespread, questions remain about whether users are adequately informed about online risks, cybercrime reporting mechanisms, and preventive practices. For instance, anecdotal evidence suggests that while many individuals are confident in using social media and online services, they may not be equally prepared to detect scams or report cyber incidents to appropriate authorities. This research paper therefore focuses on evaluating the state of cybersecurity awareness in Goa through both descriptive and inferential statistical approaches. The study aims to identify who is most aware, who remains vulnerable, and what factors influence awareness and reporting behaviors. By analyzing responses collected from a diverse set of participants—including students, professionals, and business owners—the study seeks to highlight both strengths and gaps in current awareness levels.
The structure of this paper is organized as follows: Section III reviews relevant literature on cybersecurity awareness and its importance in digital societies. Section IV outlines the working model of the study, including survey design and data analysis methods. Section V details the objectives of the research, while Section VI discusses the methodology used, including the application of descriptive and chi-square statistical analyses. Section VII presents the results, followed by discussion and interpretation. Section VIII concludes with key insights, implications, and recommendations for improving cyber literacy in Goa.

II. LITERATURE REVIEW

A. Cybersecurity Awareness in India: Current State

Multiple Indian studies consistently report high internet adoption but uneven cybersecurity awareness, with gaps in password hygiene, phishing recognition, and reporting pathways. Recent national syntheses highlight that while programs such as Cyber Swachhta Kendra, DISHA, and ISEA exist, coverage and depth remain inconsistent, especially for first-time and rural users [1].

Across higher education cohorts, awareness levels vary by institution and demographic profile; targeted instruction and repeated exposure improve outcomes, but many students still lack procedural know-how (what to do, where to report) [2,3]. Broader market analyses indicate organizations are investing in security, yet end-user practices remain a weak link—supporting the need for population-level awareness and literacy initiatives that complement enterprise controls [11].

B. Youth and Student Populations

Surveys focused on youth and higher-education institutions find strong device and social-media usage coupled with partial, self-assessed knowledge of risks. Structured training and curriculum integration consistently improve recognition of phishing/scams and safe-use behaviors [2,3]. These patterns mirror national concerns about translating "awareness" into actionable behaviors.

C. Campaigns and Digital Literacy Efforts

Recent commentaries on digital literacy and cybersecurity argue for jointly designed programs (schools, municipalities, police, and NGOs), noting that standalone one-off sessions have short-lived impact without reinforcement channels [1]. Indian reviews similarly recommend localized content, helpline signposting, and simulation-based training to bridge the "know–do" gap—points relevant to Goa's outreach planning [1].

D. Reporting Behavior And Trust In Institutions

Criminology and cybercrime reporting literature shows that trust/confidence in police is a strong predictor of whether victims report, alongside factors like age and income [4,8,14]. This provides a theoretical basis for the finding of the trust in Goa Police ↔ willingness to report (significant chi-square). Studies on cyber victim reporting further emphasize clarity of reporting pathways and expectations of police efficacy as determinants of action—again aligning with your respondents' uncertainty about how to report [7,14].

E. Goa Context: Awareness And Reporting Signals

Recent local reporting notes that Goa ranks high nationally for ability to report cybercrime, attributing gains to coordinated awareness and faster financial fraud interventions; nonetheless, outreach gaps remain [16,17]. These signals dovetail with your descriptive results (mixed trust, many unsure of reporting steps).

F. Synthesis and gap

Across the literature, three gaps emerge that the study addresses for Goa:

1) Measurement gap: Few Goa-specific, population-based assessments triangulate descriptive patterns with tested associations (e.g., status ↔ usage; trust ↔ reporting) [1,2].
2) Behavioural gap: Work often stops at knowledge levels; fewer studies link awareness to reporting intent/behavior in an Indian state context [4,14].
3) Operational gap: Evidence on how local campaigns translate into procedural literacy (exactly how/where to report) remains limited—precisely the weak spot of the data highlights [16,17].

III. RESEARCH METHODOLOGY

The purpose of this study was to evaluate the state of **cybersecurity awareness in Goa**, with a particular emphasis on identifying awareness levels, behavioural intentions, and significant associations between demographic factors and cyber practices. The methodology adopted ensured systematic collection, analysis, and interpretation of data, combining both descriptive and inferential statistical approaches**.**

A. Population and Sample

The population of interest consisted of internet users residing in Goa, spanning different demographic categories such as age, gender, educational status, and profession. To capture perspectives from a digitally active segment, the survey was primarily distributed online.

