

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

CYBERCRIME AWARENESS AMONG STUDENTS IN RAMANATHAPURAM: AN EMPIRICAL STUDY OF KNOWLEDGE, DIGITAL SAFETY AND REPORTING AWARENESS

AUTHORED BY - THOWFIK AHAMED

B.S. Abdul Rahman Crescent Institute of Science and Technology

Abstract

The internet economy and digital service industry have opened up social and learning opportunities as well as digital vulnerabilities to cyber-enabled crime. Students are active users of digital services and host and participate in social media and digital commerce, but frequent use of technology does not necessarily mean that they can recognize cybercrime and know how to respond. This study reports on self-assessed levels of cybercrime awareness; knowledge about, and recognition of, information pertaining to official reporting channels among a sample of students and young people using structured google forms with ten key questions uploaded as a dataset containing 52 responses, covering gender, age/education group, location, awareness of the term cybercrime, recognition of examples, awareness of risk from OTPs/PINs/passwords, awareness of risky links, awareness of the National Cyber Crime Reporting Portal and helpline 1930, knowledge of where, when and how to report cybercrime, and self-rated level of awareness in the last three. The study is based on a quantitative, cross-sectional and descriptive research design. Responses are described as frequencies and percentages, whereas interesting associations between grouped awareness ratings and respondent gender, location and age/education category are explored through chi-square test of independence. 42 (80.8%) respondents knew about cybercrime; 45 (86.5%) knew about the risks associated with sharing authentication details; 43 (82.7%) knew about the risks associated with clicking links from unknown sources; 14 (26.9%) knew about both the portal and helpline 1930; 26 (50.0%) knew about neither; only 17 (32.7%) knew about the portal, helpline 1930 and where, when and how to report cybercrime; and a majority (50%) self-rated as having moderate awareness, while 17 (32.7%) self-rated as having low or very low awareness. Self-assessed awareness ratings were not associated with respondent location, gender or age/education group in the chi-square test of independence; however, the lack of understanding

of where, when and how to report, combined with the high number of moderate self-rated respondents, requires interpretation. Moreover, small expected cell sizes and the cross-sectional nature of the data collected requires caution. The data suggest that some people are aware of cybercrime and have some knowledge on how to prevent it without knowing how to report it; a larger, more well-defined sample with objective measures of knowledge is recommended.

Keywords: cybercrime; cybersecurity awareness; digital literacy; students; phishing; online financial fraud; reporting literacy; Tamil Nadu; India.

1. Introduction

Digital technology is now integral to education, communication, entertainment, public services and economic activity. Students rely more and more on their smartphones, social networking sites, messaging applications, online learning platforms and digital banking. While digital technology offers greater access to information and improved inclusion in society, these same technologies also provide a fertile ground for offenders to take advantage of poor security, a lack of knowledge and awareness, misplaced trust and the speed of information sharing. Raising awareness about cybercrime, therefore, forms part of digital literacy.

Cybercrime is a collective word used to refer to different types of crimes committed through the use of computers, digital systems or online services. Some crimes rely on digital or computer systems (cyberdependent crimes) as their main method of attack, for example, unlawful computer access or malicious software. Other crimes are committed through digital means but their occurrence is not dependent on it, for example, spamming, fraud, stalking, hate crimes, identity theft and the hoaxing of victims (Jang-Jaccard and Nepal, 2014; Wall, 2007).

The student population is an appropriate group to look at as they may be at different times of their lives exposed to various risks. For those who are at school, knowledge and guidance on privacy, cyberbullying, unwanted contact and who can help through trusted adults is critical. Universities may want to focus on issues relating to phishing, the security of accounts, fraudulent payment requests, identity theft, privacy settings and official complaints processes. There is an overlap of these populations and risk is driven by individual users rather than just school or university attendance.

A key difference is between awareness and capability. A person may have come across the word cybercrime, but may not be able to distinguish scam messages; a person may know that it's dangerous to give away an OTP, but may still be caught out by an impersonator claiming

to be from a bank or government department; a person may recognise a scam, but may not know how to preserve evidence or how to report it. Capability, knowledge and attitude in information-security research have long been distinguished as separate issues, to be measured independently, rather than under the assumption that one necessarily leads to the other (Kruger & Kearney, 2006; Parsons et al., 2014). In India, the National Cyber Crime Reporting Portal is an online method through which the general public can report cybercrime.

The Indian Cyber Crime Coordination Centre (I4C) at the Ministry of Home Affairs, also supports the national protocol for cyber crime coordination, including the 1930 helpline for reporting financial cyber fraud, and provides information about the portal to report different types of cybercrime, with specific focus on crimes against women and children (Ministry of Home Affairs, 2026). The existence of a portal, however, does not imply that any and all users are aware of the portal or how and when to use it.

Cyber-safety education should, therefore, go beyond simple advice such as 'do not click on unknown links'. It should instruct learners on how to check the senders and the destination and not to pass on confidential authentication information, the importance of strong and unique passwords, enable multi-factor authentication where it is available, update software regularly, save copies of messages and transaction information, and seek help quickly when a suspected incident happens. It should also identify official reporting channels apart from other sources of advice, and avoid the blaming approach of suggesting that the targeted person caused the incident through their actions. Resources provided by CERT-In and in international child-online-protection guidance can support teachers in formulating age-appropriate lessons (CERT-In, n.d.; International Telecommunication Union [ITU], 2020). This study employs a short questionnaire to investigate how these different dimensions feature in the context of 52 respondents. The questionnaire enquires whether respondents have heard of cybercrime and recognise any examples, whether they know about OTP/PIN/password risks and suspicious links, whether they know about the reporting portal and 1930, whether they know where and how to report cybercrime and how they would rank their knowledge on this issue. This framework lends itself to a basic comparison between general awareness, preventive knowledge and reporting competence.

