ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

DOI:10.21474/IJAR01/20957
DOI URL: http://dx.doi.org/10.21474/IJAR01/20957

RESEARCH ARTICLE

AWARENESS, THREATS AND PERCEPTION OF CYBER SECURITY

Dr. Rejani R. Nair
1. Assistant Professor, Govt. Arts College, Thycaud, Tvpm.

Manuscript Info

Manuscript History
Received: 27 March 2025
Final Accepted: 30 April 2025
Published: May 2025

Key words: -
Cyber Security, Cyber Security Awareness, Cyber Security Threat, Cyber Security Perception

Abstract

With the rapid advancement of modern technology, online education has become more accessible than ever, enabling learners to receive the same high-quality experience and outcomes as traditional education through a virtual platform. However, with these advancements comes an expanded threat from cyber criminals. Computer security, cyber security or information technology security is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide. Cyber security is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. It is more important than ever to keep yourself safe. Malicious cyber activity affects students in a variety of ways, typically in the form of malware and scams. As students join classes using their personal computers and home wi-fi networks, the number of potential attack vectors has rapidly proliferated. The study attempts to find out the cyber security awareness among college students. It has also put some effort into identifying the level of awareness, and the perception of students regarding cyber security along with the measure of social media influence that cyber security plays in their daily lives.

Introduction: -

The cyber security industry is rapidly growing every day. Even with increased attention to protecting electronic information, there is ample reason for businesses, organizations, and the public to be concerned. More malware is being launched than ever before.

Cybersecurity is now a global priority as cybercrime and digital threats grow in frequency and complexity. One of the major obstacles to preventing cybercrime is the shortage of cybersecurity professionals and the lack of new talent entering the industry. In India, there is a high level of digital illiteracy because it is a country of towns and villages. Cyber security and crimes are the major threats and challenges all over the globe and digital India is no exception. Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes**.**It is the protection of internet-connected systems

Corresponding Author: - Dr. Rejani R. Nair
Address**: -** Assistant Professor, Govt. Arts College, Thycaud, Tvpm.

such as hardware, software and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centres and other computerized systems.

The topic of cyber security should be talked about more often in today's society. Students are spending more time online than ever before and are interacting online from a younger age. For many young people, the internet is a central part of their daily lives. They go online to learn, relax, have fun, share interests, access services and connect with friends, family, and online communities. Cybersecurity education provides students with the knowledge and skills they need to stay safe in online environments. It involves acknowledging the benefits and opportunities offered by the online world while understanding the risks and avoiding potential harms. Students need ongoing support to help them care for themselves and others in the online environment.

Objectives:-

1. To identify the level of basic cyber security awareness among students.
2. To determine the types of cyber security threats faced by students.
3. To assess students' perception regarding cyber security.

Methodology: -

This study used a quantitative approach in designing the questionnaire-based survey to collect data through outline method. The questions were organized to obtain the level of cyber security awareness level among the targeted participants. The study focused on college students of Thiruvananthapuram District. The sampling technique used for this study was convenient sampling. The main tools for data collection were questionnaires and an online survey was also used. Based on the above objectives the questions were drafted. This study was based on primary data and secondary data. The primary data is collected directly from 107 students. The secondary collected were from other journals, articles, newspapers, websites and other research papers.