1) A total of N = [insert exact number of responses] valid responses were collected.
2) The majority of participants were college students, with smaller proportions of working professionals, school students, business owners, and government employees (as detailed in Section VI).

3) This distribution reflects the dominance of youth in Goa's online ecosystem, aligning the sample with the most vulnerable and high-usage group of internet users.

B. Research Design

The study adopted a quantitative, cross-sectional design:

1) Descriptive analysis was applied to summarize demographic factors and awareness levels.
2) Chi-square tests of independence were conducted to examine associations between selected categorical variables.
3) The design is exploratory in terms of mapping patterns of awareness and descriptive in identifying prevailing levels of knowledge and behavior.

C. Data Collection

Data was collected through a structured online questionnaire, administered via Google Forms.

1) The questionnaire contained closed-ended questions (multiple-choice and categorical) covering:
- Demographics (age, gender, residence, status).
- Internet usage patterns.
- Awareness of online risks and ability to recognize scams.
- Willingness and knowledge of reporting cybercrime.
- Exposure to campaigns and trust in law enforcement.

2) The instrument was pilot-tested with a small group before wider distribution to ensure clarity and reliability.

D. Analytical Methods

1) Descriptive Analysis
- Frequency distributions and percentages were calculated to understand demographic breakdowns and awareness levels.
- Results were presented using tables, pie charts, and bar graphs for ease of interpretation.

2) Chi-Square Test of Independence
- Applied to examine whether significant relationships existed between variables such as:
  - Trust in Goa Police ↔ Willingness to Report Cybercrime.
  - Area of Residence ↔ Attendance at Cyber Safety Sessions.
  - Respondent Status ↔ Daily Internet Usage.
  - Knowledge of Online Risks ↔ Willingness to Report.
  - Age Group ↔ Knowledge of How to Report Cybercrime.
- For each test, observed and expected frequency tables were constructed, followed by calculation of chi-square statistic, degrees of freedom, and p-values.
- A significance level of $p < 0.05$ was used to determine statistical relevance.

3) Tools and Software
- Data analysis was carried out using Microsoft Excel and Python libraries (pandas, matplotlib).
- Visualization was used extensively to present findings in an intuitive manner.

E. Ethical Considerations

Participation in the study was voluntary, with responses collected anonymously to ensure confidentiality. Respondents were informed that their data would be used solely for academic research purposes.

IV. RESULTS & ANALYSIS

This section presents the findings of the study, organized into two parts: **descriptive statistics** that summarize general patterns of awareness, and **chi-square tests** that assess associations between demographic and behavioural variables.

A. Descriptive Analysis

1) Demographics: Age and Gender

- The majority of respondents were between **18–25 years (88%)**, followed by 26–40 years and above.
- Males formed **81.9%**, while females constituted **18.1%**, indicating a skewed gender representation.

