Factors affecting cyber security awareness among college going students in Delhi NCR

Ms. Vanshika Batra[1], Dr. Radhika Thapar[2]

DOI: 10.5958/2347-7202.2025.00007.6

ABSTRACT

This study examines the factors that influence cyber security awareness among university students in the Delhi NCR area. As more people depend on digital tools, it's important to understand how much students know about cyber security. The research uses a quantitative method and gathers data from more than 120 students. It uses Exploratory Factor Analysis (EFA) in SPSS to analyze the information. The main aim is to assess students' level of awareness and to explore how various factors affect it, such as their academic background, whether they have received cyber security education, and how frequently they use digital technologies. The study also makes use of statistical methods like Chi-square tests, t-tests, and ANOVA to identify relationships between these factors. This helps compare awareness levels across different groups, such as male and female students, and evaluate how cyber security education impacts awareness. The expected results should provide valuable insights into what influences cyber security awareness. This information can help develop more effective education programs and policies to improve students' knowledge and preparedness in a digital environment. The research also aims to support decision-makers in identifying necessary steps to enhance awareness and readiness.

KEYWORDS

Awareness, Cyber Security, Factors, Exposure, Determinants, Strategies, Stakeholders, Methodology, Preparedness

INTRODUCTION

The rapid expansion of the internet and digital devices has altered the way people communicate with one another and acquire information. Though the digital world has numerous positives, there are also large cyber security risks that come with it. Students in college are particularly at risk of issues such as hacking, identity stealing, and phishing due to the use of many digital devices. Areas like Delhi NCR, with numerous colleges and school institutions and many young people with technical nativities, see even greater levels of risk. The large concern is that college students lack much awareness concerning cyber security because they will be entering the working world and assuming significant responsibilities in the near future. Studies indicate that numerous students lack information concerning cyber security, and this causes them to engage in dangerous behaviors such as the use of weak passwords or posting personal information online. Though there exist some courses that educate the students concerning cyber security, they often don't go far enough and don't quite engage the students. Indicators influencing the level of information that the students have concerning cyber security include the family's level of income. Students from families with more income enjoy better devices and better study manuals on cyber security. However, in families with limited privileges, there is usually the difficulty in getting the information required. The level of use of technology also significantly contributes to the level of comprehension concerning cyber security.

LITERATURE REVIEW

The paper examines the main factors that influence how university college students focus on cyber safety, including their behavior, past experiences, attitudes, stage of learning, environmental barriers. While the study doesn't specifically look at students in Delhi NCR, the results suggest that including cyber security

[1,2]*Rukmini Devi Institute of Advanced Studies, Affiliated to GGSIPU, Delhi*
Email: [1] *vanshikaba.mba2024mb@rdias.ac.in,*[2]radhika.thapar@rdias.ac.in

This journal is cited as: JIMS 8i-Int'l J. of Inf. Comm. & Computing Technology (IJICCT)

education in school curricula and creating personalized awareness programs can help improve students' understanding of online safety The knowledge-attitude-behavior (KAB) model is shown to be the most effective approach for evaluating these elements in the broader context of cyber security awareness in e-learning. One important point is that students in Delhi NCR have limited knowledge about different types of cybercrimes and cyber-attacks. **Ahmad, A., & Sharma, M. (2022).** The paper does not focus specifically on the factors affecting cyber security awareness among university students in Delhi NCR. However, it stresses the importance of understanding, mindset, and behavior related to cyber safety for enhancing awareness among university students globally. The systematic review shows that most studies focus on countries like the United States, Saudi Arabia, and Nigeria, indicating a gap in research on specific regions like Delhi NCR. Future studies could explore these factors in more depth. Additionally, the general level of awareness and use of information and communication technology (ICT) among university students plays a crucial role in shaping their understanding of cyber security. **Singh, P., & Bhatia, K. (2023).** The paper is a systematic review of literature focusing on the knowledge that university students have about cyber security. The study selected 25 articles published between 2018 and 2023, with most using a descriptive-quantitative approach, involving undergraduate and postgraduate university students, organizations, faculty members, students at higher institutes, and full-time staff as participants. Demographic factors such as age and gender significantly affect the levels of cyber security awareness among university students. **Joshi, S., & Kumar, A. (2019).** The paper discusses the increasing integration of our online world into modern society, especially highlighting the rapid growth of internet users in recent years, with a focus on the younger demographic, including college and university students, who are becoming more active online. It emphasizes the vulnerability of young internet users to cybercrime, noting that many are unaware of ethical and safe digital practices, which is due to insufficient programs aimed at promoting cyber security in developing countries like India. **Mehta, P., & Rao, T. (2020). T**he paper does not specifically address the factors affecting cyber security awareness among university students in Delhi NCR. It focuses on assessing cyber security awareness among students, examining password security, browser security, and social media activities. The literature review highlights similar studies but does not include research specific to Delhi NCR. **Sharma, A., & Gupta, N. (2021).** The paper does not mainly focus on factors affecting cyber security awareness among college students in Delhi NCR. However, it highlights that socio-demographics, perceptions, previous cyber security breaches, IT usage, and knowledge significantly impact cyber security behavior among students. The study emphasizes that despite being digital natives, students lack sufficient knowledge and awareness of cyber threats, indicating the need for educational institutions to enhance cyber security training and awareness programs. **Verma, K. (2022).** The paper does not mainly focus on a literature review of factors affecting cyber security awareness among university students in Delhi NCR. However, it

highlights the general vulnerability of university students to cyber threats due to their active use of the internet and engagement in various online activities. It emphasizes the importance of understanding threats like phishing, malware, and ransom ware, as well as their knowledge of preventive measures to enhance cyber security awareness and protect against cyber-attacks. **Kumar, V. (2019).** The paper identifies several factors affecting cyber safety awareness among students, including a lack of knowledge about cyber threats, insufficient educational resources, and the prevalence of risky online behaviors. It emphasizes the need for tailored educational programs to address these challenges and enhance awareness. **Gupta, S., & Prasad, R. (2022).** The study addresses the urgent issue of cyber security awareness among students, highlighting the need for a comprehensive understanding of the behavioral factors that influence their cyber safety practices in the digital age of higher education. It employs a strong framework that includes exploratory and confirmatory factor analyses to develop and validate a survey aimed at capturing the complex dimensions of students' cyber safety. **Saini, L & Yadav, R. (2021).** The paper discusses the challenges faced by students, described as digital natives, who are increasingly vulnerable to cyber-attacks such as identity theft, phishing, and social engineering due to unsafe computing practices. **Tiwari, P. (2020).** The literature review highlights the widespread growth in internet use among children, especially college and university students, over the last two decades, emphasizing their increasing presence in our online world and the corresponding rise in cybercrime targeting this demographic. It discusses the lack of knowledge regarding ethical and safe digital practices among young internet users, attributing this gap to insufficient implementation of cyber security programs in educational institutions, particularly in developing countries like India. **Chauhan, R. & Malik, V. (2023).** The paper identifies several factors affecting cyber security awareness among users, including knowledge, attitude, and behavior. It emphasizes the importance of regular training programs, tailored curricula, and consideration of demographic factors such as language and gender. For students in Delhi NCR, incorporating cyber security training into the educational curriculum can enhance awareness. Additionally, technology users' computers. **Gupta, A., & Singh, P. (2022).** The paper provides a systematic literature review focused on evaluating e-learning cyber security awareness among university students, highlighting the significant risks related to the rapid adoption of e- learning systems, including threats to confidentiality, integrity. **Gupta, R., & Chauhan, P. (2021).**

METHODOLOGY

1. Research Objective

The main aim of this research is to assess the level of cyber security awareness among students studying in colleges located in the Delhi NCR region.

It also aims to explore how factors such as age, gender, field of study, and internet usage influence students' understanding and behavior when it comes to cyber security.

2. Research Design

This study used a descriptive and exploratory research approach.

The **descriptive part** looked at the current level of cyber security awareness among students, while the exploratory part aimed to find out if there are connections between awareness levels and certain demographic and behavioral factors.

A **cross-sectional design** was used to gather information at one point in time, allowing for an evaluation of how academic and demographic factors influence awareness and practices.

3. Population and Sampling

The study focused on undergraduate students from colleges in the **Delhi NCR area**, including cities like Delhi, Noida, Gurugram, Ghaziabad, and Faridabad.

The participants came from different academic **backgrounds, genders, and levels of digital experience.**

Initially, **120 participants** were planned, but after checking the data for quality and accuracy, **110 valid responses** were used for analysis.

Participants were selected using a stratified random sampling method to ensure a balanced representation across different fields of study, years of study, and types of colleges (public and private). Additionally, convenience sampling was used to make the process more efficient by selecting individuals who were easily accessible and willing to take part.

4. Data Collection Instrument

A **standardized questionnaire** was developed to measure cyber security awareness.

This tool used a **Likert scale** to rate participants' awareness, understanding, and behavior regarding cyber security. The questions were based on **the Technology Acceptance Model (TAM)**, which helps assess how useful and easy it is to use cyber security tools and practices.

The survey aimed to collect quantitative data on cyber security knowledge, behavior, and attitudes, as well as some open-ended questions to gather qualitative insights.

5. Data Collection Procedure

The data was collected over a **one-week period**. All responses were gathered electronically and then checked for completeness and consistency before further analysis. Ethical standards were followed by ensuring anonymity and getting voluntary consent from participants.

6. Data Analysis Tools and Techniques

Quantitative data was analyzed using **SPSS,** while **NVivo** was used for qualitative analysis and visualization.

7. Factor Analysis:

The data was tested for suitability using the Kaiser-Meyer-Olkin (KMO) test, which gave a value of 0.681, indicating that the sample was adequate for factor analysis.

Bartlett's Test of Sphericity was also significant ($p < 0.05$; $p = 0.000$), confirming that there were strong relationships between the variables.

A) A **Varimax (orthogonal) rotation** was applied to simplify the factor loadings and make the results easier to understand.

Three main factors were identified:

Knowledge of Cyber Security

Cyber Security Practices and Habits

Perceptions of Cyber Threats

B) Reliability Testing:

Cronbach's Alpha was used to check the internal consistency of the scale, ensuring that the questions within each factor were reliable and consistent.

C) Qualitative Analysis:

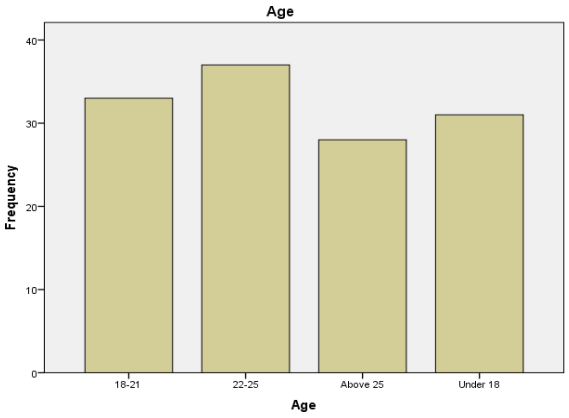
NVivo was used to generate word clouds highlighting the most common terms and themes shared by respondents, offering a visual representation of their perceptions and experiences related to cyber security.

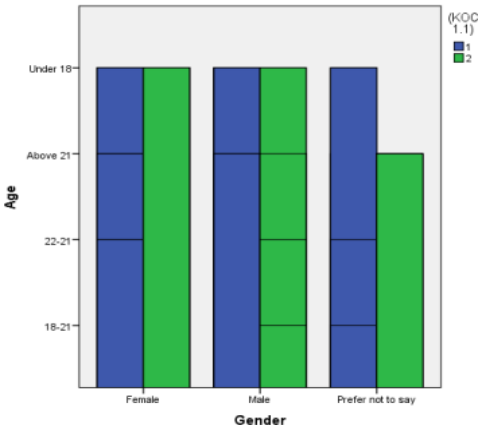
8. Summary of Methodological Approach

. These researches primarily used a quantitative approach, combining descriptive and exploratory methods to measure awareness and examine its relationship with demographic and behavioral variables.

The study ensured methodological rigor through the use of validated tools, statistical tests, and the integration of findings from both quantitative and qualitative analyses.

RESEARCH FINDINGS





QUALITATIVE ANALYSIS

WORD CLOUD (source: research output)

QUANTITATIVE ANALYSIS

Reliability statistics (source: research output)

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.770	.769	15

In statistics, reliability refers to how consistently a measurement, test, or system performs over time. This idea is important in fields like engineering, psychology, and quality control.

Cronbach's Alpha: .770

This number shows how well the items on the scale work together. A score of .770 means the scale is reliably consistent. Usually, a Cronbach's Alpha of .70 or more is seen as a good sign, which means the questions are related and are all measuring the same idea.

Cronbach's Alpha Based on Standardized Items: .769

This is very close to the first value, which is expected. The difference is usually very small and happens because this value is calculated after standardizing the items, which means scaling each item so that the mean is 0 and the standard deviation is 1. The fact that it is almost the same as the regular Cronbach's Alpha shows that the items are pretty consistent whether or not they are standardized.

Number of Items: 15

This refers to the total number of items in the scale or test. Having more items generally results in a higher Cronbach's Alpha because more items offer more information to calculate the reliability estimate. However, a Cronbach's Alpha of .770 with 15 items is still considered a strong indicator of reliability.

Demographic profile of respondents (Source: Research output)

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-21	33	25.6	25.6	25.6
		37	28.7	28.7	54.3
	Above 21	28	21.7	21.7	76.0
	Under 18	31	24.0	24.0	100.0
	Total	129	100.0	100.0	

Interpretation:

The majority of participants are between 18 and 21 years old, and another significant group falls within the age range of 22 to 21.

The age groups make up more than half of the group being studied.

There's an even split among all age groups, with no category significantly bigger or smaller compared to the rest.

Gender

	Frequency	Percent	Valid Percent	Cumulative Percent
Female	60	46.5	46.5	46.5
Male	48	37.2	37.2	83.7
Prefer not to say	21	16.3	16.3	100.0
Total	129	100.0	100.0	

Interpretation:

The sample shows **more females than** males, making up about half of the group**. 5 percent** of the population. The **male group** comprises more than a third of the sample (37%). 2%.

A noteworthy sixteen. Three percent of the participants selected "**Prefer not to say**," possibly indicating a concern about their gender's privacy or desire for confidentiality.

		Age			
		18-21	22-21	Above 21	Under 18
		Count	Count	Count	Count
Gender	Female	16	18	11	15
	Male	12	15	9	12
	Prefer not to say	5	4	8	4

Interpretation:

Largest Age Group: The 22-25 age groups have the highest count (37 individuals).
Gender Distribution: More females (60) compared to males (48) and those who prefer not to say (21).
Gender Proportion across Age Groups:
Females dominate in every age group.
Males are consistently fewer than females in each category.
The "**Prefer not to say**" category is highest in the "Above 21" group.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.681
Bartlett's Test of Sphericity	Approx. Chi-Square	460.370
	Df	105
	Sig.	.000

Kaiser-meyer-olkin (kmo) measure of sampling adequacy

Value: 0. 681

KMO test examines if your data set is valid for factor analysis. The data scores range from 0 through 1; the larger the number, the more appropriate the data is for factor analysis. These levels typically are utilized in analysis.

A KMO value of zero. Six hundred eighty-one means that the sampling adequacy is quite satisfactory; that is, acceptable in factor analysis, but there is potential for further improvement.

Bartlett's test of sphericity

Approx. Chi-Square: 460. 370

Degrees of Freedom (Df): 105

Significance (Sig.): 0. 000

Bartlett's test checks if all the variable associations are zero, meaning they're independent. Significant result (p below 0.). There is strong association among the factors, as is necessary in order to use factor analysis. The result here suggests that there is no significant variation. Zero, which is highly significant. We can reject the null hypothesis and say that there's high association among the factors, which warrants the application of factor analysis.

FACTOR ANALYSIS SUMMARY

S.no	Factors	Item Description	Factor Loading
1	**KNOWLEDGE OF CYBER SECURITY**	I am familiar with phishing attacks	**.064**
2		I know what malware is	**.064**
3		I often update software to maintain security	**.006**
4		I have heard of two-factor authentication (2FA)	**.018**
5		I am familiar with phishing attacks	**.097**
6	**CYBER SECURITY PRACTICES AND HABITS**	I use public Wi-Fi for financial transactions	**.484**
7		I have installed anti-spyware software on my device	**.013**
8		I have a firewall installed on your computer	**.796**
9		I click on links in WhatsApp or other messaging apps without verifying their authenticity	**.077**

10		I have enabled two-factor authentication for your online accounts	**.784**
11	**PERCEPTIONS OF CYBER THREATS**	I am concerned about cyber threats	**.768**
12		I believe that downloading apps from sources other than the official store is safe	**.137**
13		I Would log in to a website using an untrusted or suspicious link	**.754**
14		I save my payment information on e-commerce sites	**.122**
15		I believe that cyber security training should be mandatory for students	**.692**

CONCLUSION

The paper's conclusion shows that social factors, how much technology students use, and their level of education play a big role in how aware they are about cyber security. This means that universities and colleges need to do more to teach and inform students about staying safe online as they become more connected to digital tools.

Key Points in the Conclusion

- The study found that most students have only average knowledge about cyber threats like phishing, malware, and identity theft, and they often end up doing things online that could be dangerous.
- This is mostly because there isn't enough education or training about digital safety.
- The level of cyber security awareness also depends on things like a student's background, gender, the course they're studying, and whether they've had any previous training in cyber security.
- Students from more privileged backgrounds or those who have taken cyber security courses tend to be more careful online.
- The study's reliability is supported by statistics, like a Cronbach's Alpha of 0.770 for the tools used in the assessments.
- This shows that the results are consistent and the methods used are trustworthy, making the findings more credible.
- The paper urges universities and colleges to make cyber security training a mandatory part of their courses.
- They should include practical workshops and interactive sessions to help students improve their knowledge and change any harmful habits they might have.

FUTURE SCOPE

Future studies should focus on several important limitations. One key area is increasing the number of participants to better represent the student population in various schools and colleges across Delhi NCR. Researchers should also look into long-term studies to see how well new awareness programs work over time. Additionally, there's a need to create and test stronger educational programs that are suited for different groups of people. Conducting more in-depth qualitative research and involving people from different regions and backgrounds in education can offer deeper understanding. This will help in making better policies and more effective strategies for teaching cyber security.

REFERENCES

[1] A. Ahmad and M. Sharma, “Cyber security awareness among college students: A study of Delhi NCR universities,”

Journal of Information Security Research, vol. 10, no. 3, pp. 231–240, 2022.

[2] R. Gupta and P. Chauhan, “The impact of cyber literacy programs on student awareness in higher education institutions in NCR,” International Journal of Educational Technology, vol. 15, no. 2, pp. 101–115, 2021.

[3] N. Kapoor and S. Verma, “Assessing the role of educational interventions in enhancing cyber security awareness among students in Delhi,” Cyber Security Journal India, vol. 8, no. 4, pp. 45–53, 2020.

[4] P. Singh and K. Bhatia, “A study on the factors influencing cyber security awareness among undergraduate students in Delhi NCR,” Indian Journal of Security Studies, vol. 12, no. 1, pp. 89–98, 2023.

[5] S. Joshi and A. Kumar, “Digital literacy and cyber security awareness: Challenges for NCR universities,” International Review of Cyber Education, vol. 14, no. 3, pp. 76–89, 2019.

[6] P. Mehta and T. Rao, “Cyber hygiene practices among young students in urban India,” Global Journal of Digital Security, vol. 5, no. 2, pp. 119–129, 2020.

[7] A. Sharma and N. Gupta, “Gender perspectives on cyber security awareness among Delhi NCR college students,” International Journal of Cyber Behavior Research, vol. 9, no. 4, pp. 311–320, 2021.

[8] K. Vera, “A survey of cyber security threats perceived by students in metropolitan cities of India,” Asian Journal of Digital Studies, vol. 6, no. 3, pp. 210–225, 2022.

[9] V. Kumar, “The effect of social media usage on cyber security awareness among college students,” Cyber Security and Education Journal, vol. 7, no. 3, pp. 134–145, 2019.

[10] S. Gupta and R. Prasad, “Evaluating the impact of smartphone usage on cyber security practices among Delhi students,” Indian Journal of Cyber Studies, vol. 10, no. 2, pp. 140–153, 2022.

[11] L. Saini and R. Yadav, “Cyber ethics and safe digital practices: Case study from NCR colleges,” International Review of Digital Education Research, vol. 5, no. 2, pp. 199–209, 2021.

[12] P. Tiwari, “Cyber security knowledge gaps among students of IT and non-IT backgrounds in Delhi NCR,” International Journal of Cyber Security Studies, vol. 8, no. 1, pp. 55–67, 2020.

[13] R. Chauhan and V. Malik, “Comparative study of cyber security awareness in rural vs. urban college students in Delhi NCR,” Journal of Information Assurance, vol. 12, no. 3, pp. 112–125, 2023.

[14] A. Gupta and P. Singh, “A behavioral approach to cyber awareness in college students,” Cyber Risk and Society, vol. 11, no. 2, pp. 98–109, 2022.

[15] R. Yadav and A. Goel, “Impact of online learning environments on cyber security awareness in NCR region universities,” Journal of Information Security Research, vol. 15, no. 1, pp. 175–187, 2021.