Reviewof Literature: -

Most of the studies in the literature have revealed the fact that there is a lack of knowledge about cyber security in the younger generation. Some studies have also stated that even if the participants have the knowledge that is not enough to protect them from cyber-attacks. Erendor and Yildirim (2022) in their work "Cyber Security Awareness in Online Education: A Case Study Analysis", opined that their research study showed that although a huge number of cyber-attacks are occurring around the world, students didn't have any knowledge about cyber security and the effects of cyber-attacks overall. It has been determined that students have weak cyber security awareness. But according to Raju and et.al (2022) in their work "Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution", they concluded that their descriptive analysis showed that many students have awareness and knowledge of cyber security, cyber-attacks and cyberbullying. Elradi and et.al (2020) in their work "Cyber Security Awareness among College Students and Faculty Members in Sudanese College" states that all the participants had a fairly low level of cyber security awareness and their defensive attitude was considerably weak and didn't protect them either individually or at the institution level. But Mutunhu and et.al (2022) in their paper "Cyber Security Awareness and Education" have established that students at universities do have the prerequisite knowledge and understanding of the importance of cyber security principles, and their practical application in their day-to-day activities, and are not aware of how to protect their data. They recommended that universities should implement comprehensive awareness and education programs on cyber security awareness. Bhatnagar and Pry (2020) in their work "Students Attitudes, Awareness and Perceptions of Personal Privacy and Cyber Security in the Use of Social Media: An Initial Study", found that students are aware of privacy and security risks in the use of social media platforms and do value and suggest additional training in this domain. Today technology has provided many ways where a person can communicate with another at the same or different destination, this technology also opens a way for a cybercriminal to attack or hack certain person's information or personal data. Kaur and Kumar (2022) have revealed in their work "The Recent Trends in Cyber Security" that the endangerment of wireless communication technology and systems from various cyber-attacks is the cause detriment not only to private enterprises but also to Government organizations as well. Stevens and et.al (2022) conducted a study on "Cyber Stalking, Cyber Harassment and Adult Mental Health: A Systematic Review" and concluded that as internet use increases, there is a growing risk of online harms, including cyber stalking and cyber harassment. Their research highlighted the need to devise practical solutions to tackle and minimize this victimization. Mutunhu and et.al (2022) in their article opined that Internet-related attacks have become prevalent and are expected to increase as the reliance on the Internet also increases. Alharbi and Tasaddiq (2021) according to their study "Assessment of Cyber Security Awareness among

Students of Majmaah University" found that new types of cyber security threats that typically result in data loss and information misuse have emerged simultaneously. Maintaining data privacy in complex systems is important and necessary, particularly in organizations where the vast majority of individuals interact with these standard systems. Students engage in data breaches and digital misconduct due to the lack of knowledge and awareness of cyber security and the consequences of cybercrime. Shaikh and et.al (2020) in their article "Cyber Bullying: A Systematic Literature Review to Identify the Factors Impelling University Students Towards Cyber Bullying" explained that with the increased access to the internet, technology and social media, the problem of cyberbullying has been on the rise. Rahman and et.al (2020) in their paper "Cyber Security Education in Schools" highlight that despite the fact that the Internet has positively impacted people's lives, there are negative issues related to the use of the Internet. Cases like cyberbullying, online fraud, racial abuse, pornography and gambling have increased tremendously due to the lack of awareness among internet users to protect themselves from being victims of these acts. They also said that the past research revealed that the level of awareness among internet users is still low or moderate.

Cybersecurity is a major issue that has affected many online users in the modern world. Alqahtani (2022) tried to explain in his study "Cyber Security" that one of the essential stages in increasing cyber security is implementing an effective security awareness program. Based on the research conducted, knowledge of password security, browser security and social media activities significantly influences cyber security awareness among students. Ulven and Wangen (2022) in their paper "A Systematic Review of Cyber Security Risks in Higher Education" said that the empirical research on cyber security risks in higher education is scarce. Zwilling and et.al (2022) concluded in their study "Cyber Security Awareness and Education, that while internet users possess adequate awareness of cyber threats, they tend to implement only minimal and relatively basic protective measures. The findings further revealed a higher level of cyber knowledge is positively associated with cyber awareness, regardless of differences in respondents' countries or gender. Finally, it highlighted cross-country differences that influence the interplay between cyber awareness, knowledge, and behavior.