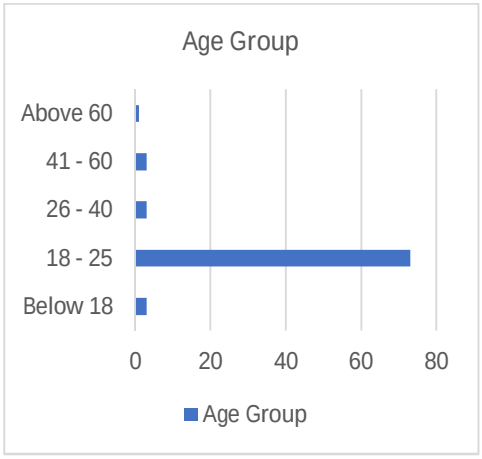


Figure 1: Bar Chart of Age Distribution

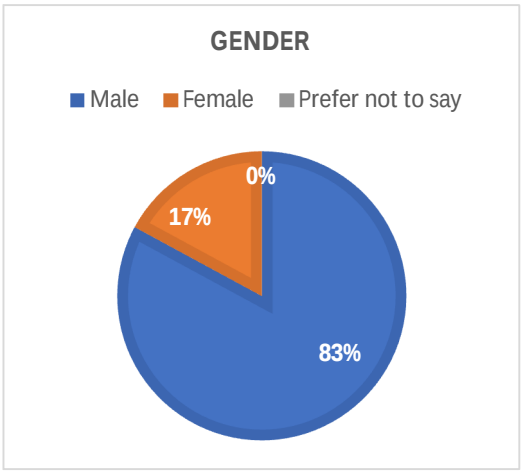


Figure 2: Pie Chart of Gender Distribution

2) Status of Respondents

- College students dominated (81.9%), with smaller shares of working professionals (6%), government employees (3.6%), school students (3.6%), and business owners (2.4%).

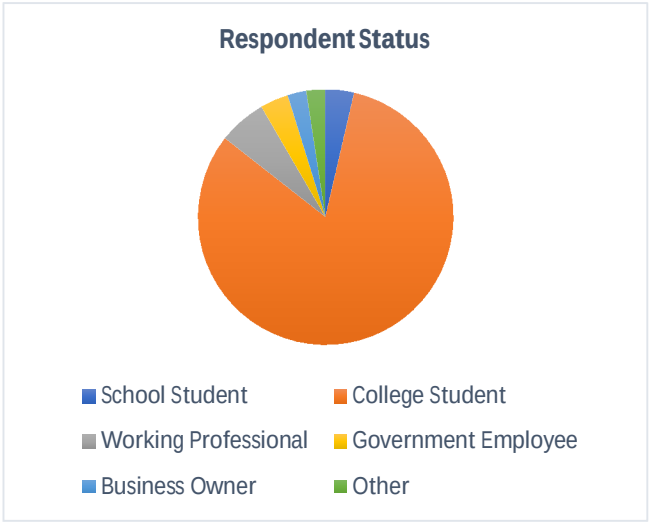


Figure 3: Pie Chart of Respondent Status

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

3) Daily Internet Usage

Heavy internet use was observed, with 33.7% online >6 hours daily, and nearly equal shares spending 1–3 hours (31.3%) and 4–6 hours (30.1%). Only 4.8% reported <1 hour.

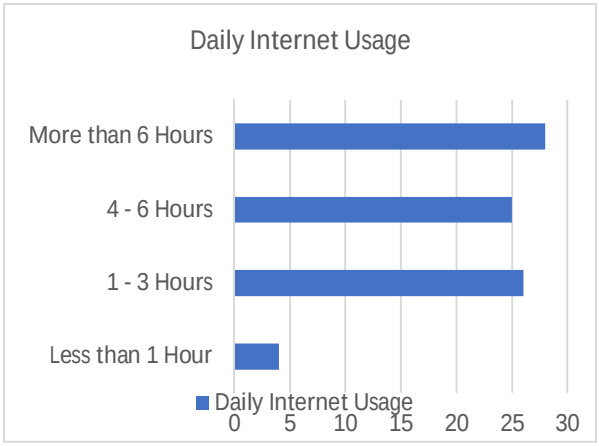


Figure 4: Bar Chart of Daily Internet Usage

4) Awareness and Risk Perception

A large share reported knowing “a little” (70.7%) about online risks, while 24.4% had only heard of them, and 4.9% knew nothing. 59% felt confident recognizing scams, but 32.5% were unsure, and 8.4% admitted inability.

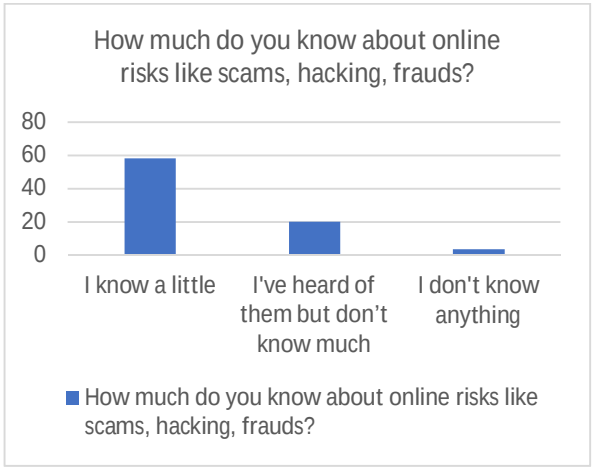


Figure 5: Bar Chart of Awareness Levels

Figure 6: Pie Chart of Scam Recognition Confidence

5) Reporting Behavior and Trust

- 66.3% expressed willingness to report cybercrime, though 28.9% said only if serious, and 4.8% would not report.
- Knowledge of reporting mechanisms was weak: 40.2% had only "heard about it" but did not know how, while 31.7% knew exactly how.
- Trust in Goa Police was mixed: 44.6% said "Yes," 44.6% "Maybe," and 10.8% "No."

