Sri Balaji Societys The Balajian Journal of Management Research
3(2) 2026, 66-82
www.publishingindia.com/journals/bjmr/
ISSN: 3049-317X(Online)

Cybercrime Awareness Among Students with Special Reference to Delhi/NCR

Radhika Thapar*, Saniya Marwah**

Abstract

This descriptive study investigates cybercrime awareness among students in Delhi-NCR, focusing on demographic profiles, knowledge levels, attitudes, and behaviors. Utilizing convenience sampling techniques, data were collected through questionnaire surveys from a diverse population. Data were collected from 127 university students using convenience sampling. The data were analyzed through EFA, which extracted five factors of cybercrime awareness, namely "Cybersecurity Awareness and Preparedness", "Personal Information Security Practices", "Technology Comfort and Support", "Cybersecurity Education and Knowledge", and "Challenges and Exposure". Respondents demonstrate a positive inclination towards recognizing and avoiding online scams, yet varying confidence levels exist regarding educational preparedness and access to resources. The conclusions underscore the importance of enhancing formal cybersecurity education and addressing communication dynamics to strengthen cybercrime awareness among students in the region. Findings indicate a promising understanding of cyber threats, with proactive behaviors such as regular password updates and file backups. This study offers valuable insights for developing targeted awareness and prevention strategies to combat cyber threats effectively. The findings indicate that students possess satisfactory awareness of cyber threats but require stronger institutional support and cybersecurity education. The study provides useful implications for universities and policymakers to strengthen cybersecurity awareness programmes.

Keywords: Cybercrime Awareness, Delhi-NCR, Cybersecurity Practices, Prevention Strategies

Introduction

Cybercrime, propelled by the rapid advancement of technology, has permeated every aspect of digital existence, posing a significant threat to individuals and institutions alike (Alsaeed et al., 2023). Students, who are among the most avid users of technology, find themselves particularly vulnerable to the myriad forms of cyber threats that abound in today's interconnected world (Jalil et al., 2024; Alfalah, 2023). This research endeavors to illuminate the critical need for cybercrime awareness among students, recognizing it as an essential component of their digital literacy and safety. The importance of cyber safety and security becomes more visible with the increase in the number of students utilizing the internet. The Internet has become a convenient source for extracting information and enhancing digital connectivity (UNESCO, 2023).

There are various dangerous cyberthreats that impact students' data. These scams manipulate students into providing personal information, leading to theft. Other threats can invade networks, disrupting students' academic activities. This disruption leads to data loss within a short span of time (Alsaeed et al., 2023; Masenya, 2023). The nascent threats include "deepfake technology", which can generate detrimental content that could affect cognitive processes; "social engineering attacks", which expose individuals and extract personal information through tricks; and the rise of dark online activities, which expose students to hazardous or inappropriate online content (Jalil et al., 2024).

Understanding the multifaceted nature of cybercrime and its potential ramifications is paramount for students to navigate the online landscape effectively. From identity theft to phishing scams and cyberbullying, the spectrum of cyber threats is vast and ever-evolving (Shah & Agarwal, 2023). Education regarding cyber safety

* Associate Professor, Rukmini Devi Institute of Advanced Studies, Guru Gobind Singh Indraprastha University, Delhi, India. Email: radhika.thapar@rdias.ac.in
** Assistant Professor, Rukmini Devi Institute of Advanced Studies, Guru Gobind Singh Indraprastha University, Delhi, India. Email: saniya.marwah@rdias.ac.in (Corresponding author)

must be prioritized to reduce dangerous circumstances. Students are safeguarded through the utilization of privacy settings, personal information, and behaving ethically in the process of managing a digitalized environment. By equipping students with the knowledge and tools to identify and mitigate these risks, the researchers attempt to empower students proactively to safeguard their digital identities and personal information (Quyen & Lien, 2022).

Furthermore, fostering a culture of cybercrime awareness among students not only protects them individually but also creates a safer digital environment for all. This project will delve into the intricate dimensions of cybercrime and its far-reaching impacts on individuals and society at large (Huraj et al., 2023). Through comprehensive analysis and practical insights, Alqahtani (2022) aims to equip students with the awareness and skills necessary to navigate the digital realm securely. By fostering a proactive approach to cybersecurity, students were empowered to become responsible digital citizens and agents of positive change in the fight against cybercrime (Hair et al., 2019; Jalil et al., 2024).

Previous researchers have focused on understanding the students' awareness of cybersecurity practices in different countries (Raju et al., 2022). This study contributes to the existing literature through the identification of students' interaction with the digital environment and translating these findings to provide crucial input in the development of policies for reducing students' exposure to different cybercrimes and promoting a safe cyberspace for a digitalized and inclusive learning environment.

Therefore, this study aims to examine students' existing level of exposure to virtual space, underlying factors of cybercrime awareness, and propose suggestions to strengthen cybersecurity awareness and promote safe digital practices. The manuscript is divided into sections as follows: review of literature, research methodology, followed by results and policy recommendations.

Review of Literature

Cybersecurity Awareness and Preparedness

Cybersecurity behaviour has gained attention in recent years. Alfalah (2023), in his study, demonstrated the dimensions of cyberthreats impacting the students' perception towards utilization of LMS. The responses were collected from the students in the Kingdom of Saudi Arabia. The results revealed that security awareness plays an important role in impacting the attitude of students towards the utilization of the Internet. Similarly, Alsaeed et al. (2023) sought to determine students' attitudes at Abdulrahman Bin Faisal University toward the Internet and their understanding of the hazards associated with cybercrime. According to the report, students have a positive attitude towards the Internet and are highly aware of the hazards associated with cybercrime. Various research studies were conducted at both planned and random sites in Palestine to better understand the variances in risk-aware cultures and teenagers' views and behaviours following the advent of cybersecurity awareness in cyberspace (Albada & Eleyan, 2024).

Personal Information Security Practices

Erendor and Yildirim (2022) conducted a survey assessing awareness of personal information security practices among students at Kyrgyz-Turkish Manas University. The findings revealed that students were unaware of the practices they should follow in the online space. Furthermore, the study suggested that learning resources should include guidelines and procedures for preventing the loss of personal information on the web appropriately. Similarly, Raju et al. (2022) reported that individuals' awareness of cyberattacks was based on information collected through questionnaires distributed to 110 students. The study emphasized the areas of improvement and ways to educate students about illicit access.

Technology Comfort and Support

Technology and information are so essential to our daily lives both personally and professionally that they have taken on a life of their own. During the COVID-19 pandemic, knowledge and technology advances more quickly and has made dependence on infrastructure a crucial element (Kaur et al., 2024). Various research frameworks, models, and variables were reviewed, and it has been found that the amount of time spent online has skyrocketed as more individuals and companies utilize emerging technologies, including social networking, cloud computing, the Internet of Things, wireless communication, and cryptocurrencies, which

are contributing to an increase in infrastructural support (Albada & Eleyan, 2024). Kenworthy et al. (2026) stated that with increased use of secure devices, applications, and controls, individuals can interact in a safe environment.