DataAnalysisAndInterpretation

Table No. 1:-Demographic Variables

Demographic Variables		
Gender	**Number of Respondents**	**Percentage**
Male	65	60.7
Female	42	39.3
Age	**Number of Respondents**	**Percentage**
18-20	48	44.9
21-23	56	52.30
24-26	3	2.8
Years of use of internet	**Number of Respondents**	**Percentage**
Less than 1 year	0	0
1 to 3 years	18	16.8
3 to 5 years	26	23.4
More than 5 years	63	58.9
Hours of use of internet per day	**Number of Respondents**	**Percentage**
Less than 1 hour a day	0	0
1 to 2 hr	18	15.9
2 to 4 hr	39	34.6
More than 4 hrs	50	45.8
Source of information on cyber security	**Number of Respondents**	**Percentage**
Newspaper	6	5.6
Social media	52	48.6
Television/Radio	8	7.5
Awareness classesconducted	36	32.7
Others	6	5.6

Source: Primary Data

Interpretation

From the above table, the majority of the respondents are male students (60.7 per cent) and female respondents 39.3 per cent. The majority of the students who attended this questionnaire belong to the age group of 21-23 years (52.3 per cent), and the rest were 44.9 per cent from the age group of 18-20 years and 2.8 per cent between 24-26yrs. The majority of the respondents were using the internet for more than 5 years (58.9 per cent), only 23.4 per cent were using the internet for a period between 3 to 5 years and 16.8 per cent for 1 to 3 years. It can be assumed that the majority of the respondents were familiar with the usage of the internet for a long period. Most of the respondents were using the internet more than hours a day (45.8 per cent), 34.6 per cent used the internet for some time of 2 to 4 hrs a day and the rest 15.9 per cent used it for a period of 1 to 2 hrs a day. The majority of the respondents heard the term cyber security from social media rather than any other sources (48.6 per cent),5.6 per cent heard from the newspaper, 7.5 per cent from awareness classes conducted by schools/colleges, and 5.6 per cent from other sources. This means social media has a greater importance in promoting cyber security.

Table No.2: -Basic Cyber Security Awareness

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I can identify latest online scams.	32	42	29	2	2
I am willing to meet internet friends in person.	8	29	35	22	13
I trust stranger's identity information given on the internet.	4	3	29	34	37
I'm willing to share personal information online.	4	4	23	30	46
Never change password.	5	14	30	17	41
Use a same password for different applications.	8	20	29	25	25
Aware about the dangers of clicking on a spam link or downloading an infected attachment.	47	27	19	5	9
Verify the identity or authorization of someone before talking on any issues	35	37	25	6	4
Do not reveal any kind of confidential information under any circumstances.	51	24	16	7	9
My device contains antivirus software.	32	35	25	11	4
Updates the antivirus software regularly	39	27	28	7	6
The two-factor authentication is important.	58	25	20	3	1

Source: Primary Data

Interpretation

The above table shows the basic level of cyber security awareness among the respondents. It is found that the majority of the students can identify the latest online scams. 54.2 per cent strongly agree that the two-factor authentication is important. 47.6 per cent of the students strongly agree not to reveal any kind of confidential information under any circumstances. 34.57 per cent agree that they verify the identity or authorization of someone before talking about any issues. The majority are aware of the dangers of clicking on a spam link. 23.36 per cent disagree that they use the same password for different applications. 42.9 per cent of the students strongly disagree that they are willing to share personal information online and 38.3 per cent strongly disagree that they never change passwords. Thus, we can conclude that the majority of the students have basic cyber security awareness.