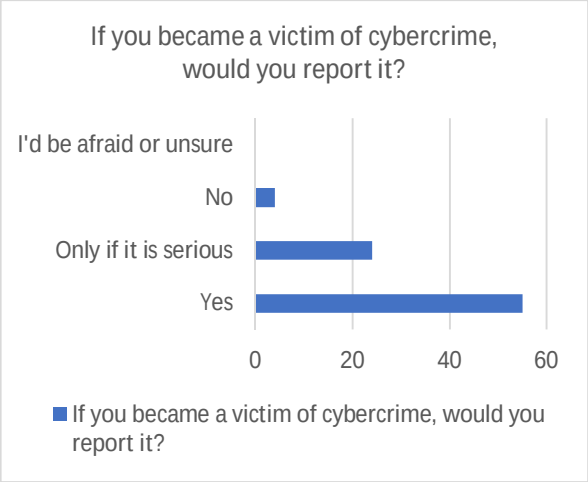


Figure 7: Bar Chart of Willingness to Report

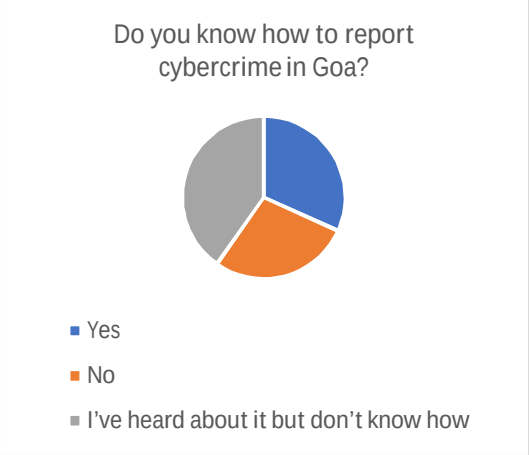


Figure 8: Pie Chart of Knowledge of Reporting Mechanisms

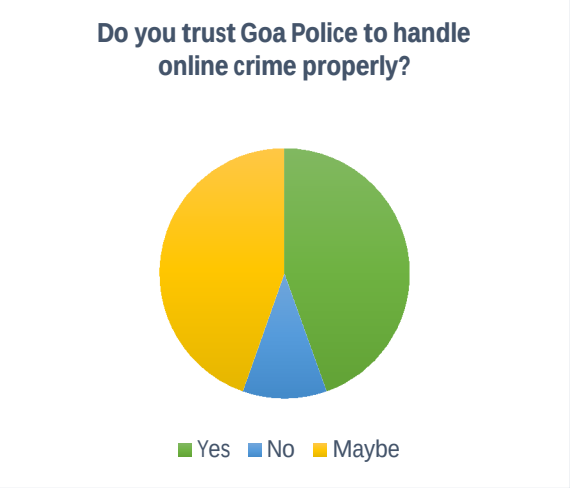


Figure 9: Pie Chart of Trust in Goa Police

6) Exposure to Awareness Campaigns

- 45.8 % had not been exposed to cyber safety campaigns, while 31.3% had, and 22.9% were unsure.
- Similarly, 55.4% had never attended a cyber safety session.