Cybersecurity Education and Knowledge

A comprehensive examination is required to provide a multitude of cybersecurity knowledge. Jalil et al. (2024) suggested implementing different stages of a cybersecurity awareness programme to control the danger of cyber threats. The participants gained knowledge about dangers and risks through the module. Likewise, a unique prototype depicting experiential learning was developed to guide professionals during utilisation in a technology-oriented environment. The outcome revealed high student engagement in tech-enabled learning (Wei-Kocsis et al., 2023). The studies explained the importance of tech-enabled learning and the competencies required to cope with the challenges and threats in the online space. Alammari et al. (2022) further extended this by evaluating the need for cybersecurity degree programmes through the validation of group decision-making techniques. The approach identified the skills and competencies professionals need to design software for students.

Challenges and Exposure

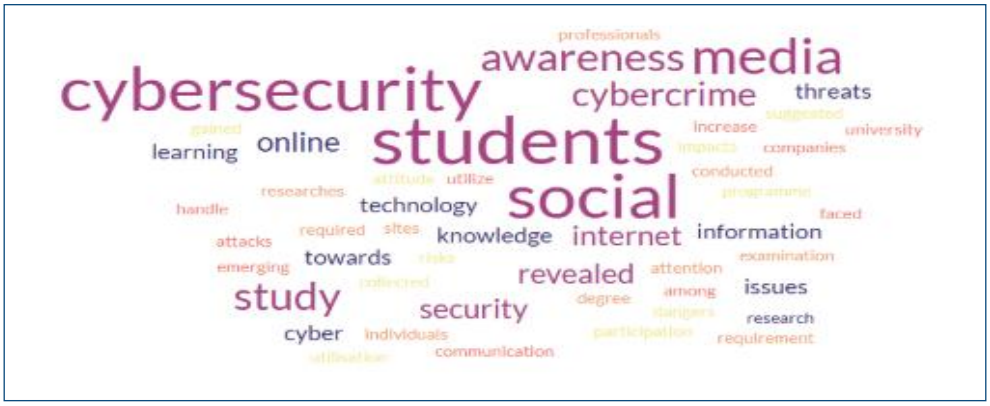
Social media has completely changed the way of interaction, communication, and exchanging information. Recently, there have been a number of social media and cybersecurity events, with people, companies, and government organizations among the victims (Zulqadri et al., 2022). Cybersecurity concerns are growing as social media usage rises. Common cybercrimes such as phishing, social engineering, virus assaults, cyberstalking, identity theft, and cybercasting are all examined (Kaur et al., 2024). Persistent weaknesses in social media platforms' security architecture have increased the frequency of criminal-led activities (Muhammad et al., 2023). For this reason, further study and instruction in cybersecurity are required to prevent similar occurrences and their effects in the future. Researchers and law enforcement still lack a complete understanding of cybercrime. According to reports from the UK Government, victims of cybercrime were reluctant to report crimes because they believed the police had the necessary tools to handle these offences. These studies also point to problems with the police, such as a lack of awareness of cybercrime (Curtis & Oxburgh, 2023).

With increased use of the internet and social media platforms, students are prone to various forms of cybercrimes. Students are not aware of cybersecurity practices, exposing them to cybercrime (Mohammed & Bamasoud, 2022). This issue calls for an urgent evaluation of students' knowledge of cybercrime practices and the underlying factors shaping cybercrime awareness. Based on the identified research gap, the present study aims to address the following questions:

- What is the level of students' exposure to the digital environment?
- What are the underlying factors of cybercrime awareness among university students in the Delhi-NCR region?
- What suggestions can be proposed for educational institutions and policymakers to strengthen cybersecurity awareness and promote safe digital practices among students?

Resolving these queries will bridge the gap and establish the study's originality by extracting substantiation from students in higher education institutes in Delhi NCR, an area that has received limited attention regarding cybercrime. The study attempts to merge the evaluation of students' exposure to the digital environment with the factors identified through EFA, which provided strong evidence for developing focused awareness initiatives. The factors were studied to develop educational resources and build students' capability to withstand cyber incidents.

A Word Cloud in "NVivo" software was constructed during a systematic review of research papers to highlight the most recurring concepts. Of these 40 words, 35 highly indexed journals supported the study's previous outcomes (Fig. 1).



Source: Authors' own compilation.

Fig. 1: Word Cloud

Construct Operationalisation and Research Framework

The scale consisted of 16 statements adapted from different sources. A five-point response format (1 = "strongly opposed", 5 = "strongly accepted") was employed (Table 1).

Cybersecurity Awareness and Preparedness

It involves adopting precautionary measures to secure digital documents and private data by understanding threats, incidents, and damage in cyberspace (Nurse, 2021; Wilson & Hash, 2003). It involves backing up important data and understanding the risks associated with sharing files.

Personal Information Security Practices

It involves the actions taken to prevent personal information from illicit access, inappropriate use, and digital attacks. Various steps to protect information, such as creating strong credentials, modifying settings, and understanding the legal consequences of sharing personal information online (Wilson & Hash, 2003; Bada et al., 2019).

Technology Comfort and Support

It involves the ability to use digital technologies, supported by the infrastructure and technical requirements needed to manage online threat concerns. Comfort in utilising the digital landscape, supported by infrastructure (Haney & Lutters, 2021; Nurse, 2021).

Cybersecurity Education and Knowledge

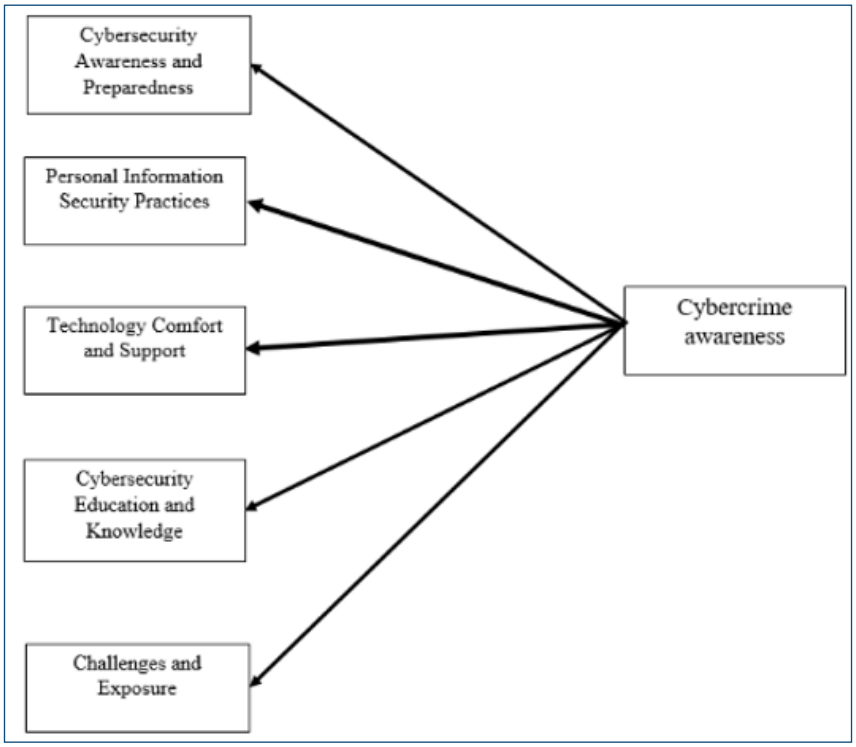
It involves the competencies and capabilities that can be developed or enhanced through cybersecurity education and training programmes to manage the hazardous threats in the digital environment (Wilson & Hash, 2003; Mendu et al., 2020)

Challenges and Exposure

It involves the hindrances an individual faces in executing cybersecurity practices and the level of vulnerability to threats, information, and incidents through the internet, media sources, and education (Haney & Lutters, 2021; Barbhuiya, 2024).