Table No.3: -Awareness on Threats Related to Cyber Security

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I am aware of security threats	45	47	13	1	1
I know how to alleviate or lessen threats.	24	42	34	6	1
Remove personal, confidential or sensitive data before giving the PC to be repaired or replaced.	42	41	16	4	4
Check antivirus software at least every week or set it for	33	42	25	5	2

automatic updates.					
Accepts unknown persons in social media.	7	21	26	27	26
Received phishing emails/messages in any form.	7	27	33	26	14
An interesting subject line makes one curious to open an email attachment.	11	26	35	17	18
I am willing to download files and documents from unsecure sites.	6	12	30	22	37
Responds to SMS containing contests that involve huge sums of money.	9	12	15	17	54
Installation of free software from untrusted source	7	13	19	20	48
Willing to deposit money requested by online friends.	8	10	15	16	58
Knows how to deal with a hacked device.	8	27	33	18	21

Source: Primary Data

Interpretation

The above table shows the awareness of threats related to cyber security among college students. 42.05 per cent of the students strongly agree that they are aware of security threats. 39.25 per cent strongly agree that they remove personal, confidential or sensitive data before giving the PC to be repaired or replaced. 39.25 per cent agree that they know how to alleviate or lessen the threats and check antivirus software at least every week or set it for automatic updates. 54.20 per cent strongly disagree that they are willing to deposit money requested by online friends. 50.46 per cent strongly disagree that they respond to SMS containing contests that involve huge sums of money. 44.85 per cent strongly disagree that they are ready to install free software from an untrusted source. Many students opined that any kind of interesting subject line makes them curious to open an email attachment. So that they are vulnerable to phishing scams, data theft etc. At a glance, we can conclude that the majority of the respondents are aware of the threats related to cyber security and if any threat happens, they are capable of handling them.

Table No.4: -Perceptions Regarding Cyber Security

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Share private photos or information via social media because it is safe to do so.	10	13	17	21	46
It is safe to use publicWi-Fi	7	26	43	14	17
A strict law reduces cyber-crime.	41	34	23	6	3
Government supervises the internet.	8	35	52	8	4
For rewards, people spend more in online games.	26	45	25	4	7
Online advertisements easily influence people.	36	54	15	2	0
Payment through links is secure.	12	10	37	25	23
Orders are placed in apps/pages without checking its authenticity.	11	25	32	17	22
Sharing OTP/any other sensitive information with others is secure.	9	12	17	14	55

Source: Primary Data

Interpretation

The above table shows the various perceptions of students regarding cyber security. 38.3 per cent of the students strongly agree that a strict law reduces cyber-crime. 54.4 per cent agree that online advertisements easily influence people. 42.05 per cent agree that for rewards, people spend more in online games. Many of the students have neutral opinions regarding the safety of using Public Wi-Fi. 23.36 per cent disagree that payment through links is secure. 51.4 per cent strongly disagree that sharing OTP/any other sensitive information with others is secure.

Hypothesis 1:

H0: There is significant difference between basic cyber security awareness among students based on Gender

H1: There is no significant difference between basic cyber security awareness among students based on Gender

Table No.5: -Independent Sample T-test

Cyber Security Awareness	Gender	Mean	Median	SD	SE	Statistic	p- value
CSA 1	M	4.05	4.00	0.876	0.1384	0.8383	0.404
	F	3.90	4.00	0.877	0.1132		
CSA 2	M	3.23	3.00	1.143	0.1808	1.6969	0.093
	F	2.83	3.00	1.122	0.1449		
CSA 3	M	2.40	2.00	0.955	0.1511	2.3189	0.022
	F	1.92	2.00	1.062	0.1371		
CSA 4	M	2.23	2.00	1.050	0.1660	1.9256	0.057
	F	1.80	1.00	1.102	0.1422		
CSA 5	M	2.48	2.00	1.301	0.2056	1.2279	0.222
	F	2.17	2.00	1.181	0.1525		
CSA 6	M	2.80	3.00	1.137	0.1797	1.0060	0.317
	F	2.55	2.00	1.268	0.1637		
CSA 7	M	3.92	4.50	1.328	0.2100	-0.3682	0.713
	F	4.02	4.00	1.142	0.1475		
CSA 8	M	3.90	4.00	1.008	0.1593	-0.1590	0.874
	F	3.93	4.00	1.039	0.1342		
CSA 9	M	4.05	4.00	1.085	0.1715	0.3849	0.701
	F	3.95	4.50	1.383	0.1785		
CSA 10	M	3.77	4.00	1.121	0.1772	0.0376	0.970
	F	3.77	4.00	1.064	0.1373		
CSA 11	M	3.90	4.00	1.105	0.1747	0.2904	0.772
	F	3.83	4.00	1.137	0.1468		
CSA 12	M	4.25	5.00	0.927	0.1465	-0.4611	0.646
	F	4.33	5.00	0.857	0.1106		
CSA Overall Average	M	3.41	3.38	0.517	0.0817		
	F	3.25	3.25	0.512	0.0661	**1.5694**	**0.120**