This paper does not suggest that it is a sample of all students in Tamil Nadu. The CSV contains categories of rural and urban domicile and three combined age/education categories; it is not possible to definitively say what the geographical scope or sampling frame of the file alone is. The aim here is somewhat narrower: to describe this one sample, to identify what it suggests there may be data gaps in reported knowledge, and to generate questions for further research.

1.1 Statement of the problem

The problem addressed in this research is that learners could be generally aware of cyber crime without equally sophisticated understanding of particular threats, preventive behaviors and formal channels of reporting crimes. If awareness-raising initiatives find that a respondent has heard of cyber crime, they could wrongly suggest that he is ready to deal with it. This study assesses that knowledge dimension separately from term recognition and risk awareness.

1.2 Purpose and objectives

The overall goal is to measure how aware and how knowledgeable students and young people in the survey are about reporting cybercrime.

To cross tabulate respondents by sex, combined age/education category, and rural or urban residence.

To determine if any of the respondents have heard of the term cybercrime. The purpose is to outline the recognition of the provided examples by the respondents.

To evaluate awareness about the risks involved in sharing your OTPs, pins and passwords. Measurement of the level of awareness around the danger of clicking on unknown links received via messaging, SMS, email and social media.

To assess self-reported awareness of the National Cyber Crime Reporting Portal and helpline 1930.

To investigate how aware people are of where and how they can report cybercrime in India.

To examine relationships among perceived level of awareness and the following variables: demographic and knowledge.

To give suggestions for the cyber-safety education and research.

1.3 Questions to research

Are the respondents familiar with the word cybercrime?

From the given list of cybercrimes, which type do respondents choose?

How aware are respondents of basic digital-security risks?

Are there respondents who knew both National Cyber Crime Reporting Portal and helpline 1930?

How aware of cybercrime do the respondents consider themselves to be?

Are the grouped awareness ratings also differentiated by gender, place of residence or combined age/education category?

"Is self-rated awareness related to reported knowledge of how to report cybercrime?"

2. Literature Review

2.1 Defining cybercrime and its changing forms Cybercrime is not a homogeneous category. According to Wall (2007), internet impacts the scope, scope, and structure of crime, and increases the complexity of traditional crime categories. In their literature review of emerging cyber-threats, Jang-Jaccard and Nepal (2014) state that "the context of cyber threat also changes, along with technology". For awareness survey instruments this indicates that it is useful to cite examples that members can understand, but not be exhaustive. The current multiple-choice question includes hacking, online financial scam, cyberstalking, identity theft and phishing, 'all of the above' and 'don't know'. The categories that it includes are helpful because they signify different types of harm; System intrusion, trickery to obtain financial gain, unwanted surveillance or contact, malicious use of personal information and account deception. The limitation of the single-choice question is that it cannot adequately test people's knowledge as there may be many correct options that can apply at the same time. This influences the interpretation of the results and the subsequent design of the questionnaires.

2.2 Information-security awareness as a multidimensional construct

Kruger and Kearney (2006) created an information-security awareness assessment prototype, claiming that organisations require robust means of monitoring awareness initiatives. Their paper is applicable since it focuses on awareness as something that can be measured, like a tangible item, as opposed to an intangible or assumed concept. Parsons et al. (2014) created and validated the Human Aspects of Information Security Questionnaire (HAIS-Q) exploring connections between knowledge, attitudes and self-reported behaviour. They state that knowledge and attitudes are related to behaviour but are not interchangeable measures. Bulgurcu, Cavusoglu and Benbasat (2010) explore policy compliance through beliefs and awareness; Puhakainen and Siponen (2010) investigate security training as a way to enable compliance. These results justify a pragmatic message for student research: information might not be all. Training should motivate why it is necessary to do something protective and supply it with live, measured opportunity. A simple questionnaire that asks if the reader is aware of a threat is a coarse measure against which to evaluate a policy, but it is not, as such, an impartial test of performance.

McCormac et al. (2017) take personality differences and security awareness into account, supporting the previous argument for careful measurement of awareness. Anderson & Agarwal (2010) investigate security behaviour intentions of home-computer users and highlight the role of people's perceptions and beliefs in their protective behaviour intentions. Dinev & Hart (2006) are about (privacy) decision-making in e-commerce; however, they also show that

decision-making online may be a balancing act of perceived benefits and privacy concerns. This opens the door to understanding the nature of people-being aware of a risk-and yet engaging in risky behaviour.

2.3 Students, young people and online safety the online experiences of young users vary depending on their age, their access to digital technology, family support, the educational environment and the types of platform they engage with.

ITU (2020) offers an online guide for parents and teachers on child online protection. The advice aids a holistic approach where learners, families, teachers, providers and decision makers work together. This information is pertinent to this research as one category of the survey is called '05-18 years - School' so the age range should be verified against the actual participants and the survey's intended age groups. Verma and Kushwaha (2021) conducted research on cybersecurity awareness among secondart school students in Lucknow. The sample consisted of 100 students and a specially designed scale for awareness was used. The present article is relevant as the research has been conducted on the students and has measured the variations on gender and type of school. A study of this kind shows that the awareness level of learners regarding cybercrime has already been established for the Indian context and thus the present paper should not be the first to do so.

In a study of the awareness of cyber crime and cyber security in 178 postgraduate commerce students of the Coimbatore district of Tamil Nadu, Kaleeshwari and Jegadeeshwaran (2024) found that questionnaire data and the descriptive analysis as well as differences tests 'had given a useful tool for identifying the level of the awareness on awareness of cyber crime and cyber security', though they remarked the limitation due to only drawing the conclusion from postgraduate commerce students from the Coimbatore district. This is a particularly significant point in relation to this project: here the survey brings the empirical context to the present project, although given the much smaller and more mixed sample, with particular relevance to knowledge of official procedures, the contribution of this survey is 'exploratory' rather than merely claiming to be the first study of 'cybercrime awareness' within Tamil Nadu.

There is some recent work investigating whether awareness can be increased through education. Vishnoi, Sharma, Lata and Bahuguna (2026) have published a quasi-experimental study of school students in Dehradun, looking at pre-test and post-test knowledge around an awareness session. Their study differs methodologically from this cross-sectional survey, but shows an important difference: describing baseline awareness is a single point measurement, whereas assessing an intervention compares pre-intervention data with post-intervention data.

2.4 Phishing, social engineering and authentication information

Phishing involves messages or websites which masquerade as those from a trusted source, encouraging people to give away credentials, open attachments, click on links or make a payment. This issue of identifying the signs of phishing is described by Furnell (2007). Although the methods employed by the offenders may evolve, the educational task should be there; learners could be taught to question the origin of the message, recognize abnormal urgency, verify the request using a separate channel and never input sensitive information on an unverified website.

Users may regard passwords, PINs, and one-time passwords as just another fact, even though these can be used to access accounts or authorize payments. Questions of awareness about sharing that information therefore raise a real-world security issue. However, a binary answer only captures self-reported knowledge. More robust research could present subjects with plausible messages or require them to make decisions in a simulated scenario, as opposed to simply knowing a rule.

2.5 Reporting literacy and institutional responses

A good way of responding to a cybercrime is, if the incident can be reported in a timely fashion, to save any evidence relevant to the crime, contact the bank or payment service where this is relevant, and use prescribed procedures for complaints. The public reporting portal and helpline 1930 in India, run by the Ministry of Home Affairs, are examples of the public reporting system. Awareness of reporting is thus a relatively good separate topic for survey research.

Report security incidents is a different case where awareness gaps could occur, Parsons et al. (2014, the study about Australian government organisations) suggested. While the issue about the work context is obvious, the suggestion of this article can add evidence to the general argument that to know how to handle incidents is the part of security awareness. Understanding how to report (reporting literacy) involves more than just remember a number: What is the goal of this contact point? What contents should users have ready? Why do they need to save the evidence? What they can and can not do?

2.6 Information and education campaigns

They ask 'what is it about cybersecurity awareness campaigns that makes them ineffective in leading to behaviour change? Bada, Sasse and Nurse (2019) is a good reminder that campaigns should be assessed not only by the amount of exposure or number of materials being circulated. Campaigns may be successful at creating awareness without changing decision making. Action research on training-based compliance (Puhakainen and Siponen, 2010) and NIST's approach to organisational learning and evaluation on cybersecurity and privacy learning programmes (NIST, 2024) are informative.

(CERT-In) CERT-In offers awareness materials and guidelines to foster safe digital practice ITU's child-online-protection guidance also shares age-appropriate learning strategies which could be useful in shaping lessons for students, with a focus on how to safely handle authentication data, recognising suspicious links and dealing with privacy and report incidents.

2.7 Synthesis and research gap

The literature we find indicates that cybercrime awareness is multi-faceted, that self-reporting of knowledge is different from behaviour and that education campaign efforts need to be assessed. Already available Indian data includes awareness levels among school students and also among post-graduate students (including among post-graduate commerce students in Coimbatore). For our study, the defensible gap is thus limited and situated: a modest preliminary description of a mixed bag of questionnaire responses on reporting-channel awareness as well as rudimentary security-risk awareness.

The study compares reported awareness of OTP/PIN/password risks and unknown links with knowledge of the National Cyber Crime Reporting Portal and helpline 1930. It also investigates self-rated awareness vis-à-vis demographic categories and knowledge of reporting procedures. While this design could be useful to select questions for a full study, the (convenience) sample size, sampling frame uncertainty, and questionnaire limitations do not support assumptions of significant novelty or representativeness.

3. Hypotheses

The following hypotheses were generated before exploring the cross-tabulation. Due to a small survey and the number of variables that rely on self-reporting, the tests should be treated as exploratory, not confirmatory.

H1: The combined age/education group is related to self-reported awareness of cybercrime.

H2: There is a link between place of residence (rural/urban) and perceptions of overall cybercrime awareness.

H3: Gender is related to the self-reporting of overall knowledge of cybercrimes.

H4: The majority of participants report having knowledge of basic security risks than the majority report knowing about both official reporting channels.

H5: People who say that they know how and where to report cyber crime are likely to rate their overall awareness as being high or very high.

For H1-H3 the null hypothesis is that the two categorical variables are independent. H4 is simply a comparison of proportions and is not an association test. H5 tests an association

between the binary form of the reporting-knowledge question and the binned awareness rating. The analysis makes no causal claims.

4. Research Gap

The research gap must be described in terms of prior evidence than by simply claiming that there is no research done. Prior research has focused on cyber-crime awareness among secondary-school students and post-graduate commerce students in Tamil Nadu. Prior research has also constructed an instrument to measure information-security awareness and has tested a security awareness training program. This research doesn't substitute these.

Rather, it explores five more specific needs. Firstly, that it provides a description of different levels of awareness among a small sub-sample of the population, including an awareness of cyber-crime, some specific examples, and some details on basic prevention and reporting requirements. Secondly, that it makes a distinction between awareness of the National Cyber Crime Reporting Portal and 1930, and awareness of cyber crime in general. Thirdly, that it compares awareness of different genders, residents and combined gender/education groupings. Fourthly, that it provides a reference point for a larger sample, or to compare against the awareness levels of a wider intervention. Finally, that it reveals limitations of the questionnaire to be amended in the further rounds.

This contribution is exploratory and descriptive. To know whether the specific combination of variables has been previously explored in the selected locality, a systematic review of the literature needs to be carried out. The article should not claim that it is the first study in Tamil Nadu unless this was verified by searching relevant databases.

5. Research Design

5.1 Approach and design

It employs a quantitative, cross-sectional descriptive survey design. It is quantitative as the data responses are groupings which can be analysed numerically as percentages. It is cross-sectional as the data was collected at one point in time without further follow-up. It is descriptive as the aim is primarily to examine what is happening, being an explorative study of awareness, rather than examining why.

5.2 Population and sample

It seems that the questionnaire is addressed to students and youth. The CSV file has 52 records. The unified age/education categories are '05-18 years - School' (16), '18-22 years - UG' (19)

and '23 years & above - PG' (17). The file has also fields for gender and rural /urban. The population, area and recruitment methods of the study sample need to be clarified by the researcher before the final submission. The data file cannot be used to generalize to the population of Tamil Nadu.

5.3 Sampling

Sampling is not specified on the CSV. If the questionnaire link was sent to students who were available (personally or by online groups), then convenience sampling may be an appropriate description of how the sample was recruited- but this will have to be determined from the researcher's notes, not assumed. In a convenience sample, we do not know the probability of any individual being included in the study- generalisation as a prevalence estimate would not be appropriate.

5.4 Instrument

The instrument is a closed Google-Forms questionnaire of ten items. There are three demographic items and seven items measuring cybercrime recognition (two yes/no/don't know, one list of examples for ten different types of cybercrime with single choice options, one category of reporting channels with multiple-choice option, one five-point self-rating from very low to very high). The questionnaire is short and simple, though not a validated cyber security-awareness scale.

5.5 Source of data and time period

The only data source is the CSV export of the table in Google Forms, CSV file uploaded. The timestamps in the table reveal responses from 7 October 2026 to 24 October 2026. There are 52 rows of data with 11 columns, including the timestamp. There are no missing values for the ten substantive questionnaire columns in this export table.

5.6 Ethical consideration

The paper ought to include the actual consent procedure, if participation was voluntary, if the purpose of the research was explained to participants, and the confidentiality involved. Since one of the categories requires school age, confirmation of the ages of actual participants as well as the appropriate institutional ethics protocols should be followed. Parental/guardian consent may also be required. The data in the CSV has no names in the columns displayed, however dates/times and demographic combinations may be unduly identifying in small groups. The raw file should not have extraneous metadata published.

5.7 Scope

This research only measures awareness and self-reporting. It does not, for example, measure actual experience of cybercrime, the number of incidents suffered, security behaviour in

practice, knowledge of legal provisions, the response quality of police or criminal justice authorities, or the effects of cybercrime awareness training. These topics must not be expected to be covered by the measures presented here.

6. Research Methods

6.1 Data preparation

CSV file 2 was imported and checked for number of records, names of columns, number of responses and missing values. There were 52 response records and 11 columns. Frequencies were derived directly from the CSV, not estimated from a PDF version. Summaries of each categorical variable were compiled, providing counts and percentages, the denominator being 52 unless otherwise indicated.

6.2 Descriptive statistics

For gender and age/education category, frequency and percentage distributions were used. For residence and the six awareness questions and for the overall awareness rating, percentages were rounded to one decimal place. Whenever possible, the report states the exact response options that have been used in the dataset to prevent blindly changing the instrument.

6.3 Grouping the overall awareness rating

For a rough screen of potential problems with exploratory cross-tabling the self-rating five levels of the adult self-rating (5 HA, 4 H, 3 N, 2 L, 1 VL) were collapsed to three (High, Moderate, Low) where High = 5 and 4, Moderate = 3, and Low = 2 and 1. This makes the tables more "manageable" but less accurate in table columns and counts and can distort significance tests. The original table has been shown separately. This grouped "result" should be considered a simple exploratory and descriptive tool, not a validated scale.

6.4 Chi-square tests

Pearson's chi-square test of independence. An additional comparison between grouped awareness and a dichotomous version of Q9: I know someone who, with those who answered Yes to Q9 versus those who answered No or Not sure to Q9, was made. Standard significance of .05. ($p < .05$) test results have been interpreted with caution as several expected counts less than five weaken the chi-square approximation. For a number of comparisons, exact or Monte Carlo tests might be more appropriate and increased sample size would better estimate inference.

6.5 Principles of interpretation

This analysis makes a difference between the descriptive results and the statistical inference. The percentage refers to the sample, and does not in and of itself infer any population

prevalence. The p-value is not a measure of the magnitude of an association or its clinical significance, and does not imply causal relations. The cross-sectional design cannot imply a temporal sequence.

6.6 Reproducibility

These are replicable from the uploaded CSV using your favourite spreadsheet or statistical package. When submitting for a journal publication, the author should keep the original analysis file clean, a codebook defining what each variable is, and a version of the questionnaire. If making raw data available, remove timestamps, or other metadata not needed for replication, and the release should be ethically permissible.

7. Results

7.1 Respondent profile

Variable	Category	n	%
Gender	Male	36	69.2%
Gender	Female	16	30.8%
Age/education category	18–22 years – Undergraduate	19	36.5%
Age/education category	23 years and above – Postgraduate	17	32.7%
Age/education category	05–18 years – School	16	30.8%
Residence	Urban	28	53.8%
Residence	Rural	24	46.2%

The sample includes 36 male respondents (69.2%) and 16 female respondents (30.8%). The largest combined age/education group is undergraduates aged 18–22 (19; 36.5%), followed by postgraduates aged 23 and above (17; 32.7%) and the school category (16; 30.8%). Twenty-eight respondents reported urban residence (53.8%) and 24 reported rural residence (46.2%). The distribution provides respondents from both residence categories, but the sample is not necessarily balanced by gender or education.

The combined age/education variable is a limitation. It does not permit the researcher to distinguish whether differences are associated with age, education or both. The school label also includes a broad stated range, '05–18 years', which should be checked for clarity and appropriateness in the final questionnaire.

7.2 Familiarity with the term cybercrime

Response	n	%
Yes	42	80.8%

Not sure	5	9.6%
No	5	9.6%

Forty-two respondents (80.8%) answered 'Yes' to having heard of cybercrime. Five (9.6%) answered 'No' and five (9.6%) were unsure. This indicates that the term was familiar to most respondents in the sample. It does not show that they possess detailed knowledge of cybercrime or can correctly identify every listed offence.

7.3 Recognition of cybercrime examples

Selected response	n	%
All of the above	11	21.2%
Hacking	10	19.2%
Online financial fraud	10	19.2%
Cyberstalking	9	17.3%
Identity theft	5	9.6%
I don't know	5	9.6%
Phishing	2	3.8%

11 respondents (21.2%) responded 'All of the above'. Hacking and online financial fraud were selected by 10 respondents (19.2%), cyberstalking by nine (17.3%), identity theft by five (9.6%), 'I don't know' by five (9.6%), and phishing by two (3.8%). Given this is a single choice question, these frequencies should not be interpreted as a score of knowledge. Several individual options could be selected concurrently as valid examples. For example, a person who selected hacking could also identify phishing as a form of hacking but would have been limited to one answer.

A later version would employ a multiple-select question or else a series of separate true/ false or scenario type items, one for each example. An objective score could then be derived by referencing an answer key. This would allow more defensible comparisons than the single-choice item.

7.4 Awareness of authentication-information risks

Response	n	%
Yes	45	86.5%
Not sure	4	7.7%
No	3	5.8%

A total of 45 respondents (86.5%) said they knew that giving out an OTP, PIN or password can cause cyber fraud. Three (5.8%) said 'No' and four (7.7%) said they didn't know. This was the most affirmative answer given in response to the basic security-awareness questions. But self-reporting knowledge does not mean safe behaviour, as the study found out the participants' actions or whether they had ever shared secrets.

This finding could lead to a concrete lesson such as: "Do not give passwords, PINs and OTPs to callers who claim to be from the bank, a payment service or the government. Make sure that you independently verify odd requests; do not use contact information provided exclusively in a suspicious message."

7.5 Awareness of unknown-link risks

Response	n	%
Yes	43	82.7%
No	6	11.5%
Not sure	3	5.8%

Forty-three (82.7%) respondents said that they were aware of the risk linked to unknown links; six (11.5%) responded 'No' and three (5.8%) were not sure. This is evidence that most respondents are aware of the warning about unknown links. However this does not prove that they know how to recognise a valid link from a malicious one. Some malicious messages claim to be from known organisations.

Other types of simulated exercises for a follow-up could include presenting a range of several messages and asking the participant to identify warning signs, reasoning through these and choosing an appropriate next step to take. This would test applied recognition, not self-report.

7.6 Awareness of the National Cyber Crime Reporting Portal and helpline 1930

Response	n	%
No, neither	26	50.0%
Yes, both	14	26.9%
Only 1930	8	15.4%
Only the portal	4	7.7%

More than a quarter of respondents (26.9%) were aware of both the portal and 1930; 15.4% knew only 1930; 7.7% knew only the portal; and 50.0% knew neither. In total, 73.1% of respondents (38) did not report knowing both channels. This is an important descriptive finding because it reveals an apparent gap in respondents' reporting behaviour: 1930 and the portal warn against 'basic' but not 'specific' forms of cybercrime.

You will be asked a series of questions about having heard of the named channels, not whether they have ever used the channel or if they are able to complete a complaint successfully. The question also joins two mechanisms in one statement. In the next questionnaire you could ask: do you know the portal?, do you know the helpline number? Do you understand what the channels do? Do you know what evidence to keep?

7.7 Knowledge of where and how to report

Response	n	%
Not sure	19	36.5%
Yes	17	32.7%
No	16	30.8%

17 respondents (32.7%) of reporting channel questionnaire affirmed that they knew where and how to report cybercrime in India. 16 (30.8%) responded with a 'No', and 19 (36.5%) responded with a 'Not sure'. Therefore 35 respondents (67.3%) failed to answer affirmatively to the reporting channel question, which may be conflicting but the questions on reporting do not necessarily measure the same concept.

A lesson could demonstrate to pupils the official reporting portal and describe the function of the 1930 reporting line for financial cyber crime. The lesson should make clear that the reporting portal is not a replacement for emergency assistance when there is a direct physical threat to life and that the relevant local authority or bank may need to be contacted.

7.8 Self-rated overall cybercrime awareness

Awareness rating	n	%
Moderate	26	50.0%
Low	13	25.0%
Very High	6	11.5%
Very Low	4	7.7%
High	3	5.8%

Twenty-six respondents (50.0%) deemed their consciousness to be moderate. Thirteen (25.0%) stated that it was low, four (7.7%) very low, three (5.8%) high and six (11.5%) very high. When categories for chosen comparisons are combined, nine respondents (17.3%) rated themselves high or very high, 26 (50.0%) moderate, and 17 (32.7%) low or very low.

Again, the self-rating would indicate that the majority of respondents do not have a high level of awareness, though this is a fairly subjective measurement and, as previously discussed, a

high confidence level, previous knowledge or personal standards may be in-herent in the response. A validated scale or knowledge test would need to be used for stronger conclusions.

7.9 Comparison of grouped awareness by demographic variables

For exploratory analysis, the five response levels were collapsed into High (High/Very High), Moderate, and Low (Low/Very Low). The following table shows counts and within-group percentages.

Variable	Group	High n	High %	Moderate n	Moderate %	Low n	Low %	Total
Age/education	05–18 years – School	3	18.8%	9	56.2%	4	25.0%	16
Age/education	18–22 years – Undergraduate	1	5.3%	9	47.4%	9	47.4%	19
Age/education	23 years and above – Postgraduate	5	29.4%	8	47.1%	4	23.5%	17
Residence	Rural	5	20.8%	11	45.8%	8	33.3%	24
Residence	Urban	4	14.3%	15	53.6%	9	32.1%	28
Gender	Female	2	12.5%	9	56.2%	5	31.2%	16
Gender	Male	7	19.4%	17	47.2%	12	33.3%	36

Postgraduates also more frequently reported they had high or very high knowledge levels (5 of 17; 29.4%) than the other two groups. In this case the school group showed the same pattern, with 3 of 16 (18.8%) reporting high knowledge levels. No such pattern was found with undergraduates (1 of 19; 5.3%), but the small sample size makes conclusions regarding education versus age unclear as they are collapsed together.

Residence had the following distribution: high or very high (20.8% 5 of 24 rural, 14.3% 4 of 28 urban), low or very low (33.3% 8 of 24 rural, 32.1% 9 of 28 urban). Gender: high or very

high (19.4% 7 of 36 male, 12.5% 2 of 16 female). These are just descriptive differences, and should not be taken as representative of a gender or rural-urban effect.

7.10 Exploratory hypothesis tests

Comparison	χ^2	df	p-value	Interpretation
Age/education category vs grouped awareness	5.21	4	0.266	Not statistically significant at .05
Residence vs grouped awareness	0.48	2	0.786	Not statistically significant at .05
Gender vs grouped awareness	0.50	2	0.777	Not statistically significant at .05
Q6 awareness (Yes vs No/Not sure) vs grouped awareness	5.86	2	0.054	Not significant at .05; borderline
Q9 reporting knowledge (Yes vs No/Not sure) vs grouped awareness	16.69	2	0.0002	Statistically significant in exploratory Pearson test

The Pearson chi-square did not show evidence of a statistically significant association between grouped self rated awareness and combined age/education category, $\chi^2(4) = 5.21$, $p=.266$; residence, $\chi^2(2) = 0.48$, $p=.786$; and gender, $\chi^2(2) = 0.50$, $p=.777$. Hence, the test failed to find evidence of an association, but this does not imply that there definitely is not one. Q6 versus grouped awareness = Chi-square(2) = 5.86, $p =.054$ This is not quite below the.05 level, so you should not speak of it as statistically significant. But it is very close, and there are low expected counts, so we should use caution about approximation.

For Q9, those who answered "Yes" were compared to those who answered "No" or "Not sure". Exploratory pearson test result was $\chi^2(2) = 16.69$, $p <.001$. Of those 17 who answered "Yes", 8 rated knowledge high or very high, 7 moderate and 2 low/very low. Of those 35 who answered either "No" or "Not sure", 1 rated high/very high, 19 moderate and 15 low/very low. Self-

reported reporting knowledge and self-rated overall awareness are associated with each other in this sample.

But a number of expected counts in the Q9 comparison are less than five. In that case the p-value must be considered approximate, and the better test is an exact or Monte Carlo test. Also, the association here could be partly a matter of the same people describing both themselves (know and report) or a third factor influencing both.

7.11 Summary of findings

Most respondents had heard of cybercrime (80.8%). The observed reported awareness of OTP/PIN/password risks (86.5%) and unknown-link risks (82.7%) was relatively high. Few (26.9%) said they were aware of the National Cyber Crime Reporting Portal and helpline 1930. Metade dos respondentes afirmou não conhecer nenhum dos dois canais e 67,3% não afirmou saber onde e como realizar a denúncia de crimes cibernéticos. Half rated their overall awareness as low to very low. No strong relationships between the grouped awareness variables and these demographic groups emerged in the exploratory testing. Self-rated and grouping of self-rated knowledge of where and how to report a cybercrime was compared in an exploratory test with the potential for small-cell limitations and self-report bias.

8. Discussion

The findings highlight the difference between being aware of cybercrime and knowing where to report it. Over four in five respondents have heard of cybercrime, and 90 per cent could identify two common security threats, but less than a quarter knew both the portal and helpline 1930. The finding provides evidence in favour of measuring awareness on several different dimensions rather than a general one.

This finding fits with the information-security literature where knowledge, attitudes and behaviour are differentiated. Parsons et al. (2014) call for security awareness to be measured systematically; their HAIS-Q research, for instance, shows how knowledge, attitudes and behaviour relate to each other without conflating them. We are unable to measure behaviour directly in the survey, but the differences between security-risk awareness and reportingchannel awareness show why we need several measures.

The high proportion of yes responses to OTP/PIN/password risks could be because people are aware of common warnings about banking fraud and digital payments. We do not know the reason for this awareness however. The survey did not inquire about how they are aware, have they taken training, or do they know someone that has suffered some form of fraud. A follow

up questionnaire should ask the source of their information: school/college, family, the media, banks, government messaging, personal experience.

The unknown-link outcome must also be more nuanced. A respondent may be aware of the warning but can be duped by convincing imposters. Impersonation attempts, whether via phishing or other social engineering techniques, often profit from familiarity, sight, feel, and emotional state. Phishing, according to Furnell (2007), can better be detected through education based on real examples, although only empirical testing can determine a standard warning.

The key practical takeaway relates to reporting literacy: 50% of the respondents did not claim to know the portal or helpline 1930 and two-third of respondents did not claim to know how to report cybercrime. The government has presented the national portal and 1930 helpline as part of the country's cybercrime reporting mechanism. An awareness programme should highlight the different function of the portal and helpline, what information to retain and why reporting quickly in financial cyber crime cases can be critical. School students should be taught to hold on to messages, screenshots, transaction references and other information without passing on suspicious content to others.

The link between Q9 and self-rated awareness might reflect that the individuals who report that they know about reporting processes also think of themselves as more aware of cybercrime. However, this result should not be over-interpreted. Both measures are self-reported and thought to be conceptually related. An individual who tends to feel more confident of himself in his answers may be more likely to select Yes for both questions. The cross-sectional nature of the data (no dynamics are given) does not prove direction, and more objective questions (and an intervention design) would yield stronger evidence.

No statistically significant relationships were found between grouped awareness and gender, locality or combined age/education group. This does not mean that the groups are equally aware of accounting. The sample is not huge; the categories are unbalanced and the combined age/education category is difficult to interpret. Because of low statistical power, it is possible that there were differences, but they were not statistically significant. A larger study needs to separate age and education, sample from several schools and predetermine a sample size. The one-select format of the question on examples of cybercrime was also a critical design concern. There were only 11 answers of 'All of the above', but this number does not imply that the other answers could not identify more than one crime. The forced choice situation of the single examples prevented a genuinely discriminative response which would involve multiple responses, a 'don't know' option and a pre-designed scoring rule.

These findings should be set next to prior work in Indian samples including Verma and Kushwaha (2021) secondary-school students, and Kaleeshwari and Jegadeeshwaran (2024) postgraduate commerce students in Coimbatore, where it is evident that student cybercrime awareness already exists. The current paper contributes a small exploratory dimension, set of commentary (reporting mechanisms) and comparison (to prevention awareness) which is not directly comparable (samples, instruments, sample sizes varied).

The takeaway is not necessarily to produce more awareness messaging, as awareness efforts should be assessed in the light of learning. Bada et al. (2019) warn that even awareness campaigns don't necessarily change behaviour; NIST (2024) offer a clear methodology for cybersecurity and privacy training programmes. Institutions could survey via a short pre-test, provide a mixed media, interactive presentation, and then follow up with a post-test after an appropriate window of time. The survey could assess the ability to detect phishing, to choose an appropriate response, to identify reportable incidents and to name the correct reporting channels.

For school age, lesson contents must be age-appropriate and include cyberbullying, privacy, unwanted contact, digital footprints and getting help; for university students, in addition, information should include online financial fraud, scams, employment and scholarship scams, identity theft, account recovery, digital payments and evidence preservation. All learners should be informed that victimisation is nothing to be ashamed of and that reporting allows the relevant authorities to investigate and take action; do not give false hopes that reporting will lead to the recovery of funds or a specific legal resolution.

The greater value of the paper is in methods as well as description. It reveals how a simple survey can distinguish several aspects of reported awareness; but it also illustrates the constraints of such a brief measure. Researchers should resist the idea of a self-rated awareness as a unidimensional, objective variable, and disaggregate awareness, confidence, intention and behaviour. The present results can inform the next iteration of the questionnaire and a larger sample study (caveats noted).

9. Recommendations

9.1 Educational organisations' recommendations

Incorporate bite-sized, ongoing sessions on cyber-safety instead of a single annual presentation. Make sure that students are aware of phishing, impersonation, dodgy links, scam scholarships and fake payment requests. DO NOT share OTPs, PINs and passwords with callers or message senders, even if they say they are calling from a trusted organisation.

Show how to verify organisations' websites and contact them using contact details obtained independently. NCCRP and helpline 1930 in cyber-fraud reporting in the financial sector.

Teach evidence preservation: keep the best messages, screenshots, references, dates and contact details, the evidence must not be changed.

Offer age-specific advice on cyberbullying, privacy, unwanted contact and how to get help from a trusted adult. Assess each awareness session with pre-test and post-test questions, not just by the fact of its being attended.

9.2 Suggestions for future investigators

Sample you can increase with a described population, geographical locations, sampling method, and recruitment procedure. Record age and educational level as individual variables. Revise the question based on a good cybercrime-example to permit several responses or develop separate scored questions.

Use scenario-based questions to evaluate recognition and safe decision-making.

Identify the success of previously held cyber-safety training and sources.

Differentiate between awareness of the portal and awareness of 1930 and awareness of how to fill a report.

Apply suitable exact or Monte Carlo tests if the expected cell count is low.

Design a pre/post test/longitudinal study to measure effectiveness/retention of the cyber-safety education.

Documented voluntary agreement with safeguards for privacy and any special considerations required for participants under the age of 18. A priors and analysis plans should be pre-registered if possible and both significant and non-significant findings should be reported.

10. Study Limitations

First, the small sample size ($n=52$) allows for descriptive analysis, but not precision and the ability to compare subgroups. Second, the CSV does not specify the sampling frame (university students: where? How recruited?) or describe the geographical coverage, so the sample cannot be assumed to be representative of students in Tamil Nadu. Third, the report summarizes self-report data that is subject to recall, interpretation and social-desirability bias. Fourth, it is not clear that the questionnaire is a validated scale and there is no provision for an objective measure of knowledge.

Fifth, the question about the type of cybercrime is listed as a single choice item even though multiple answers can be true, so response interpretation is restricted. Sixth, age and education are combined into a single variable, so their individual relationships with awareness cannot be

investigated. Seventh, the cross-sectional design does not allow for inference of causality or comparison of changes over time. Eighth, the study does not measure whether the individual was a victim of cybercrime, whether they engaged in real-life security behaviour, whether they received previous training, or whether they used a reporting mechanism. Ninth, some cell sizes in the chi-square tables are small, so the assumptions of using asymptotic p-values are not met. Tenth, the study has not tested an educational programme, so advice on training is based on the apparent gaps in this sample and past literature rather than direct measurements of programme efficacy.

Presenting these limitations should be straightforward. They do not diminish the descriptive work, but do limit what can be said and flag where further work can be done.

11. Conclusion

This study looked at the self-reported awareness of cybercrime among 52 respondents using a structured Google Forms questionnaire. It looked at general knowledge of cybercrime, knowledge of specific examples, awareness of OTP/PIN/password security, awareness of suspicious links, awareness of the National Cyber Crime Reporting Portal and helpline 1930, awareness of how to report cybercrime, and overall self-reported awareness. 84.6% of all respondents had heard of cybercrime and the reported awareness of being aware of the risks of sharing authentication information and clicking unknown links was 86.5% and 82.7% respectively. The reported awareness of both official channels to report a cybercrime was 26.9% with 50.0% not knowing any. 32.7% knew where and how to report cybercrime, and 50.0% rated themselves as moderately aware of cybercrime prevention messages. These initial results suggest that while people may be aware of prevention messages, they may not know how to take further action in response to cybercrime.

No significant relationships between the grouped awareness and demographics, grouped awareness categories by gender, residence and grouped self-rated awareness categories by combined age/education were found with the exploratory demographic comparisons. There was a statistically significant relationship between reporting knowledge and grouped self-rated awareness with a regular (Pearson) chi-square calculation, but the expected counts are too small and the self-reported, cross-sectional nature of the data means that it should be validated using an exact or Monte Carlo procedure and be interpreted as an association and not a cause and effect relationship.

The findings endorse effective cyber-safety education that encompasses threat awareness and reporting literacy. Schoolchildren need guidance on safeguarding private information,

evaluating dubious messages, keeping potential evidence and recognising reporting mechanisms. Schools need to test the effectiveness of these courses, through knowledge questions and follow-up evaluations.

These results are exploratory and cannot be assumed to be representative of all students in Tamil Nadu. A larger study with a more transparent sampling strategy, a more carefully designed questionnaire and discrete items on knowledge, attitudes and behaviour would yield more robust evidence. The main message, for me, is that cybercrime literacy is more like a constellation than a binary condition.

References

1. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643.
2. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. <https://arxiv.org/abs/1901.02672>
3. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.
4. Computer Emergency Response Team–India. (n.d.). Awareness booklets. <https://www.cert-in.org.in/AwarenessBooklets.jsp>
5. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80.
6. Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud & Security*, 2007(3), 10–15.
7. Government of India. (2000). Information Technology Act, 2000. India Code. <https://www.indiacode.nic.in/>
8. International Telecommunication Union. (2020). Guidelines for parents and educators on child online protection. ITU. <https://www.itu.int/pub/S-GEN-COP.EDUC-2020>
9. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993. <https://doi.org/10.1016/j.jcss.2014.02.005>
10. Kaleeshwari, S., & Jegadeeshwaran, M. (2024). Quantitative assessment of the cybersecurity and cybercrime awareness among postgraduate commerce students in the

- Coimbatore District, India. *Asian Journal of Probability and Statistics*, 26(9), 185–197.
<https://doi.org/10.9734/ajpas/2024/v26i9653>
11. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296.
<https://doi.org/10.1016/j.cose.2006.02.008>
 12. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151–156.
 13. National Institute of Standards and Technology. (2024). Building a cybersecurity and privacy learning program (Special Publication 800-50, Revision 1). U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/50/r1/final>
 14. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176.
<https://doi.org/10.1016/j.cose.2013.12.003>
 15. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, 22(4), 334–345.
<https://doi.org/10.1108/IMCS-10-2013-0078>
 16. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778.
 17. Verma, M. K., & Kushwaha, S. S. (2021). Awareness towards cybercrime among secondary school students: The role of gender and school management. *Safer Communities*, 20(3), 150–158. <https://doi.org/10.1108/SC-07-2020-0026>
 18. Vishnoi, R., Sharma, S., Lata, K., & Bahuguna, D. (2026). Understanding cyber crime awareness levels among school students: A quasi-experimental study in Dehradun. *Adolescência e Saúde*, 21(9s), 1900–1907. <https://doi.org/10.67440/ahj.vi.2715>
 19. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
 20. Ministry of Home Affairs, Government of India. (2026, July 22). National cybercrime response mechanism. Press Information Bureau.