Table 1: Questionnaire Items and Sources

Factors	*Codes*	*No. of Items*	*Sources*
Cybersecurity Awareness and Preparedness	CAP	5	Adapted from Alharbi & Tassaddiq (2021); Alsaeed et al. (2023)
Personal Information Security Practices	PISP	4	
Technology Comfort and Support	TCS	3	
Cybersecurity Education and Knowledge	CEK	2	
Challenges and Exposure	CK	2	



Source: Authors' own compilation.

Fig. 2: Research Framework

Research Methodology

The survey method and quantitative approach were employed to examine awareness among students regarding cybercrime on a national level. The collected information provides an overall view of students' awareness through the employment of descriptive and inferential statistics. The universe of study includes higher education and secondary school students in various colleges/institutes/universities in Delhi NCR. Because information on students' cybersecurity awareness was limited, a convenience sampling method was employed. The questionnaire underlying five factors of cybercrime awareness was developed in English. The demographic variables along with the statement were evaluated for the purpose of ensuring "content validity (CV)" and "face validity (FV)". FV was evaluated by a member of the research team and then by the Head of Department.

CV was evaluated by 6 experts who possess a minimum of 5 years of experience and expertise in technology, education, and psychology. The suggestions were considered and incorporated in such a manner that the technical jargon was substituted with easy words. A feasibility study was undertaken to assess the workability, achievability, and practicability of the sample of 50 students through online surveys via WhatsApp and Gmail. This was because the target participants were very active on both platforms, which proved useful. During the pilot testing, the reliability statistic was 0.85. The tests ensured the reliability of the scale Hair et al., 2019). The

obtained data of 170 students were cleaned and filtered after removing missing and inconsistent responses. As per Chin (1988), the sample size should be 10 times the number of the greatest statements of the construct. Therefore, the least sample size should be at least 100. The researcher prioritizes data quality over quantity to ensure the accuracy of the findings. Therefore, the researchers investigated 127 responses using factor analysis in SPSS and Excel.

Out of 127 individuals, 70 individuals belong to the male category. 90 individuals belong to the school. 100 individuals have their email ids whereas 40 individuals use electronic gadgets for 2 hours to 4 hours. 67 individuals have not enrolled in the tech-enabled courses (Table 2).

Table 2: Sample Characteristics

Category	*Frequency*	*Percentage*	*Valid Percentage*	*Cumulative Percentage*
Gender				
Male	70	55.11	55.11	55.11
Female	47	37.00	37.00	92.1
Transgender	10	7.87	7.87	100
Type of Educational Institute				
School	90	70.86	70.86	70.86
HEI	37	29.13	29.13	100
Internet Access at Home				
Yes	110	86.61	86.61	86.61
No	17	13.39	13.39	100
Distribution of Email ID				
Yes	100	78.74	78.74	78.74
No	27	21.26	21.26	100
Use of Digital Devices Per Day				
Upto 30 mins	15	11.8	11.8	11.8
30 mins to 1 hour	20	15.74	15.74	27.54
1 hour to 2 hours	50	39.37	39.37	66.91
2 hours to 4 hours	40	31.49	31.49	98.4
More than 4 hours	2	1.6	1.6	100
Participation in Courses Related to ICT				
Yes	67	52.76	52.76	52.76
No	60	47.44	47.44	100

Source: Authors' own compilation.

Data Analysis

Analysis of Data About Students' Exposure to the Digital Environment

The collected information, based on the statements, is presented by subgroup under each section.

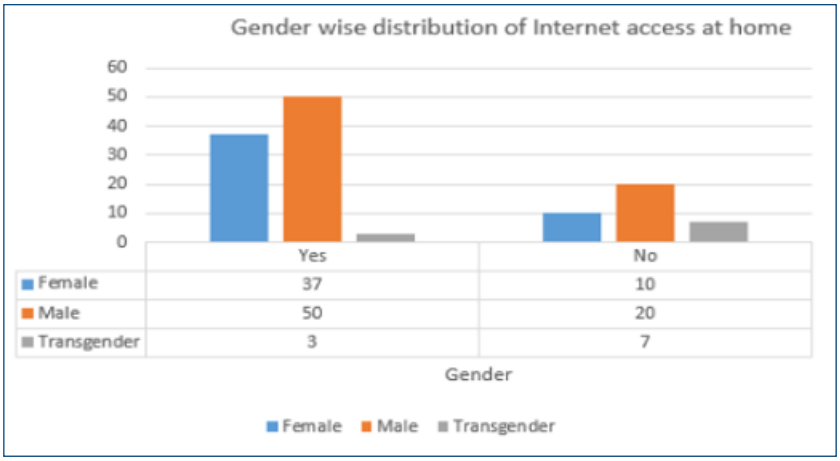
- *Sex Wise Distribution of "Internet Access at Home"*

The given figures display that 50 "males" have web approachability at home, followed by 3 "females" and 3 "transgender." Whereas, 20 "males" do not have web approachability at home, followed by 10 "females" and 7 "transgender" (Table 3 & Fig. 3).

Table 3: Internet Access at Home

Gender	*Yes*	*No*	*Total*
Female	37(78.72)	10(21.28)	47(100)
Male	50(71.42)	20(28.58)	70(100)
Transgender	3(30)	7(70)	10(100)

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 3: Graphical Representation of Internet Access at Home

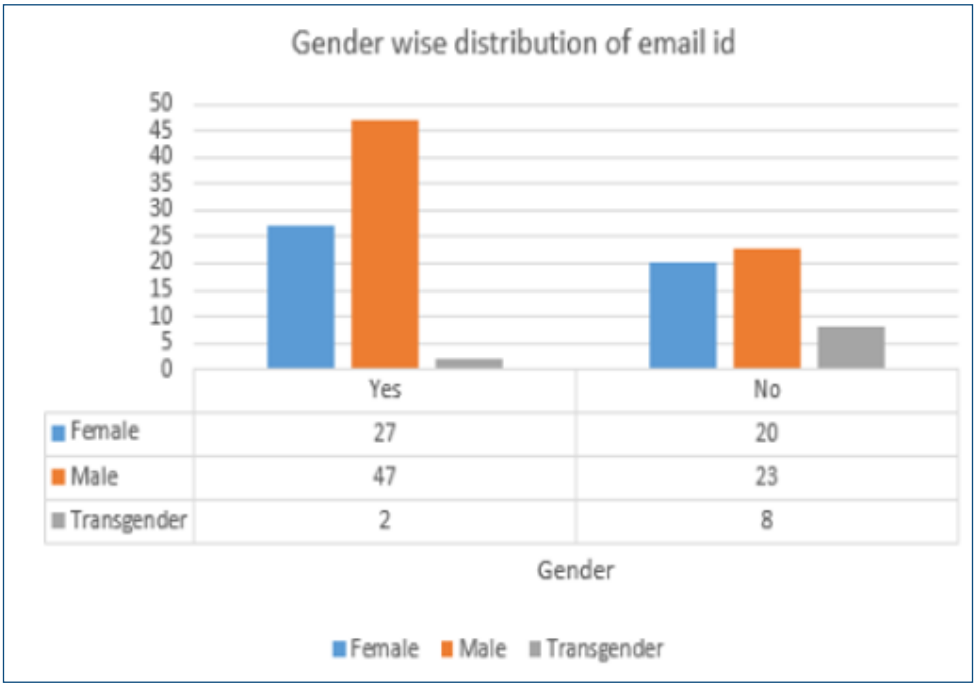
- *Sex Wise "Distribution of Email ID"*

The figures display that 47 "males" possess an email ID, followed by 27 "females" and 2 "transgender." Whereas, 23 "males" do not possess an email ID, followed by 20 "females" and 8 "transgender" (Table 4 & Fig. 4).