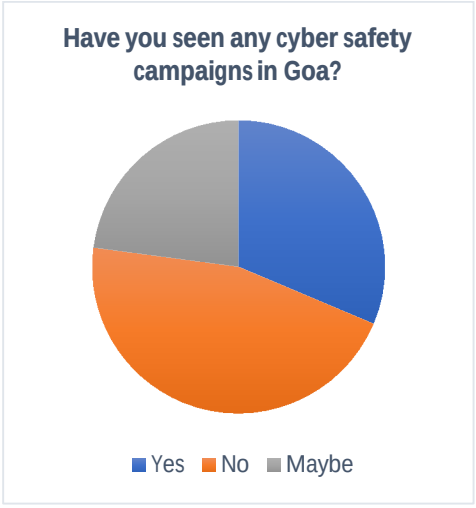


Figure 10: Pie Chart of Campaign Exposure

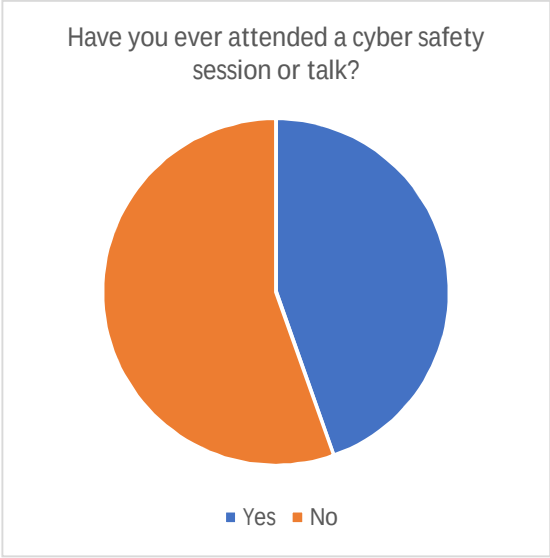


Figure 11: Pie Chart of Session Attendance

B. Inferential Analysis (Chi-Square Tests)

1) Trust in Goa Police ↔ Willingness to Report Cybercrime

- $\chi^2 = 18.09$, df = 4, p = 0.0012 (<0.05).
- **Significant association found**: Respondents who trust police are more likely to report.

Observed Frequency Table

Trust in Goa Police	No	Only if it is serious	Yes
Maybe	0	17	20
No	2	3	4
Yes	2	4	30

Expected Frequency Table

Trust in Goa Police	No	Only if it is serious	Yes
Maybe	1.80	10.83	24.37
No	0.44	2.63	5.93
Yes	1.76	10.54	23.71

Table 1: Observed vs. Expected Frequencies for Trust vs. Reporting

2) *Area of Residence ↔ Attendance at Cyber Safety Sessions*
   - $\chi^2 = 0.000$, df = 1, p = 1.000 (>0.05).
   - No significant association: Urban vs. rural location does not affect attendance.

Observed Frequency Table

Area of Residence	No	Yes
Rural	11	9
Urban	34	27

Expected Frequency Table

Area of Residence	No	Yes
Rural	11.11	8.89
Urban	33.89	27.11

Table 2: Observed vs. Expected Frequencies for Residence vs. Attendance

3) *Respondent Status ↔ Daily Internet Usage*
   - $\chi^2 = 56.71$, df = 15, p < 0.001.
   - Strong significant association: College students reported the highest “>6 hours” use.

Observed Frequency Table

Status	1–3 hours	4–6 hours	Less than 1 hour	More than 6 hours
Business Owner	0	1	1	0
College Student	21	21	0	25
Government Employee	0	1	0	2
Other	1	0	1	0
School Student	0	1	2	0
Working Professional	4	1	0	0

Expected Frequency Table

Status	1–3 hours	4–6 hours	Less than 1 hour	More than 6 hours
Business Owner	0.63	0.61	0.1	0.66
College Student	21.24	20.43	3.27	22.06
Government Employee	0.95	0.91	0.15	0.99
Other	0.63	0.61	0.1	0.66
School Student	0.95	0.91	0.15	0.99
Working Professional	1.59	1.52	0.24	1.65

Table 3: Observed vs. Expected Frequencies for Status vs. Usage

4) *Knowledge of Online Risks ↔ Willingness to Report Cybercrime*
   - $\chi^2 = 7.64$, df = 4, p = 0.105 (>0.05).
   - No significant association: Knowing about risks does not directly influence reporting.