Source: Primary Data

Interpretation

The above table shows basic cyber security awareness among students concerning gender and it has been analyzed using Independent Sample T-test. All of the p values are greater than 0.05 allowing rejecting the null hypothesis and accepting the alternative hypothesis. Thus, it can be concluded that there is no significant difference between basic cyber security awareness among students based on Gender.

Findings

Basic Cyber security awareness among Students

The respondents answered that they observe the news related to cyber security on social media or news. They agree that they can identify the latest online scams. The majority strongly disagree that they trust strangers' identity information given on the internet and that they are willing to share their personal information online. Some strongly disagree that they never change passwords. Most of them strongly agree that they were aware of the dangers of clicking on a spam link or downloading an infected attachment and agree to verify the identity or authorization of someone before talking about any issues. The majority strongly agree to not reveal any kind of confidential information under any circumstances. Mostly agree that their device contains antivirus software and strongly agree that they update their antivirus software regularly. The majority strongly agree that two-factor authentication is important.

Awareness on threats related to Cyber security

The majority of the respondents were aware of cyber security threats. They knew how to eliminate or lessen the threats and strongly agreed that they remove personal, confidential, or sensitive data before giving the PC to be repaired or replaced. The majority of the respondents do not accept unknown persons on social media. The respondents were neutral in their opinion that an interesting subject line makes them curious to open an email attachment. Most of the respondents are not willing to deposit money requested by online friends.

Perceptions Regarding Cyber security

The majority of the respondents are not willing to share private photos or information via social media as they know that it is not safe to do so. Most of them believe that a strict law reduces cybercrimes. Most of the students agree that for rewards, people spend more on online games, and online advertisements easily influence people. The majority strongly disagree that sharing OTP/ any other sensitive information with others is secure.

Suggestions: -

Cyber-attacks frequently occur as a result of outdated systems and software. Maintain a sturdy and up-to-date system to prevent this problem. The technique of defending computers, laptops, mobile phones, and tablets from harmful threats and online attacks is known as endpoint security which should be resorted to by individuals. Ensure that the best password policy is in place and followed. A smart password policy if strictly adhered will stop users from choosing passwords that are simple to guess and should lock accounts after a predetermined number of failed tries. Only download free software from reputable websites; otherwise, you risk experiencing various cyber issues. Only click on URLs you are familiar with and feel are secure. It could lead to device hacking by clicking on strange links.

Try to stay away from giving out information to strangers online. It leads to the hacking of the user's personal information and may result in numerous financial losses. Regularly check the account settings to make sure your device is safe from cyber-attacks. Hackers can utilize other public networks or build their own to steal peoples' information covertly. It is advised to avoid critical activities like online shopping or banking when using public Wi-Fi. Ensuring the websites you visit are secure or setting up a virtual private network are some of the ways to safeguard your device when utilizing public Wi-Fi. Viruses can slow down a device, delete or corrupt files, and designate hard drive failures as problems. Viruses are eliminated and removed by antivirus software before they may harm your gadgets. Antivirus software that protects against viruses may also stop spam, defend your device against hackers, safeguard your files and data, and provide security for the device.

Reference: -

1. Alharabi, T &Tassaddiq, A. (2021). “The Importance of Cyber security Education in School” “Assessment of Cyber Security Awareness among Students of Majmaah University”- Big Data and Cognitive Computing 5 (2), 23, 2021 https://www.mdpi.com/2504-2289/5/2/23
2. Alqahtani, M.A. (2022). “Factors affecting cyber security awareness among university students”, - Applied Sciences 12(5), 2589, 2022 https://www.mdpi.com/2076-3417/12/5/2589
3. Bhatnagar, N & Pry, M. (2020). “Student Attitudes, Awareness and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An initial Study”-Information Systems Education Journal 18(1), 48-58, 2020 https://files.eric.ed.gov/fulltext/ EJ1246231.pdf
4. Chasanah, B. R., &Candiwan, C. (2020). Analysis of College Students’ Cybersecurity Awareness in Indonesia. SISFORMA, 7(2), 49-57.https://journal.unika.ac.id/ index.php /sisforma/article/view/2706
5. Erendor, M.E & Yildrim, M. (2022). “Cyber Security Awareness in Online Education: A Case Study Analysis”- IEEE Access 10, 52319-52335, 2022. https://ieeexplore.ieee.org/ document /9766123
6. Kaur, J &Ramkumar KR. (2022). “The recent Trends in Cyber Security: A Review”, Journal of King Saud University- Computer and Information Sciences 34(8), 5766-5781, 2022 https://doi.org/10.1016/j.jksuci.2021.01.018.
7. Kovacevic, A., Putnik, N &Toskovic, O. (2020). Factors Related to Cyber Security Behavior. IEEE Access. Vol 8, 125140-125148. Digital Object Identifier 10.1109/ ACCESS. 2020.3007867
8. Mai, P.T & Tick, A. (2021). “Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam”- Acta PolytechnicaHungarica 18 (8), 67-89, 2021 DOI: 10.12700/APH.18.8.2021.8.4 https://www.researchgate.net /publication/354864771_
9. Mutunhu, B., Dube, S., Cube, N&Sibanda, S. (2022). “Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology” -Proceedings of the International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria, 5-7, 2022 https://ieomsociety.org › proceedings

10. Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. Kalpa Publications in Computing Volume 12, 2019, Pages 272–280 Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019. https://easychair.org/publications/paper/wVsR
11. Rahman, N.A.A., I Sairi, I.H., Zizi, N.A.M&Khalid, F. (2020). "The Importance of Cybersecurity Education in School"- International Journal of Information and Education Technology 10(5), 378-382, 2020https://www.researchgate.net/publication/340714158
12. Raju, R., Hidayah, N., Rahman, A & Ahmed, 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, 2022 https://myjms.mohe .gov.my/ index.php/AJUE/article/view/18967
13. Sheikh, F.B., Rehman, M &Amin, A. (2020). "Cyberbullying: A systematic literature review to identify the factors impelling university students towards cyberbullying"- IEEE Access 8, 148031-148051, 2020 https://ieeexplore.ieee.org/document/9163353
14. Stevens, F., Nurse, J, RC & Arief, B. (2021). "Cyber stalking, cyber harassment, and adult mental health: A systematic review"- Cyberpsychology, Behavior, and Social Networking, 24(6), 367-376, 2021 https://doi.org/10.1089/cyber.2020.0253
15. Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M &Choo K-K.R. (2020). "A Systematic Literature Review of Block chain Cyber security"- Digital Communications and Networks 6(2), 147-156, 2020 https:// www.sciencedirect.com/science/article/pii/S235286 4818301536
16. Ulven, B &Wangen, G. (2021). "A Systematic Review of Cybersecurity Risks in Higher Education"- Future Internet 13(2), 39, 2021 https://doi.org/10.3390/fi13020039
17. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F &Basim H.N. (2022). "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study"-Journal of Computer Information Systems 62 (1), 82-97, 2022 https://www.researchgate.net/ publication /339273589_