ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Assessing Students' Awareness and Practices Regarding Cyber Security in Dakshina Kannada District

Dr. Bharathy[1]., Shraddha[2]

[1]Lecturer, Department of Post-Graduate Studies in Commerce, Govinda Dasa College, Surathkal, Mangaluru

[2] M.Com, Department of Post-Graduate Studies in Commerce, Govinda Dasa College, Surathkal, Mangaluru

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1408000104

Abstract

Purpose

There is growing dependency on technology among students who use the internet regularly. This creates concern regarding cyber security in this digital era. The purpose of this study is to investigate the level of cyber security knowledge and practice among Dakshina Kannada District students. The study investigates how different factors affect knowledge of cyber security among students.

Design/Methodology/Approach

Primary data was obtained from the students studying in Dakshina Kannada District and secondary data was collected from academic literature, scholarly journals, research articles, and government reports, to support the findings.

Findings

According to the findings, although many students are active online users, a sizable portion do not know enough about safe online practices, which highlight awareness gaps among students in Dakshina Kannada District.

Originality or Value

The report stresses the importance of community-based initiatives, focused awareness campaigns, including cyber security instruction in university curriculum as it plays an important role in creating a safer digital environment in Dakshina Kannada District. The findings provide necessary information to educators, legislators, and advocates for digital safety for building youth cyber resilience.

Keywords: Cybersecurity awareness, Cyber safety practices, Students awareness, Cybercrime prevention, Digital literacy, Cyber threat.

I. Introduction

The world has become digital and this digitally connected world creates concern with regards to cyber security. Particularly if we talk about youth, who are the most active users of the internet, they are the ones who become victims of these cybercrimes. With the growth in online platforms, young individuals are becoming more vulnerable to cyber threats such as cybercrime, identity theft, hacking, and online fraud as they depend on online platforms for education, socializing, and entertainment. Even with their frequent usage of digital technology, many students remain unaware of the risks posed by these cyber threats and often fail to take necessary security measures to protect themselves (Sethi & Dutta, 2021).

The COVID-19 pandemic has further increased the role of the internet in education. This made schools and universities shift from their traditional classroom teaching to online learning platforms. This switch in the education system has increased the student's engagement with the digital world, making them more exposed to cyber threats. In regions like Dakshina Kannada, where there is a mix of urban and rural areas with varying levels of internet access and digital literacy, the challenges of cyber security awareness are particularly obvious. Many students, especially in rural areas lack formal education, which may deprive them from being aware about cyber security practices, such as recognizing phishing attempts, managing passwords securely, and safeguarding personal information (Algarni, Xu, & Chan, 2015). This gap in cyber security knowledge among youth makes them at a higher risk of online exploitation and cybercrime. (Anwar et al., 2017)

This study examines youth awareness of cybercrime and cyber security in the Dakshina Kannada district. The study will look into how socioeconomic variables including occupation, income, and education affect students' understanding of cyber security in Dakshina Kannada District. Access to digital resources and cybersecurity education are recognized to be impacted by socioeconomic conditions (Algarni, Xu, & Chan, 2015). While students from lower-income or rural backgrounds may not have had as much exposure to efforts that teach cyber security knowledge, higher-income students are more likely to have greater access to resources and digital security tools. The study will assess student's general awareness, knowledge and security protocol in such situations, as well as the impact of their prior exposure to cyber experience with cyber threats, such as becoming the targets of online fraud or data breaches. Prior research has shown that personal encounters with cybercrime frequently result in a more proactive attitude toward internet safety (Sethi & Dutta, 2021). The study will also explore daily cyber security practices of

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

students', such as password management, software updates, and the use of two-factor authentication which are essential to protect themselves from cyber threats. Even though students are aware of security practices, they may fail to implement them consistently. For example, students often neglect the importance of passwords and fail to update their security software regularly. Thus, identifying these gaps helps in employing cyber security programs which is also vital for designing targeted educational programs that address the specific needs of students in Dakshina Kannada.