Observed Frequency Table

How much do you know about online risks?	No	Only if it is serious	Yes
I don't know anything	1	0	2
I know a little	2	15	41
I've heard of them but don't know much	1	8	11

Expected Frequency Table

How much do you know about online risks?	No	Only if it is serious	Yes
I don't know anything	0.15	0.85	2
I know a little	2.86	16.47	38.67
I've heard of them but don't know much	0.99	5.68	13.33

Table 4: Frequencies for Knowledge vs. Reporting

5) *Age Group ↔ Knowledge of How to Report Cybercrime*
   - $\chi^2 = 6.70$, df = 8, p = 0.569 (>0.05).
   - **No significant association**: Age does not determine knowledge of reporting channels.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

Observed Frequency Table

Age Group	I've heard about it but don't know how	No	Yes
18-25	28	20	23
26-40	2	0	1
41-60	2	1	0
Above 60	1	0	0
Below 18	0	1	2

Expected Frequency Table

Age Group	I've heard about it but don't know how	No	Yes
18-25	28.93	19.28	22.79
26-40	1.22	0.81	0.96
41-60	1.22	0.81	0.96
Above 60	0.41	0.27	0.32
Below 18	1.22	0.81	0.96

Table 5: Frequencies for Age vs. Reporting Knowledge

C. Summary of Findings

1) High internet use but limited awareness: Most respondents spend >6 hours online yet only "know a little" about risks.
2) Reporting gap: Willingness exists, but procedural knowledge is weak.
3) Trust matters: Confidence in police strongly predicts willingness to report.
4) Outreach gap: Nearly half had never attended campaigns or sessions, indicating insufficient awareness drives.
5) Demographic influence: Student status is a significant factor shaping daily internet use.

V. DISCUSSION

The results of this study provide valuable insights into the state of cybersecurity awareness in Goa and highlight both strengths and persistent gaps.

A. Demographics and Digital Habits

The overwhelming dominance of 18–25-year-old college students reflects the reality that young adults constitute the most digitally active group in Goa. This is consistent with prior studies in Indian higher education institutions, which also identified students as heavy internet users with variable cybersecurity awareness levels [2,3]. The high proportion of respondents spending more than 6 hours online daily indicates both opportunity and vulnerability: while this group is digitally literate, their constant exposure increases susceptibility to scams, phishing, and other forms of cybercrime.

B. Awareness and Risk Perception

Although most respondents reported knowing "a little" about online risks, few demonstrated deeper knowledge. This echoes national findings that awareness in India is broad but shallow, with many users able to identify risks in theory but lacking in procedural defenses or technical literacy [1,3]. Similarly, while nearly 60% claimed to recognize scams, one-third were uncertain, underscoring the confidence gap between perceived and actual competence in handling cyber threats.

C. Reporting Behavior and Institutional Trust

The study revealed a crucial finding: trust in Goa Police significantly influenced willingness to report cybercrime (χ^2, $p < 0.05$). This aligns with global and Indian criminology research, which emphasizes that reporting is shaped not only by awareness but by confidence in law enforcement to respond effectively [4,8]. The fact that many respondents were unsure about how to report cybercrime (40.7%) further illustrates a critical gap: while national cybercrime portals exist [14], local users remain unclear about the exact procedures. This supports earlier findings that awareness campaigns must move beyond risk information to include step-by-step reporting guidance [17].

D. Exposure to Awareness Campaigns

Nearly half of respondents had never attended a cyber safety campaign or session. This low exposure highlights a weakness in outreach efforts within Goa. Prior studies stress that one-off events have limited long-term effect, and recommend regular, localized, and interactive training programs [1,6]. The current results therefore suggest a need for more visible, sustained, and youth-oriented awareness initiatives.

E. Role of Demographics in Cyber Practices

The chi-square analysis identified that status (student vs. professional) was significantly associated with internet usage patterns, with college students spending the most time online. However, age, area of residence, and knowledge of risks did not show significant associations with reporting knowledge or willingness. This suggests that behavioural outcomes may be shaped less by demographics alone, and more by contextual factors such as institutional trust and exposure to awareness interventions.

F. Implications for Goa

1) Youth as the focus: Given their dominance in internet usage, awareness campaigns in Goa must be tailored to college students and young adults.
2) Building trust in institutions: Strengthening the public image and responsiveness of Goa Police in handling cybercrime could directly increase reporting rates.
3) Bridging the procedural gap: Campaigns must not only raise awareness but also teach the “how-to” of reporting through demonstrations, helplines, and local outreach.
4) Expanding campaign reach: With nearly half of respondents never exposed to cyber safety programs, wider coverage is essential for inclusive digital resilience.