Table 4: Distribution of Email ID

Gender	*Yes*	*No*	*Total*
Female	27(57.44)	20(42.56)	47(100)
Male	47(67.14)	23(32.86)	70(100)
Transgender	2(20)	8(80)	10(100)

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 4: Graphical Representation of Gender-Wise Distribution of Email ID

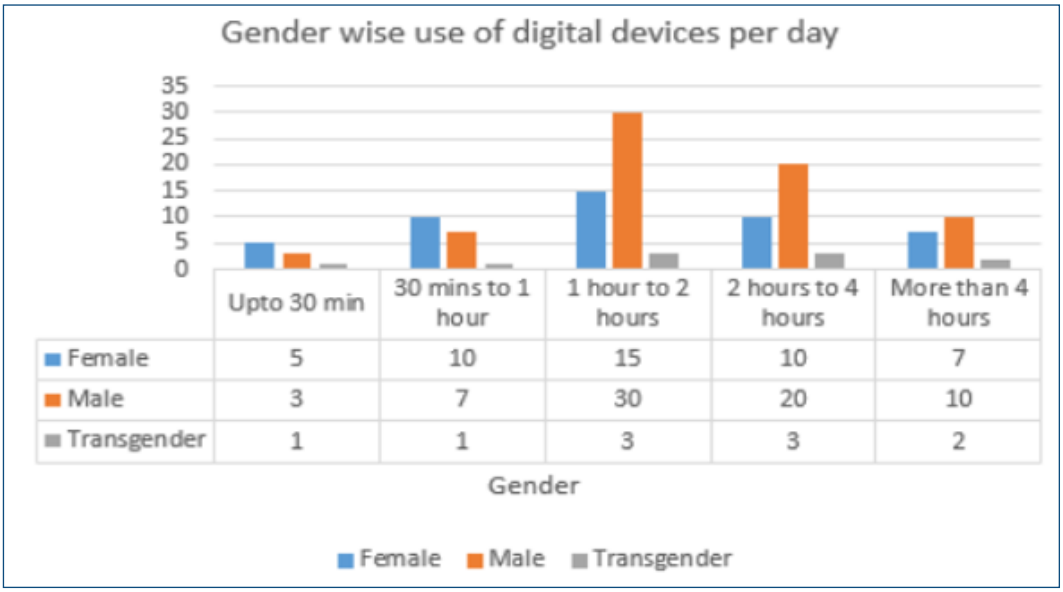
- *Sex Wise "Use of Digital Devices Per Day"*

The figures display that 30 "males" use electronic gadgets for 1 to 2 hours daily, followed by 15 "females" and 3 "transgender" (Table 5 & Fig. 5).

Table 5: Use of Digital Devices Per Day

Gender	*Up to 30 Mins*	*30 Mins to 1 Hour*	*1 Hour to 2 Hours*	*2 Hours to 4 Hours*	*More than 4 Hours*	*Total*
Female	5(10.63)	10(21.27)	15(31.91)	10(21.27)	7(14.89)	47(100)
Male	3 (4.28)	7(10)	30(42.85)	20(28.57)	10(14.28)	70(100)
Transgender	1(10)	1(10)	3(30)	3(30)	2(20)	10(100)

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 5: Graphical Representation of Gender-Wise Use of Digital Devices Per Day

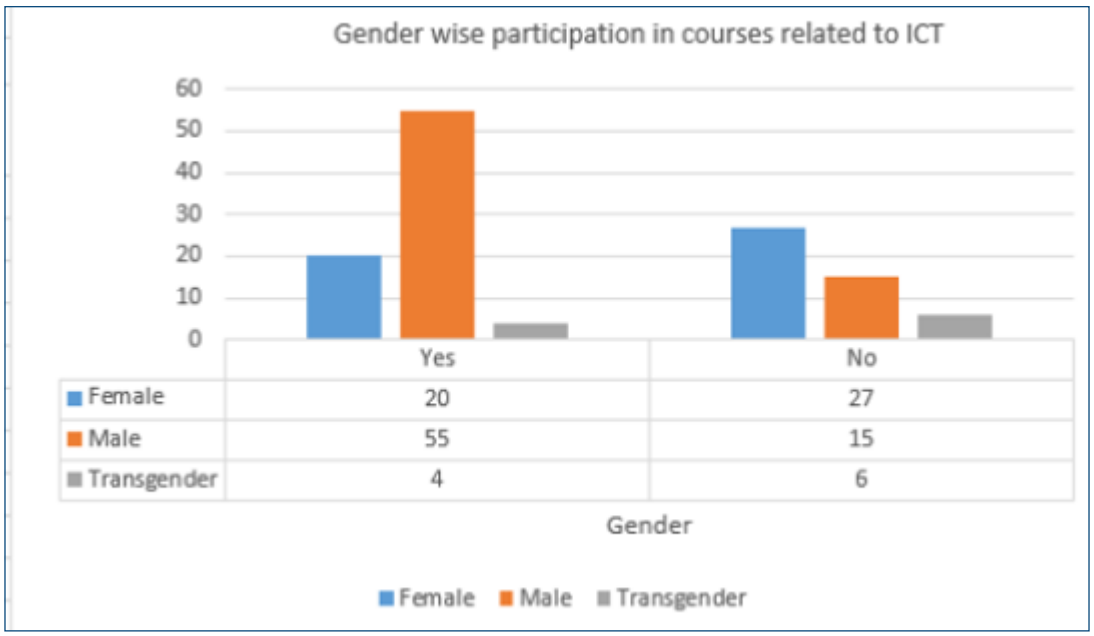
- *Sex Wise "Participation in Courses Related to ICT"*

The figures show that 55 "males" enrolled in tech-enabled courses, followed by 20 "females" and 4 "transgender". Whereas, 27 "females" have not enrolled in tech-enabled courses, followed by 15 "males" and 6 "transgender" (Table 6 & Fig. 6).

Table 6: Participation in Courses Related to ICT

Gender	*Yes*	*No*	*Total*
Female	20(42.56)	27(57.44)	47(100)
Male	55(78.57)	15(21.43)	70(100)
Transgender	4(40)	6(60)	10(100)

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 6: Graphical Representation of Participation in Courses Related to ICT

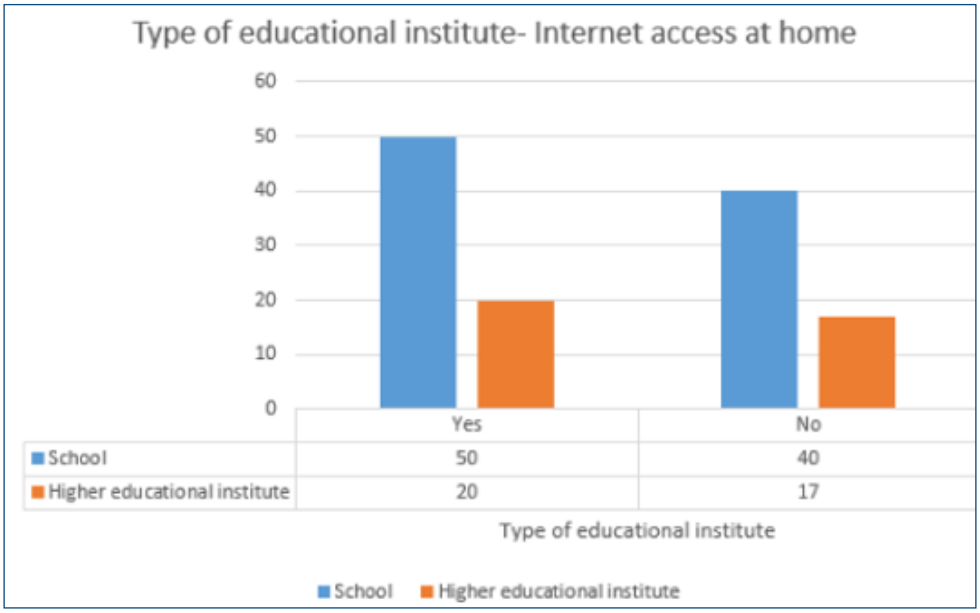
- *Educational Institute-Wise Distribution of "Internet Access at Home"*

The given figures show that 50 individuals from the school have web approachability at home, followed by 20 individuals from HEI. Whereas 40 individuals from the school do not have web approachability at home, followed by 17 individuals from HEI (Table 7 & Fig. 7).

Table 7: Internet Access at Home

Types of Educational Institute	*Yes*	*No*	*Total*
School	50(55.55)	40(44.44)	90100)
Higher Educational Institute	20(54.05)	17(45.94)	37(100)

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 7: Graphical Representation of Internet Access at Home

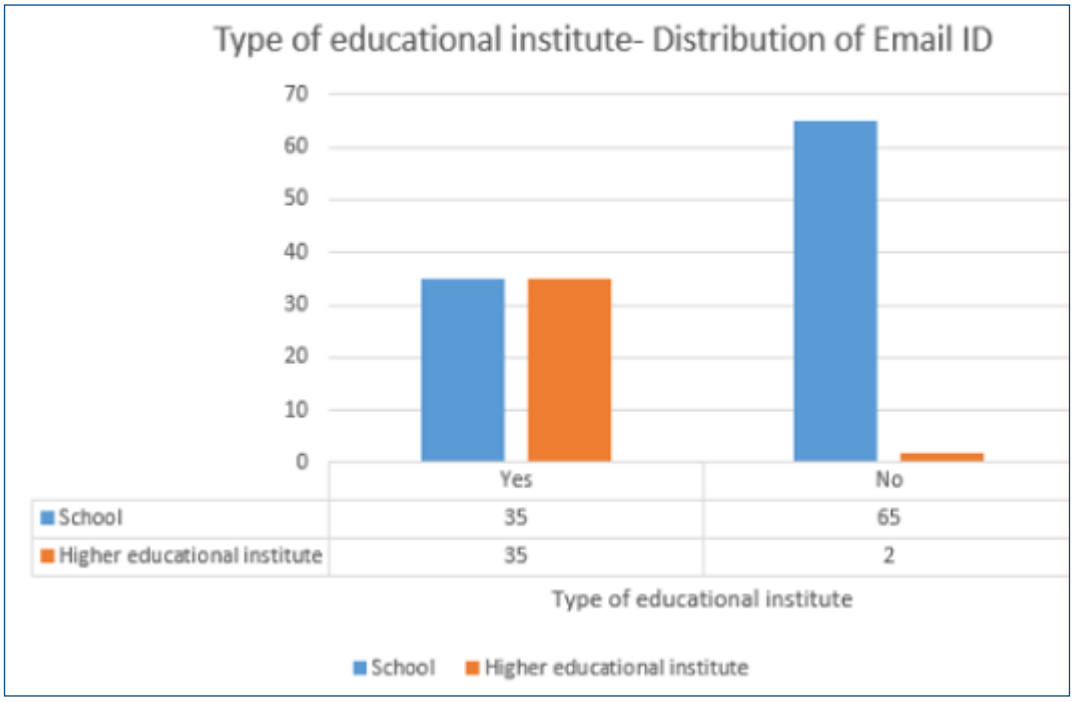
- *Educational Institute-Wise "Distribution of Email ID"*

The figures show that 35 individuals from the school possess an email ID, followed by 35 individuals from HEI. Whereas, 65 individuals from the school do not possess an email ID, followed by 2 individuals from HEI (Table 8 & Fig. 8).

Table 8: Distribution of Email ID

Types of Educational Institute	*Yes*	*No*	*Total*
School	35(38.88)	65(72.22)	90100)
Higher Educational Institute	35(94.59)	2(5.5)	37(100)"

Source: Authors' own compilation.



Source: Authors' own compilation

Fig. 8: Graphical Representation of Distribution of Email ID

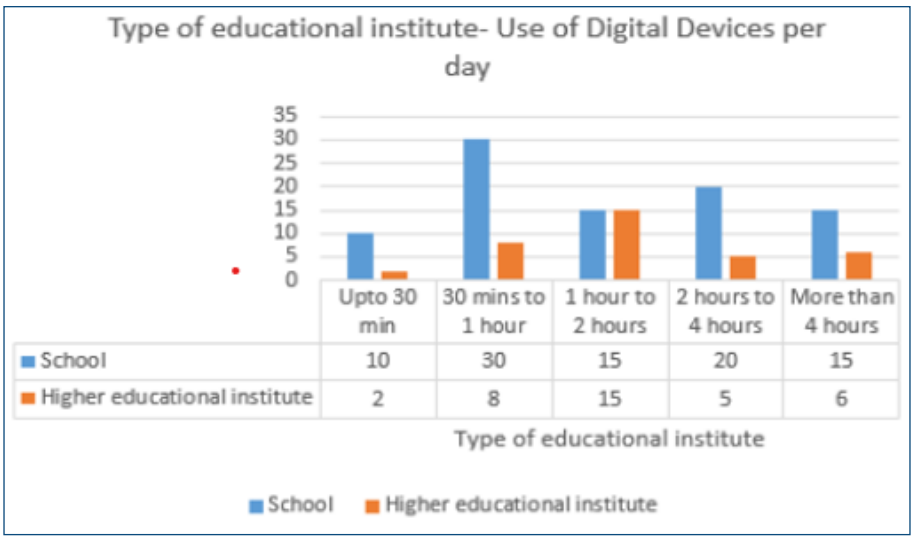
- *Educational Institute-Wise "Use of Digital Devices Per Day"*

The figures show that the 30 individuals from the school use electronic gadgets for 30 mins to 1 hour, followed by 15 individuals from HEI (Table 9 & Fig. 9).

Table 9: Use of Digital Devices Per Day

Type of Educational Institute	*Up to 30 Mins*	*30 Mins to 1 Hour*	*1 Hour To 2 Hours*	*2 Hours To 4 Hours*	*More Than 4 Hours*	*Total*
School	10 (11.11)	30 (33.33)	15 (16.66)	20 (22.22)	15 (16.66)	90 (100)
Higher education institute	2 (5.4)	8 (21.62)	15 (40.54)	5 (13.51)	6 (16.21)	10 (100)"

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 9: Graphical Representation Use of Digital Devices Per Day

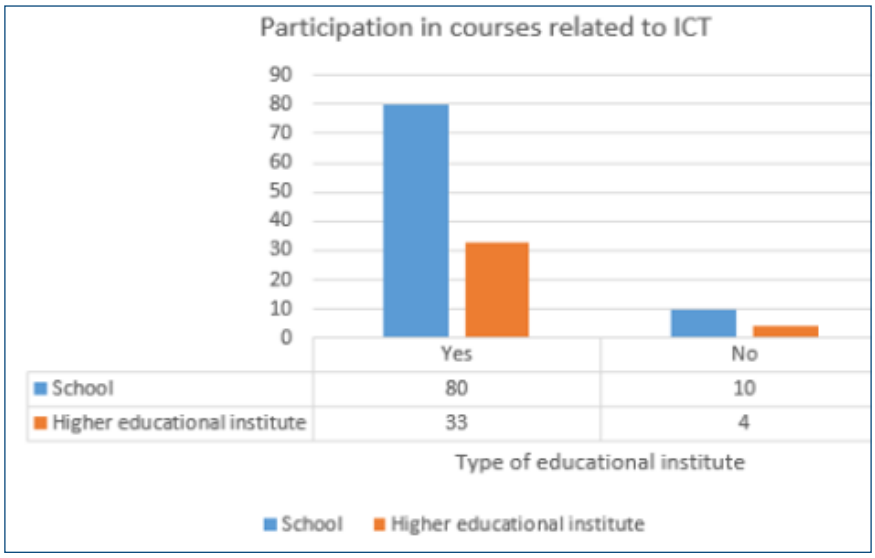
- *Educational Institute-Wise "Participation in Courses Related to ICT"*

The figures show that 80 individuals from schools enrolled in tech-enabled courses, followed by 33 individuals from HEIs. Whereas 10 individuals from schools have not enrolled in tech-enabled courses, followed by 4 individuals from HEIs (Table 10 & Fig. 10).

Table 10: Participation in Courses Related to ICT

Types of Educational Institute	*Yes*	*No*	*Total*
School	80(88.88)	10(11.11)	90100)
Higher Educational Institute	33(89.18)	4(10.81)	37(100)"

Source: Authors' own compilation.



Source: Authors' own compilation.

Fig. 10: Graphical Representation of Participation in Courses Related to ICT

Quantitative Analysis Using Exploratory Factor Analysis (EFA)

- *Reliability Statistics*

The "Cronbach's alpha" for 16 items was recorded as 0.827, which is higher than the standard value of 0.7, as shown in Table 11. The tests in Table 12 are used to measure the sufficiency of the size for factor analysis. The figure displays that the value of KMO, i.e., 0.795, is acceptable. Moreover, Bartlett's Test of Sphericity produced a value of 567.239 ($p < 0.001$), leading to the appropriateness of the data for analysis (Table 11 & Table 12).

Table 11: Reliability Statistics

Cronbach's Alpha	*N of Items*
.827	16

Table 12: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.795
Bartlett's Test of Sphericity	Approx. Chi-Square	567.239
	df	120
	Sig.	.000

- *Total Variance*

PCA was calculated to identify the dimensions of the measurement scale. The retention of components was determined using the scree plot and eigenvalue criterion (Hair et al., 2019). All the components accounted for the value of 61.27% of the total variance, depicting that the constructs reflect the structure of the observed data. The first component exhibited an eigenvalue of 4.903 (30.646% variance), depicting the most powerful and impactful factor. The second component exhibited an eigenvalue of 1.514 (9.461% variance), bringing the cumulative value to 40.107%. The third component exhibited an eigenvalue of 1.304 (8.151% variance), bringing the cumulative value to 48.25%. The fourth component exhibited an eigenvalue of 1.058 (6.612% variance), bringing the cumulative value to 54.870%. The fifth component exhibited an eigenvalue of 1.024 (6.403% variance), bringing the cumulative value to 61.273%. The rotated solution revealed that the first component accounted for 15.188% variance. The fifth component accounted for 8.505% variance. The overall cumulative value remains constant at 61.273%. According to Hair et al. (2019), a cumulative variance of 60% or higher is acceptable for the research (Table 13 & Fig. 11).

Table 13: Total Variance Explained

Component	*Initial Eigenvalues*			*Extraction Sums of Squared Loadings*			*Rotation Sums of Squared Loadings*		
	Total	*% of Variance*	*Cumulative %*	*Total*	*% of Variance*	*Cumulative %*	*Total*	*% of Variance*	*Cumulative %*
1	4.903	30.646	30.646	4.903	30.646	30.646	2.430	15.188	15.188
2	1.514	9.461	40.107	1.514	9.461	40.107	2.320	14.498	29.687
3	1.304	8.151	48.258	1.304	8.151	48.258	2.001	12.506	42.193
4	1.058	6.612	54.870	1.058	6.612	54.870	1.692	10.576	52.768
5	1.024	6.403	61.273	1.024	6.403	61.273	1.361	8.505	61.273
6	.871	5.444	66.717						
7	.838	5.236	71.953						
8	.788	4.926	76.879						
9	.697	4.355	81.234						
10	.605	3.780	85.014						
11	.530	3.309	88.324						
12	.489	3.055	91.378						
13	.416	2.600	93.979						
14	.375	2.342	96.320						
15	.325	2.029	98.350						
16	.264	1.650	100.000						
Extraction Method: Principal Component Analysis.									

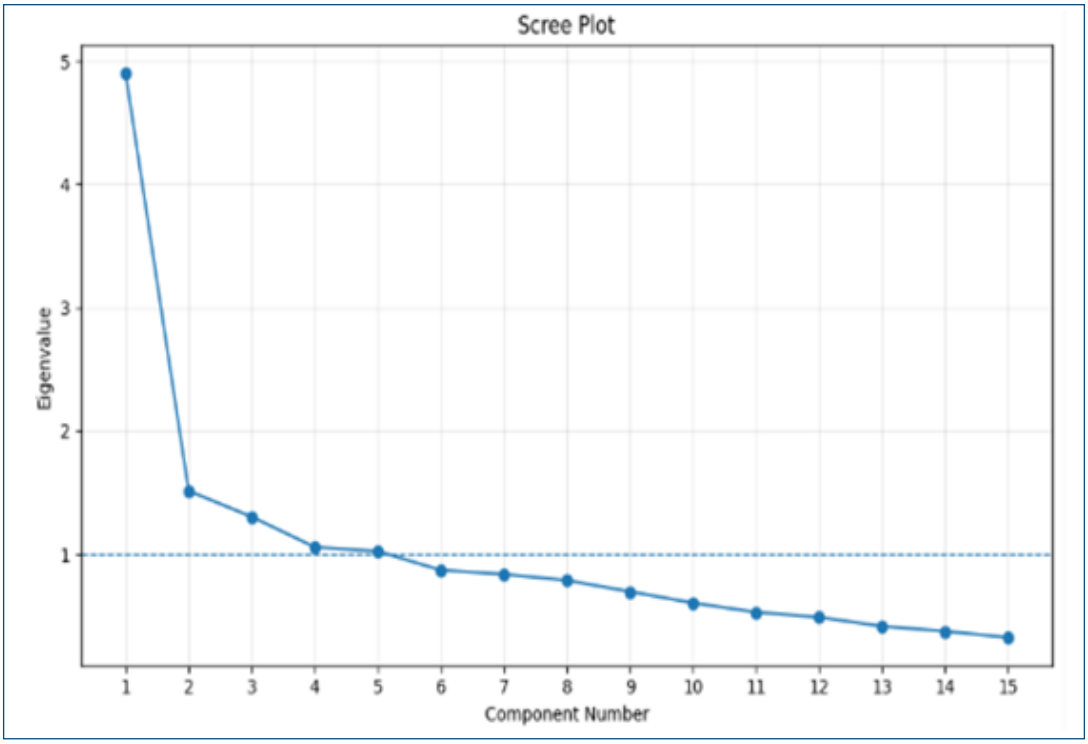


Fig. 11: Screeplot

- *Factor Loadings*

All retained statements demonstrated factor loadings above the standard 0.40 threshold (Hair et al., 2019), resulting in the extraction of five factors using EFA. The first factor, CAP, comprises five statements with factor loadings from 0.485 to 0.791. This factor captured students' readiness regarding cybersecurity. The second factor, PISP, comprises four statements with factor loadings from 0.641 to 0.768. This factor captured the online practices students follow to protect their personal information. The third factor, TCS, comprises three statements with factor loadings from 0.648 to 0.764. This factor captured the ease of using technologies through support and resources. The fourth factor, CEK, comprises two statements with factor loadings from 0.832 to 0.821. This factor captured the formal education and training required to prepare respondents with cybersecurity knowledge and skills. The fifth factor, CE, comprises two statements that assessed the challenges of maintaining cybersecurity habits and exposure to news and events. These two statements were retained based on their factor loadings (0.826 to 0.677), which indicate their relevance in explaining the character of cybercrime awareness among students (Table 14).

Table 14: Summary of Factor Loadings

Factors	*Items*	*Factor Loadings*
CAP	CAP1	.791
	CAP2	.711
	CAP3	.683
	CAP4	.537
	CAP5	.485
PISP	PISP1	.768
	PISP2	.757
	PISP3	.648
	PISP4	.641

Factors	*Items*	*Factor Loadings*
TCS	TCS1	.764
	TCS2	.682
	TCS3	.648
CEK	CEK1	.832
	CEK2	.821
CE	CE1	.826
	CE2	.677

Discussions

The survey findings reveal a diverse respondent demographic, predominantly young adults with significant representation from graduates. Both genders are equally represented. Underlying factors such as CAP, PISP, TCS, CEK, and CE explained 61.27% of the deviations, leading to the definition of cybercrime awareness as a multifaceted variable (Hair et al., 2019). The extracted factors defining cybercrime awareness are consistent with the previous literature (Alharbi & Tassaddiq, 2021; Alsaeed et al., 2023). Previous work defined awareness as the combined concepts of wisdom, attitude, and web-based activities (Alharbi & Tassaddiq, 2021; Alsaeed et al., 2023).

The factor CAP defines an individual's ability to identify and cope with threats during online activities (Nurse, 2021; Wilson & Hash, 2003). The positive behavior has been observed amongst individuals who possess awareness about online activities (Wahid et al., 2021). The PISP factor highlights the importance of changing settings, i.e., usernames and passwords, to create a safe environment for accessing online services. They also demonstrate proactive security measures such as updating passwords and backing up important files. These outcomes align with Bada et al. (2019), who found that studying legal requirements has also become essential as a practice. The factor TCS defines the infrastructural and resource requirements for handling technical competencies. These findings align with Haney and Lutters (2021), who found that guidance and resources from the institute affect respondents' perceptions of risks in the digital environment. Despite a substantial proportion discussing cybersecurity with peers and accessing support services, challenges in practicing good cybersecurity habits persist. The factor CEK shows that most respondents feel confident identifying phishing emails and understanding the risks of sharing personal information online as part of training and educational programmes.

While a majority feel confident in recognizing and avoiding online scams, a significant portion remains neutral. A considerable percentage engage in cyber-security education or training, which drastically improves digital competency skills (Erendor & Yildirim, 2022; Jalil et al., 2024). However, respondents report relatively high exposure to cybercrime-related information and confidence in educational initiatives that promote cybercrime awareness (Alammari et al., 2022). Managing and coordinating online activities faces challenges. The news and media contribute to threats that act as obstacles in the online universe. These challenges can be reduced through the support of training and educational support (Albada & Eleyan, 2024).

The results contribute to the research repository, which emphasizes the adoption of holistic approach towards inclusive education on cybersecurity (Muhammad et al., 2023; Alsharida et al., 2023).

Conclusion

The study investigated sample characteristics related to students' approachability to the digital world in schools and HEIs in Delhi-NCR. The analysis of the data revealed that male students have web approachability at home, email ownership, frequently utilised digital devices, and are enrolled in tech-enabled courses. The majority of the students from HEIs reported owning email accounts and enrolling in tech-enabled courses, while school students have web approachability at home. The majority of the students utilize electronic gadgets for at least one hour per day. Yet, disparities exist in accessing electronic resources among different groups, thereby signifying the importance of inclusive digital education. EFA was employed to identify the five underlying factors

of cybercrime awareness. The results demonstrated that the existence of CAP, PISP, TCS, CEK, and CE generated awareness of damages and threats, yet there is a requirement for inculcating training, online practices, and learning to evolve within the digital environment. The research provides the framework for evaluating cybercrime awareness among the learners. The results are helpful for HEIs, schools, and policymakers to develop policies targeting awareness programmes, integrating the policies with academics, and augmenting initiatives. The initiative should be implemented in alignment with the curriculum. The curriculum should include topics like threats, damages, guidelines, protocols, privacy, and online policies. These concepts will help individuals in developing an effective digital environment. The theoretical knowledge should be imparted through workshops and sessions. Students should be provided with hands-on experience of handling cybercrime, developing strategies, and equipping them with skills to create a safe digitalised world. Moreover, future researchers can utilize CFA and SEM to validate the holistic framework through the employment of samples (Hair et al., 2019).

Implications

Theoretical Implications

The given study signifies its importance through its contribution in the form of a well-defined structure on cybercrime awareness. This structure encompasses five constructs which were tested and analyzed through EFA among schools and HEIs. The previous studies emphasized overall awareness level, which has been further extended by incorporating technical, educational, cognitive, and psychological exposure to threats (Hair et al., 2019). This outcome is further supported by the study, which suggests that individual and contextual features affect awareness (Nurse, 2021; Mendu et al., 2020)

Managerial Implications

This study has various implications for different stakeholders within the economy. Educational institutes should merge the concept of cybercrime awareness into educational materials and resources. Education should be taught through the organisation of workshops, seminars, and classroom engagement activities. This further enhances awareness and digital competency among the students (Jalil et al., 2024; Erendor & Yildirim, 2022). The supporting staff of universities guides students in reporting damages and threats during the process of availing web services. This helps boost students' confidence in managing challenges in the online space (Haney & Lutters, 2021). Educational institutes should collaborate with policymakers for the purpose of deriving policies and initiatives towards cybersecurity awareness for the stakeholders. Also, continuous awareness campaigns and evaluations should be implemented to promote a safe environment (Kaur et al., 2024; Muhammad et al., 2023). Moreover, institutes should foster a culture of lifelong learners through collaboration, discussion, certification programmes, competitions, and continuous learning.

Limitations

The study is subject to sampling biases as it primarily focused on students in the Delhi/NCR region, limiting the generalizability of its findings. The study is focused on students from schools and HEIs. The current study adopted a cross-sectional research design. The study focused on five underlying dimensions, and responses were collected through a Google Form, which was prepared in English only.

Scope for Future Research

Extending the research to encompass students from diverse geographical locations across India could offer a more comprehensive understanding of cybercrime awareness among students. Additionally, replicating the study in different regions or countries with varying demographics and societal norms could enhance its external validity and provide a more nuanced perspective on cybercrime awareness. For future scope, longitudinal studies could offer valuable insights by tracking changes in cybercrime awareness and behaviors among students over time. Also, analyzing parents' and teachers' online behavior, including internet usage patterns and responses to simulated phishing attempts, could provide further insights into their susceptibility to cyber threats and help tailor intervention strategies accordingly. Also, workshops and seminars can be incorporated to teach students from schools and HEI students.

Acknowledgements

The authors acknowledge all the participants, experts, and faculty members for contributing their valuable time to the successful completion of this study.

Funding Disclosure

The authors declare that they have not received any funding from external sources.

Conflict of Interest Statement

The authors declare that there are no conflicts of interest that could have impacted the study.

AI Disclosure

The authors declare that no Artificial Intelligence (AI) tools or AI-assisted technologies were used in the preparation, writing, analysis, or development of this manuscript.

References

Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Computer Science*, *8*, e827. https://doi.org/10.7717/peerj-cs.827

Albada, O. M., & Eleyan, D. (2024). Cybersecurity awareness of vulnerabilities: Attacks, solutions, and cybersecurity behavior in Palestine: Literature review. *Cybersecurity Journal*.

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cybersecurity perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences*, *10*(4), 136–144. https://doi.org/10.21833/ijaas.2023.04.017

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), Article 23.

Alsaeed, H. R., Elsayad, W. A., Abd El Ghani, R. T., & Hassan, M. A. (2023). Awareness of cybercrime risks and its relationship to attitude toward Internet use among university students. *Journal of Positive School Psychology*, *7*(10), 108–123.

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, Article 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, *12*(5), Article 2589. https://doi.org/10.3390/app12052589

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. https://doi.org/10.48550/arXiv.1901.02672

Barbhuiya, R. K. (2024). Cyber-safety: Concepts, threats, and essential measures. *Indian Journal of Educational Technology*, *6*(I), 361–376. https://journals.ncert.gov.in/IJET/article/view/487

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573–592.

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, *10*, 52319–52335. https://doi.org/10.1109/ACCESS.2022.3171829

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). London: Cengage Learning.

Haney, J. M., & Lutters, W. G. (2021). Cybersecurity advocates: Discovering the characteristics and skills of an emergent role. *Information & Computer Security*, *29*(3), 485–499. https://doi.org/10.1108/ICS-08-2020-0131

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring cyber security awareness: A comparison between computer science and media science students. *TEM Journal*, *12*(2), 623–633. https://doi.org/10.18421/TEM122-05

Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaiah, M. A. (2024). Cybersecurity awareness among secondary school students post-COVID-19 pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115–127. https://doi.org/10.37934/araset.37.1.115127

Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., Maheshwari, S., Pinjarkar, L., &

Gangarde, R. (2024). Social media in the digital age: A comprehensive review of impacts, challenges, and cybercrime. *Engineering Proceedings, 62*(1), 6.

Kenworthy, A. L., McManus Warnell, J., & Opatska, S. (2026). Hope as educational infrastructure within war in Ukraine: A future created, not just awaited. *Teaching in Higher Education*, 1–19. https://doi.org/10.1080/13562517.2026.2673383

Masenya, T. M. (2023). Awareness and knowledge of cyber ethical behaviour by students in higher education institutions in South Africa. In F. F. Adedoyin & B. Christiansen (Eds.), *Advances in information security, privacy, and ethics* (pp. 33–48). IGI Global. https://doi.org/10.4018/978-1-6684-7207-1.ch002

Mendu, S., Baglione, A., Baee, S., Wu, C., Ng, B., Shaked, A., Clore, G., Boukhechba, M., & Barnes, L. (2020). A framework for understanding the relationship between social media discourse and mental health. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW2), Article 144. https://doi.org/10.1145/3415215

Mohammed, M., & Bamasoud, D. M. (2022). The impact of enhancing awareness of cybersecurity on university students: A survey paper. *Journal of Theoretical and Applied Information Technology*, *100*(15), 4756–4766. https://www.scopus.com/inward/record.uri?eid=2s2.085138808067&partnerID=40&md5=f5409059905f855f94029d0526d10d6b

Muhammad, G., Pratama, A. R., Shaloom, C., & Cassandra, C. (2023). Cybersecurity awareness literature review: A bibliometric analysis. In *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)* (pp. 195–199). IEEE. https://doi.org/10.1109/ICIMCIS60089.2023.10349013

Nurse, J. R. C. (2019). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In J. R. C. Nurse (Ed.), *The Oxford handbook of cyberpsychology* (pp. 662–690). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

Quyen, D., & Lien, N. H. (2022). Literature review of research in the area of digital safety competency for school-age students and the prospect of digital safety education in Vietnam. *Vietnam Journal of Educational Sciences*, *18*(3), 40–51. https://doi.org/10.15625/2615-8957/22210304

Raju, R., Rahman, N. H. A., & Ahmad, A. (2022). Cyber security awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education*, *18*(3), 756–766. https://doi.org/10.24191/ajue.v18i3.18967

Shah, P., & Agarwal, A. (2023). Cyber Suraksha: A card game for smartphone security awareness. *Information and Computer Security*, *31*(5), 576–600. https://doi.org/10.1108/ICS-05-2022-008

UNESCO. (2023). *Global Education Monitoring Report 2023: Technology in education – A tool on whose terms?* UNESCO Publishing. https://doi.org/10.54676/HABJ1624

Wahid, S. D. M., Buja, A. G., Hasrol Jono, M. N. H., & Aziz, A. A. (2021). Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modelling. *International Journal of Advanced Technology and Engineering Exploration*, *8*(74), 73–81. https://doi.org/10.19101/IJATEE.2020.S1762116

Wei-Kocsis, J., Sabounchi, M., Mendis, G. J., Fernando, P., Yang, B., & Zhang, T. (2023). Cybersecurity education in the age of artificial intelligence: A novel proactive and collaborative learning paradigm. *IEEE Transactions on Education*, *66*(4), 312–322. https://doi.org/10.1109/TE.2023.3337337

Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program* (NIST Special Publication 800-50). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50

Zulqadri, D. M., Mustadi, A., & Retnawati, H. (2022). Digital safety during online learning: What we do to protect our student? *Jurnal Iqra': Kajian Ilmu Pendidikan*, *7*(1), 178–191. https://doi.org/10.25217/ji.v7i1.17