The results of this research will help in enhancing cyber security awareness by creating practical recommendations. The study will suggest the integration of cyber security education into educational programs, and the execution of policy measures intended to improve digital literacy for students. The research seeks to equip students with essential resources to safeguard against cyber threats by offering a more community-focused method to cyber security instruction. In summary, this study aims to offer important insights into the cyber security awareness among young people in Dakshina Kannada. By examining the elements affecting students' cyber security awareness, this research will guide upcoming education programs, community initiatives, and policy strategies to improve cyber security knowledge and practices among young people, ensuring they are prepared to interact safely and securely in the digital landscape.

Objectives of the Study

- ❖ To assess the level of awareness among students about cybercrime
- ❖ To study the level of awareness among youth about cyber security
- ❖ To investigate the effect of prior experience with cyber threats on cybercrime awareness
- ❖ To provide actionable recommendations for enhancing cybercrime awareness.

Statement of the Problem

In this digital generation, people have made the internet as part of their lives by investing themselves in various online platforms for various needs such as for academics, payments and many more. Where there are chances of being the victim of cybercrime. Cybercrime creates a significant problem to individuals, especially to youth. Despite awareness campaigns and individuals taking security measures people still become victims of cyber-attacks. This raises concern regarding the level of awareness they have about cybercrime and security measures particularly among students. Thus, the study focuses on identifying the student's awareness and practices.

II. Research Methodology

Research Design

The research was carried out concerning the research subject. The study is an empirical one using both primary and secondary data. Primary data was obtained from the students studying in Dakshina Kannada District. The data was collected through a structured questionnaire containing questions relating to the title and objectives of the study. The questionnaire included the demographic information and the subjective information. For the study the secondary data used from published research articles and journals. These sources were referred to identify gaps in the study, to support formulation of objectives and to compare findings of current study with the previous studies.

Sample size and techniques

For the study, a sample of 100 respondents was taken from Dakshina Kannada district through a survey.

Timing of data collection: Data was collected from 100 respondents via Google Forms between 29 December 2024 and 29 March 2025

Tools for data analysis

Analysis of data is done through basic statistical methods. Some of the relevant and interesting data are presented in the form of percentages.

Limitations of the Study

The study is based on assessment done on the data collected by the residents of Dakshina Kannada District. The study concentrates on cyber security awareness and practices of a sample of only 100 respondents. An element of personal bias may affect the data to some extent. With the knowledge of these limitations, an attempt is made to assess students' awareness and practices regarding cyber security.

III. Review of Literature

Author(s)	Highlights
Garba et al. (2022)	Emphasized the importance of cybersecurity knowledge due to increasing internet dependence. Explored cyber bullying, personal information protection, internet banking, internet addiction, and self-protection.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

	Found high awareness in internet banking but only moderate in other areas. Majority respondents were male. Suggested targeted awareness and more focus on female students. Future research to implement cybersecurity education programs.
Sani et al. (2024)	Investigated cybercrime awareness among undergraduates. Found basic knowledge of identity theft, phishing, revenge pornography, cyber bullying, and hacking. Low awareness of cyber laws. Male students more aware than females. Recommended seminars and workshops. Noted limitations due to small sample and limited cybercrime types. Suggested larger future studies.
Kant, R. (2023).	Highlighted the importance of cybersecurity due to internet integration in daily life. No significant gender or academic course–based differences, but urban students were more aware. Many students unaware of malware, cyber harassment, phishing, and identity theft. Called for stronger education and regular awareness activities.
Choudhary, R.(2020)	Studied awareness among students in professional vs traditional courses. Professional course students had higher awareness. No major gender-based differences. Found average awareness overall. Recommended organized workshops and suggested government-set guidelines.
Meena et al. (2020)	Focused on the rising threat of cybercrime among youth and teenagers. Found limited knowledge on self-protection despite awareness of cybercrime. Suggested awareness campaigns, mandatory IT education, stronger rural regulations, and public-private cooperation. Recommended enhanced education, awareness, and legal frameworks.

Data Analysis and Interpretation

Table No. 01 Respondents' Level of Agreement with Statements Related to Cybercrime

No.	Statements	1	2	3	4	5	W	M	R
1	People with access to the internet are more likely to know about cybercrime.	33	44	23	--	--	190	1.90	**2**
2	Higher education helps people understand the risks and types of cybercrime	34	54	12	--	--	178	1.78	**1**
3	People living in urban areas are more likely to be informed about cybercrime than those in rural areas.	31	50	16	03	--	191	1.91	**3**
4	Access to technology plays a significant role in awareness about cybercrime.	29	50	18	03	--	195	1.95	**4**
Overall		**127**	**198**	**69**	**06**	--	--	**1.89**	---

Source: Survey data

The respondents' level of agreement with statements related to cybercrime collected from a 5-point Likert- type scale with the range of level as Strongly agree (1), agree (2), Neutral (3), disagree (4) and Strongly Disagree (5). 'W' stands for weighted sum, 'M' stands for Mean and 'R' stands for Rank.

The data reflects how respondents perceive different factors contributing to cybercrime awareness, based on a 5-point Likert scale. The lower the mean score, the stronger the agreement with the statement.

Statement 2: "Higher education helps people understand the risks and types of cybercrime" (Mean = 1.78, Rank = 1). This statement received the strongest agreement among respondents. It indicates that education is perceived as the most influential factor in helping individuals understand and recognize cybercrime. Respondents believe that as educational levels rise, so does awareness of cybercrime threats and preventive measures.

Statement 1: "People with access to the internet are more likely to know about cybercrime" (Mean = 1.90, Rank = 2). This shows that respondents agree that internet access plays a major role in increasing exposure to information about cybercrime. Access to online resources appears to significantly contribute to knowledge and awareness.

Statement 3: "People living in urban areas are more likely to be informed about cybercrime than those in rural areas" (Mean = 1.91, Rank = 3). This suggests a moderate agreement, indicating that location (urban vs. rural) may influence awareness levels. Respondents perceive that urban populations tend to have better access to information, education, and technology—factors that can boost cybercrime awareness.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Statement 4: "Access to technology plays a significant role in awareness about cybercrime" (Mean = 1.95, Rank = 4). Although still agreed upon, this statement received the highest mean score, suggesting slightly lower agreement relative to other factors. This could imply that while access to technology is important, respondents see education and internet access as more direct drivers of cybercrime awareness.

Table No. 02 Respondents' Opinion on Cyber Security Awareness and Online Safety Measures

No.	Statements	1	2	3	4	5	W	M	R
1.	Cyber security is important for protecting personal information online.	49	42	8	1	--	161	1.61	**1**
2.	I regularly use strong passwords to protect my online accounts.	31	60	9	--	--	178	1.78	**3**
3.	I believe that cyber security is important for protecting my personal data from being misused.	47	39	14	--	--	167	1.67	**2**
4.	I feel confident in my ability to recognize and avoid online security threats.	21	60	16	3	--	201	2.01	**5**
5.	I think cyber security is something that everyone should be aware of, not just experts.	37	47	14	2	--	181	1.81	**4**
Overall			**185**	**248**	**61**	**06**	**--**	**--**	**8.88**

Source: Survey data

The respondents' opinion on cyber security awareness and online safety measures collected from a 5-point Likert- type scale with the range of level as Strongly agree (1), agree (2), Neutral (3), disagree (4) and Strongly Disagree (5).

The data reflects respondents' opinion on cyber security awareness and data security measures, based on a 5-point Likert scale. The lower the mean score, the stronger the agreement with the statement.

Statement 1: "Cyber security is important for protecting personal information online" (Mean = 1.61, Rank = 1). This statement received highest rank, which indicates that respondents have high level of awareness regarding the need for cyber security in protecting their personal information in online.

Statement 3: " I believe that cyber security is important for protecting my personal data from being misused" (Mean = 1.67, Rank = 2). This indicate that people understand the risk of data being misused. This also indicates the respondents trust security measure tools in protecting their information.

Statement 2: "I regularly use strong passwords to protect my online accounts" (Mean = 1.78, Rank = 3). This shows that majority of respondents take online safety measures by using strong passwords. It reflects good security habits among respondents.

Statement 5: "I think cyber security is something that everyone should be aware of, not just experts." (Mean = 1.81, Rank = 4). This indicates that the respondents believe that cybersecurity is not just for experts, but it should be common knowledge among all. This statement is rank indicates that people still view technical domain, highlights the need of initiatives to be taken to raise cyber security awareness and motivate more individuals to take cyber security seriously.

Statement 4: "I feel confident in my ability to recognize and avoid online security threats " (Mean = 2.01, Rank = 5). Among all other statements this statement ranked the lowest, showing that respondents lack confidence and ability in detecting and avoiding threats. It indicates a gap in the knowledge and skill of the respondents about cyber security. Even if they value cyber security, they feel that they are not well equipped to handle real-world threats. This highlights the necessity of practical awareness training and workshops to build digital literacy and threat recognition skills among people.

IV. Major Findings

- 100% students responded that they are familiar with the term cybercrime.
- 100% of students agreed (Yes) that cybercrime is a growing problem.
- The statement "Higher education helps people understand the risks and types of cybercrime" (Mean = 1.78) ranked first. This indicates that the majority of respondents believe that higher education helps people understand the risks and types of cybercrime.
- The majority of students (96%) responded that they are familiar with the term cyber security.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

- The statement "Cyber security is important for protecting personal information online" (Mean = 1.61) ranked first. This indicates that the majority of respondents believe that cyber security is important for protecting personal information online.
- Majority of 80% of students responded that they avoid public Wi-Fi for sensitive activities to secure online information.
- A majority of 92% of students responded that they possess the knowledge to recognise secure websites.
- A majority of 95% students responded that people should be more careful about the information they share online. A majority of 73% of students responded that they use antivirus or security software.
- Majority of 53% of students responded that social media campaigns are effective strategies for cybercrime awareness.
- The statement “There should be more educational programs in schools and colleges about cybercrime and online safety” (Mean = 1.71) ranked first. This indicates that the majority of respondents believe that there should be more educational programs in schools and colleges about cybercrime and online safety.
- Majority of 98% of students responded that there is a need for increased government action to prevent cybercrime.

Recommendations

- It would be better to familiarize basic cybersecurity modules as part of ICT or general awareness subjects in school and colleges to educate students about safe internet practices, password hygiene, phishing, and data privacy.
- More awareness campaigns by government bodies and NGOs targeted at students, particularly in rural or economically weaker areas helps in preventing cyber risks.
- Parents and teachers should be informed about cybersecurity issues so they can guide and support students in developing safe online habits.

V. Conclusion

The study highlights that students in Dakshina Kannada District are more engaged with digital platforms. Although still their knowledge regarding cybercrime and their cyber security practices remain insufficient to save themselves from potential risks. Many students lack essential knowledge about cyber threats such as safe browsing habits, and data protection measures etc., which creates concern in this digital era. It is also observed that socioeconomic factors and prior exposure are the factors which influence their level of awareness regarding cyber incidents. This information helps educational institutions, policymakers, and community organizations to implement structured cyber security education and awareness programs. These initiatives promote digital literacy and encourage responsible online behaviour among students which can significantly help in reducing students' vulnerability to cyber threats and build a more secure online environment for the youth.

Reference

1. Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering (IJECE), 12(1), 572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584
2. Sani, K. M., Hassan, M. A., Saidu, M., Kabiru, S., & Tata, U. D. (2024). Investigating Undergraduate Students Levels of Cybercrime Awareness: A Study of Northwest University Sokoto, Sokoto State, Nigeria. International Journal of Social Sciences & Educational Studies, 12(1), 19-39.
3. Kant, R. (2023). Cyber-security awareness in India: How much students of higher education are aware ? GESJ: Education Science and Psychology, 2(67). ISSN 1512-1801.
4. Choudhary, M. (2020). Cyber crime awareness among higher education students from Haryana with respect to various demographical variables. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(7). ISSN 1567-214X.
5. Meena, Y., Sankhla, M. S., Mohril, S., & Kumar, R. (2020). Cybercrime: Youth awareness survey in Delhi NCR, India. Forensic Research & Criminology International Journal, 8(5). https://doi.org/10.15406/frcij.2020.08.00309
6. Sethi, A., & Dutta, S. (2021). Cybersecurity awareness among students: A study. International Journal of Computer Applications, 183(23), 1-6. https://doi.org/10.5120/ijca2021921757
7. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees’ cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.050
8. Algarni, A., Xu, Y., & Chan, T. (2015). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. European Journal of Information Systems, 26(6), 661–687. https://doi.org/10.1057/ejis.2015.3.