G. Comparison with Literature

The findings of this study are consistent with prior research showing that awareness alone is insufficient if not accompanied by procedural knowledge and institutional trust [1,8,17]. However, this study contributes a Goa-specific perspective by quantitatively demonstrating the role of trust in police as a predictor of reporting behavior, an aspect that has been less explored in state-level Indian contexts.

VI. CONCLUSION

This study investigated the state of cybersecurity awareness in Goa through a combination of descriptive analysis and chi-square statistical testing. The findings highlight both progress and persistent challenges in fostering safe digital practices among Goan internet users.

The descriptive results revealed that the majority of respondents were young college students, spending extensive time online yet possessing only partial knowledge of online risks. While many could recognize scams in principle, a significant portion remained uncertain, reflecting a confidence gap. Importantly, although willingness to report cybercrime was high, knowledge of how to report remained limited, with nearly half of respondents unclear about procedures.

The inferential analysis underscored the decisive role of institutional trust: willingness to report was significantly associated with trust in Goa Police, suggesting that strengthening public confidence in law enforcement is essential for improving reporting rates. Other demographic factors such as age and residence were not significant predictors of reporting knowledge, reinforcing the idea that awareness outcomes depend more on institutional and contextual factors than on demographics alone.

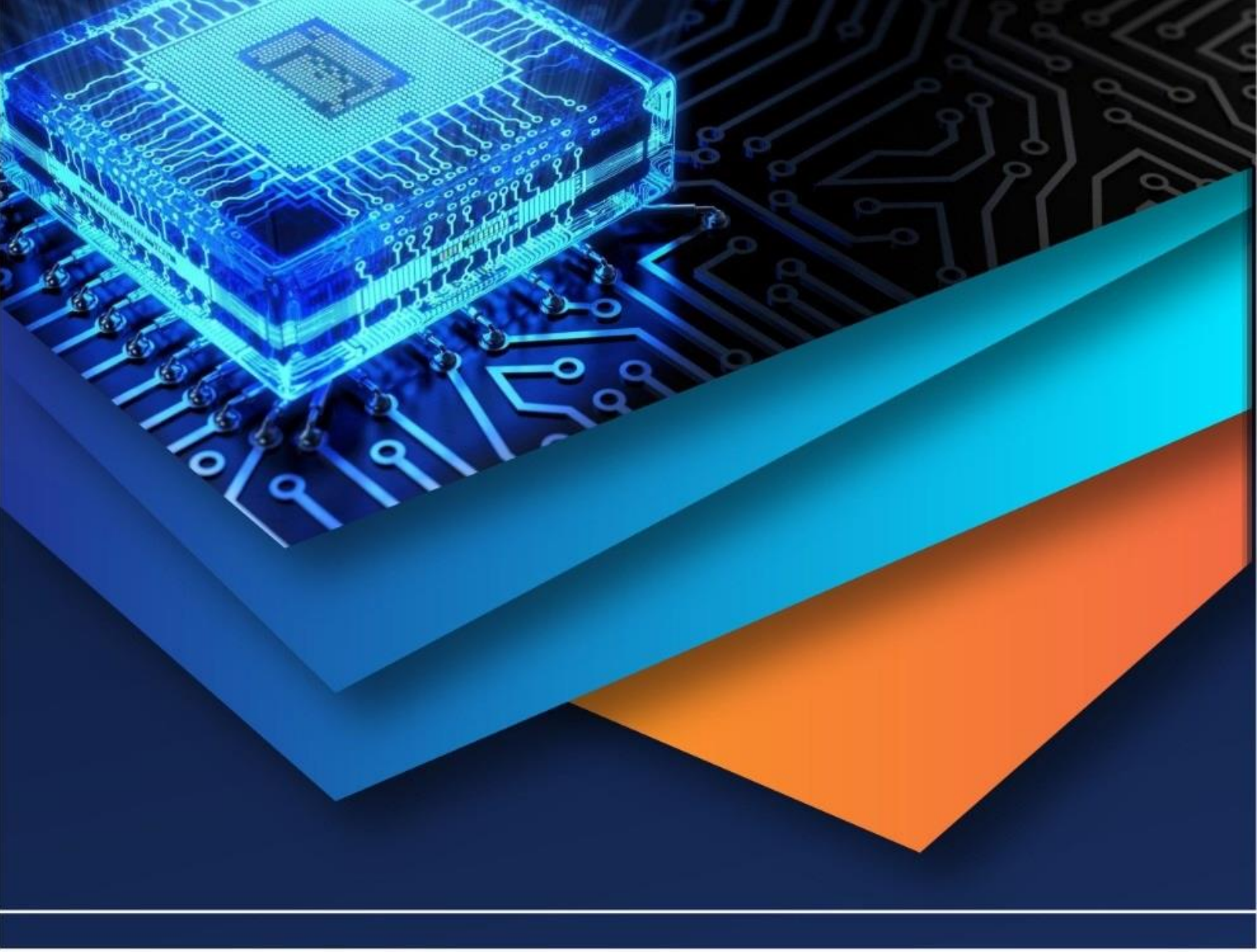
Taken together, the results point to four critical implications:

1) Youth-centric focus: Campaigns must target college students and young adults, who dominate internet usage in Goa.
2) Institutional trust-building: Enhancing responsiveness and visibility of police cybercrime units will encourage victims to report incidents.
3) Bridging the procedural gap: Outreach efforts should emphasize not only risk awareness but also practical steps for reporting through local helplines, cyber cells, and the national cybercrime portal.
4) Expanding outreach: Sustained, interactive, and localized campaigns are needed to increase exposure, particularly for those who have never attended formal sessions.

In conclusion, the study demonstrates that while Goa's internet users—particularly youth—are highly active online, they remain partially prepared to face cyber threats. Strengthening cyber literacy through trust-based, practical, and targeted interventions will be vital for ensuring digital safety and resilience in the state.

REFERENCES

[1] "Cybersecurity awareness and digital literacy in the context of Digital India," *All Research Journal*, Vol. 11, Issue 4 (2025) — analyzing government programs such as Cyber Swachhta Kendra, DISHA, and ISEA and highlighting gaps in awareness efforts All Research Journal.
[2] "Cyber Security Awareness Among Higher Education Students," BHU (2025) — assessing rural UG/PG student awareness using a self-constructed tool BHU.
[3] "A STUDY ON THE AWARENESS OF CYBER SAFETY AND SECURITY AMONG STUDENTS," NCERT (2024) — emphasizing the vulnerability of students to phishing, data breaches, and cyberbullying CIET.
[4] "The Role of Six States Police to Mitigating the Cyber Crime in India," *IJARCCE* (2025) — exploring how state police units manage cybercrime via case studies Peer-reviewed Journal.
[5] "National Cybercrime Reporting Portal," Wikipedia (2025) — overview of the national reporting portal launched in December 2023 by I4C Wikipedia.
[6] "Indian Cyber Crime Coordination Centre (I4C)," Wikipedia (2025) — detailing the government's national initiative to coordinate cybercrime response Wikipedia.
[7] "India's cybersecurity at a glance: 2025 threat report reveals alarming trends," *TechGig* (Dec 2024) — summarizing DSCI-Seqrite report with malware stats and threat trends TechGig.
[8] "Cybersecurity 2025 – India," *Chambers & Partners* (2025) — reviewing India's dual challenge of progress in cybersecurity and vulnerabilities, including policy responses Chambers Practice Guides.
[9] "Cybercrime in India: Legal framework and enforcement challenges," *The Law Communicants* (2025) — discussing public awareness campaigns and digital literacy programs The Law Communicants.
[10] "A comprehensive survey of cybercrimes in India over the last decade," *arXiv* (2025) — documenting cybercrime escalation in India and the need for public awareness and regulation arXiv.
[11] "Online Authentication Habits of Indian Users," *arXiv* (2025) — examining Indian users' use of 2FA, password managers, and password reuse tendencies arXiv.
[12] "ShieldUp!: Inoculating Users Against Online Scams Using A Game Based Intervention," *arXiv* (2025) — an RCT of a gamified intervention improving scam recognition among Indian users arXiv.
[13] "Gujarat trails in reporting cybercrime on portal," *Times of India* (June 2025) — highlighting regional disparities in citizens' ability to report cybercrime online The Times of India.
[14] "Cyber fraud losses see 24% drop in Telangana, thanks to awareness," *Times of India* (2025) — demonstrating the impact of awareness campaigns in reducing losses The Times of India.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY