

Cybersecurity Awareness among College and University Students

Saifurrahman Tanveer Alam Shaikh¹, Aarti Sanjay Gawai²

¹ Student, Department of Information Technology and Computer Science, D.G Ruparel College of Arts, Science and Commerce, Mumbai, Maharashtra, India

atalver005@gmail.com

² Assistant Professor, Department of Information Technology and Computer Science, D.G. Ruparel College of Arts, Science and Commerce, Mumbai, Maharashtra, India

aartigawai1611@gmail.com

Abstract

This proposed study will assess cybersecurity awareness and self-reported safe online practices among students at D.G Ruparel College. Its rationale is that student cybersecurity knowledge, awareness, and practices are related but distinct dimensions, and that survey responses about behavior should not be treated as direct observation. The study will use a quantitative, cross-sectional questionnaire to measure knowledge of common online threats, awareness and perceptions, protective practices, and prior cybersecurity training. It will examine associations between awareness and reported practices and explore differences by academic program, year of study, and training history. Data will be summarized using descriptive statistics and analyzed with suitable group comparisons, correlation, and—if the sample size and assumptions permit—multivariable regression. Participation will be voluntary and subject to institutional ethics approval; no passwords or account credentials will be collected. The study is expected to produce an institution-specific profile of student awareness and reported practices and identify topics for targeted cybersecurity education. Since the proposed design is cross-sectional and relies primarily on self-report, its findings will describe associations and reported behavior rather than establish causality or verify actual behavior.

and training, and suggests these constructs can be considered in a student-awareness study.

This proposed study will assess cybersecurity awareness and self-reported safe online practices among students at D.G Ruparel College. It will examine whether awareness and reported practices vary by selected academic and training-related characteristics. The findings are intended to inform locally relevant student cybersecurity education; they will not be assumed in advance.

Common Cybersecurity Threats Relevant to Students



Fig.1. Common Cybersecurity Threats

Introduction

College students use digital platforms for academic, social, and personal activities, making cybersecurity awareness and everyday protective practices relevant concerns for higher education. However, awareness and knowledge do not necessarily translate into consistent security behavior. A survey of university students examined cyber-hygiene knowledge, awareness, and practices as related dimensions, reporting that students' knowledge and awareness did not consistently correspond to their reported behavior.

Student-focused research has assessed a range of areas, including password practices, phishing awareness, security tools, and training. A validated cybersecurity-awareness measure for university students used exploratory and confirmatory factor analyses and examined behavior across different student demographic groups. Other work has examined relationships among knowledge, attitude, behavior,

Literature Review

Knowledge, awareness, and cyber-hygiene practices

Cybersecurity awareness should be considered alongside actual or reported practices rather than treated as a single knowledge score. A survey study of university students used a 30-question cyber-hygiene instrument to assess knowledge, awareness, and behavioral practices. It reported that these outcomes were related, while also describing low knowledge and unsatisfactory awareness despite acceptable reported behavior. This supports measuring knowledge, awareness, and reported practices as separate domains in the proposed study

Measuring student cybersecurity awareness

Measurement design is central to a student-awareness project. Bognár and Bottyán developed and validated a personal cybersecurity-awareness survey for university students, using exploratory and confirmatory factor analyses and a structural equation model to examine dimensions of student cybersecurity behavior. Their work also compared behavior across student

demographic groups. The proposed questionnaire should therefore be piloted, use clearly defined domains, and avoid treating an unvalidated collection of questions as a single reliable score.

Training and individual factors

Fattah, Wagimin, and Nurlia examined knowledge, attitude, behavior, and training in relation to cybersecurity awareness among university students. Their study used survey data from 64 students and reported positive relationships between those factors and awareness. This provides a rationale for collecting information about prior cybersecurity training and exploring its association with awareness and practices in the proposed setting. Because the study is limited to a sample and context different from the proposed institution, the relationship should be tested locally rather than presumed.

Differences across student groups

A questionnaire study of 136 Saudi university students assessed awareness and considered gender, location, and study department. The study reported higher awareness among students in computing and information-technology departments and differences associated with location, while reporting no significant gender difference in awareness. Such results illustrate why academic program and other locally relevant characteristics may be examined; they do not establish that the same patterns will occur at D.G Ruparel College.

Phishing and the limits of self-report

Phishing provides a concrete domain for assessing knowledge and protective practices. A study applying an adapted Health Belief Model to university students found that perceived severity, perceived importance, self-efficacy, and cues to action were statistically significant predictors of self-reported security behavior. The study also cautioned that self-reported behavior reflects perceived or intended actions rather than directly observed actions. Accordingly, the proposed project will describe questionnaire answers as self-reported practices and will not claim to have directly measured actual behavior.

Research Gap

The reviewed studies provide examples of student surveys, awareness measures, and analyses of training or student characteristics, but the evidence summarized here comes from different institutional and national settings. For the proposed project, the key practical gap is the absence of a locally measured profile for D.G Ruparel College: the institution-specific level of students' cybersecurity knowledge and awareness, their self-reported protective practices, and the extent to which these outcomes are associated with prior training and academic characteristics. Existing findings cannot be assumed to represent this institution because the cited studies sampled different student populations and settings.

This is a proposed local research gap, not a claim that no other research exists. Before final submission, conduct a fuller literature search for studies from your country, institution, or comparable colleges and refine the gap accordingly.

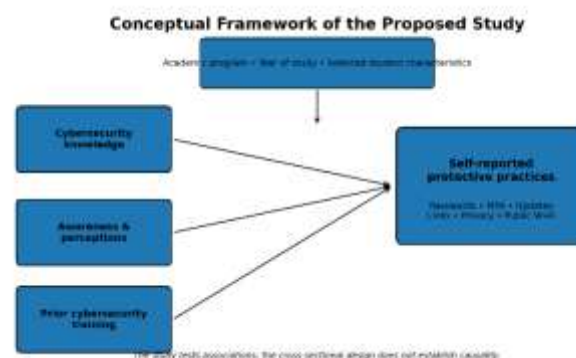


Fig.2. Conceptual Framework

Objectives

General objective

To assess cybersecurity awareness and self-reported safe online practices among students at D.G Ruparel College, and examine factors associated with these outcomes.

Specific objectives

1. To measure students' cybersecurity knowledge and awareness of common online threats, including phishing, password compromise, unsafe links, malware, and privacy risks.
2. To describe students' self-reported protective online-security practices, including password management, multi-factor authentication, software updates, suspicious-message handling, and public Wi-Fi use.
3. To examine the relationship between cybersecurity knowledge/awareness and self-reported protective practices.
4. To assess whether awareness and reported practices differ by academic program, year of study, and prior cybersecurity training.
5. To examine the association between prior cybersecurity training and students' awareness and reported protective practices while accounting for selected student characteristics.
6. To recommend practical student cybersecurity-awareness activities based on the study findings.

Research Methodology

Research design

A quantitative, cross-sectional questionnaire survey is proposed. It can describe awareness and reported practices at one point in time and test associations among measured variables. Because the data are cross-sectional, the study cannot

establish that training or awareness caused any reported behavior.

Proposed Research Methodology Flow



Ethics throughout: informed consent • voluntary participation • no personal identifiers • secure data

Cross-sectional questionnaire results describe associations and self-reported practices

Fig.3. Research Methodology Flow

Study setting and population

The study will take place at D.G Ruparel College, Mumbai, Maharashtra, India. The target population will be students currently enrolled in MSc Information Technology (MSc IT). Define the eligible age range and whether undergraduate, postgraduate, or both groups are included. If participants under 18 may be recruited, consult the institutional ethics committee about additional consent requirements.

Sampling and sample size

Where an approved student list is available, stratified sampling by academic program and year of study may improve representation across those groups. If a full sampling frame is unavailable, a documented convenience or volunteer sampling approach may be used, with selection bias acknowledged. Determine the sample size after confirming the eligible population, expected response rate, and planned statistical analyses; the final calculation should be reported in the submitted proposal.

Data-collection instrument

Use a structured questionnaire with the following domains:

- Participant characteristics:** age group, academic program, year of study, frequency of internet use, and prior cybersecurity training.
- Knowledge:** objective questions about phishing, password strength and reuse, multi-factor authentication, software updates, suspicious links, malware, and public networks. Include an option for respondents to indicate that they are unsure of the correct answer.
- Awareness and perceptions:** perceived importance and severity of common threats, confidence in responding to suspicious messages, and awareness of institutional support or reporting channels.
- Self-reported practices:** password management, use of multi-factor authentication, software updates, link verification, privacy settings, and public Wi-Fi practices.

Questionnaire Domains



Fig.4. Questionnaire Domains

Where possible, adapt a validated student-focused scale rather than creating all items from scratch. Existing student work has validated a cybersecurity-awareness survey using factor-analysis methods, while other work has assessed cyber-hygiene through a structured questionnaire. Any adaptation should be documented, checked for relevance to the local context, and piloted before the main survey.

Pilot study and data collection

Pilot the questionnaire with a small group resembling the target population, if feasible. Check clarity, completion time, missing responses, and whether the response options are suitable. Improve the wording of unclear questions before proceeding with the main data collection. Recruit participants using an approved procedure, provide an information sheet, obtain informed consent, and collect responses through a secure online or paper-based method.

Data analysis

Use descriptive statistics to summarize participants and item-level responses. Calculate separate domain scores for knowledge, awareness/perceptions, and protective practices using a pre-specified scoring approach. Assess internal consistency where appropriate. Use suitable group-comparison tests for differences across training history, academic program, or year of study. Use correlation and, if the sample size and assumptions permit, multivariable regression to examine associations between awareness and reported practices while adjusting for selected characteristics. Report effect estimates and uncertainty as well as statistical significance.

Interpret practice outcomes as self-reported rather than directly observed behavior, consistent with published work noting this limitation of student self-report.

Ethical considerations

Obtain approval from the relevant institutional ethics committee and any required permissions before recruitment. Participation should be voluntary, based on informed consent, and unrelated to grades or access to services. The questionnaire will not require participants to share passwords or login credentials. Minimize identifying information, store responses securely, restrict access to the data, and report findings in aggregate. Any simulated phishing or behavioral tasks would require explicit ethics approval and an appropriate risk-minimization and debriefing plan; it is not necessary for the proposed questionnaire study.

Scope and Limitations

The proposed study is limited to students at D.G Ruparel College and will examine cybersecurity knowledge, awareness, selected protective practices, and associated student or training characteristics during one data-collection period. It will not measure all dimensions of cybersecurity or establish causal effects of awareness training.

A single-institution sample may not represent students at other colleges or in other countries. If volunteer or convenience sampling is used, students who choose to participate may differ from those who do not. Questionnaire responses may be affected by recall error or social-desirability bias and will not by themselves verify actual behavior. Cross-sectional data can identify associations but cannot show whether awareness leads to safer practices or whether other factors explain the association. These limitations should guide the interpretation of results.

Conclusion

This proposal presents a feasible MSc study of cybersecurity awareness among college students, with a focus on measuring knowledge, awareness, and self-reported online-security practices as distinct but related domains. Prior university-student research supports including questionnaire measurement, training history, academic characteristics, and phishing-related content, while also underscoring that self-reported practices are not the same as observed behavior. By collecting institution-specific data at D.G Ruparel College, the study can identify local educational priorities without assuming in advance what the results will show.

References

- Aljohani, W. M., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). *Cybersecurity Awareness Level: The Case of Saudi Arabia University Students*.
- Alqahtani, S., & Nanda, P. (2024). *Enhancing Phishing Resilience in Academia: The Mediating Role of Anti-Phishing Tools on Student Awareness and Behavior*.
- Alsiddig, M., Altigani Badwi, A. A., & Idriss, O. A. (2020). *Cyber security awareness among students and faculty members in a Sudanese college*. <https://doi.org/10.30564/ese.v2i2.2477>
- Baraković, S., & Barakovic, J. (2022). *Cyber hygiene knowledge, awareness, and behavioral practices of university students*.
- Bognár, L., & Bottyán, L. (2024). *Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students*.
- Fattah, A., Wagimin, W., & Nurlia, N. (2023). *Enhancing Cybersecurity Awareness among University Students: A*

Study on the Relationship between Knowledge, Attitude, Behavior, and Training.

Garba, A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). *A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach*.

Gwenhure, A. K. (2025). *University students' security behavior against email phishing attacks: insights from the health belief model*.

Irfan, H., Jamshaid, K., Akhter, R., & Shakeel, R. (2020). *Cybersecurity and Multidisciplinary Students: A Survey*.

Khaled, M., Saleh, M., Nasser, Y., Salah, F., Hani, A., Ahmed, M., Abdullah, A., Adell, A., Abdullah, M. F., & Alsakkaf, N. (2025). *A Study on the Cyber Attack Awareness Among Students: University of Science and Technology Case Study*.

Rounds, M., Pendegraft, R., Pendegraft, N., & Stone, R. (2008). *Student Survey on Computer Security Awareness And Responsiveness*.

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). *A survey on internet usage and cybersecurity awareness in students*.

Verma, V., & Pawar, J. (2024). *Assessment Of Students Cybersecurity Awareness And Strategies To Safeguard Against Cyber Threats*.

Yildirim, M., & Erendor, M. (2024). *A Comparative Analysis of Cyber Security Behaviours of University Students*.

Zhang, C., & Prichard, J. (2009). *An Empirical Study of Cyber Security Perceptions, Awareness and Practice*.

BIOGRAPHIES



Mr. Saifurrahman Tanveer Alam Shaikh

M. Sc. Information Technology
Student, Dept. of IT/CS,
D. G. Ruparel College



Ms. Aarti Sanjay Gawai
M.Sc. Information Technology
Asst. Prof., Dept. of IT/CS,
D. G. Ruparel College