Journal of Community Development | E-ISSN. 2747-2760 | Volume: 4, Nomor 2, December, **2023**, *Page*: 139-156

Socializing the Impact: An Analysis of the Theory of Planned Behavior's Influence on Increasing University Students' Cybersecurity Awareness

Varsha Parikh[1], Mansi Nimbekar[2]

[1]Associate Professor, [2]Former Postgraduate Research Scholar
Department of Extension and Communication Faculty of Family and Community Sciences
The Maharaja Sayajirao University of Baroda, Vadodara 390002 Gujarat, India

varshaparikh-extcommphd@msubarod.ac.in

Abstract

DOI: https://doi.org/10.47134/comdev.v4i2.162
*Correspondensi: Varsha Parikh
Email: varshaparikh-extcommphd@msubarod.ac.in

Received: 17-11-2023
Accepted: 20-12-2023
Published: 26-12-2023

The study aimed to assess cybersecurity awareness among university students in Vadodara, India, using the Theory of Planned Behavior (TPB) framework. The study involved 242 students from selected universities, selected using a snowball sampling method. Data was collected through Google Forms and email, and the Statistical Package for the Social Sciences (SPSS) programme was used for statistical analysis. The majority of students were young (18-23 years old), with moderate internet usage and primary digital competency skills. Only 17% reported experiencing issues during cyber surfing. The study found that most students had low awareness, lower knowledge, and negative perceptions about cybersecurity. Most students followed unsafe cybersecurity practices and had a negative attitude towards cybersecurity. The study also examined the correlation between TPB constructs.

Keywords: *Cybersecurity, University students, Theory of planned behaviour, Digital competency, knowledge, self-perception, actual skills and behaviour, attitude*

I. INTRODUCTION

Nowadays, cyberspace is an integral part of existence, yet twenty years ago, this concept appeared like something out of science fiction. Cyberspace is the term used to describe the virtual environment or computer world made possible by the Internet. The internet, which comprises the “World Wide Web (www), User Network (USENET), and IRC (Internet Relay Chat)," is the greatest portion of cyberspace (Redmonster.In., 2022). Today, the usage of the internet penetrates every facet of life. In the twenty-first century, people spend a lot of time online, whether it is for work, school, fun, gaming, or any other reason.

The Internet and Mobile Association of India (IAMAI) and consulting firm Kantar predict that by 2025, there will be nearly 1 billion internet users in India. More than half of all online shoppers in the nation use social commerce platforms, which have enabled over 500 million digital transactions. Furthermore, by

2025, it is projected that half of all students will be enrolled in online courses. The aforementioned statistics highlight assures the security pressing necessity of augmenting cyber awareness campaigns and executing innovative endeavours to and durability of India's swiftly growing digital terrain. The public's awareness of cyberspace is being raised through events like National Cyber Security Awareness Month (NCSAM) and campaigns like "Cyber Swachhta Abhiyaan: Cyber Hygiene Campaign. “These initiatives, along with the establishment of organizations like the National Cyber Coordination Center and the Cyber Swachhta Kendra, show India's ongoing commitment to increasing cyber security awareness and readiness. Protecting the interests of the growing online population as the digital ecosystem grows, however, will require increased efforts from the government as well as from other stakeholders in order to prioritize and develop cutting-edge cyber awareness initiatives. (Pramshu, 2022, May 17).

Confidentiality, Integrity, and Availability (CIA) Triad - The three essentials for data protection are confidentiality, integrity, and availability; however, problems with any one of them may impact the other two. The CIA trio lays out the fundamentals of an efficient digital asset protection approach. It is a fundamental cybersecurity paradigm that provides the foundation for the creation of security regulations intended to safeguard data. These three key concepts of the CIA Triad are observed as follows: Information must be kept confidential so that only those with the proper authorization can access it. Integrity is connected to data reliability and validity. The data must be accurate, and any changes must be obvious. Accessibility is crucial since data is only useful if it is available.

University vulnerability to cyber threats and attacks at the global level and in India- Although almost every major industry confronts severe cybersecurity concerns, in the last two years, cyberattacks have increased in frequency against higher education institutions around the world, posing a severe threat to the security of scientific data and education. As there have been so many attacks on educational institutions lately, the industry is on high alert.

Significance of cyber security awareness- When the COVID-19 pandemic began, students wishing to advance their education without attending classes or training facilities paid close attention to online computing platforms. Nonetheless, this has attracted the unwanted attention of threat actors and advertisers hiding behind legitimate links, attachments, and websites. In addition, threat actors most frequently impersonated Zoom, Moodle, and Google Meet among other online learning platforms in the second half of 2021, according to Kaspersky, which reflects the importance of cybersecurity awareness amongst university staff and students in higher education institutions. To seek answers to the research questions, it was decided to conduct a research study on “Cybersecurity awareness among the university students of Vadodara, Gujarat, India in 2022–23 considering following objectives."

Objectives of the study : 1. To prepare the profile of the selected university students of the Vadodara; 2. To assess cybersecurity awareness using the Theory of Planned Behavior (TPB) constructs, viz., knowledge, self-perceptions, actual skills and behaviours, and attitude, among the selected university students of Vadodara; 3. To study the differences in the TPB constructs, viz., knowledge, self-perceptions, actual skills and behaviour, and attitude, among the selected university students of Vadodara concerning the selected variables; 4. To study the co-relations within the TPB constructs, viz., knowledge, self-perceptions, actual skills and behaviours, and attitude, in the context of cybersecurity awareness.

Null Hypothesis of the study : There will be no co-relation within the TPB constructs, viz., knowledge, self-perceptions, actual skills and behaviours, and attitude toward cybersecurity awareness.

II. METHOD

Icek Ajzen developed the Theory of Planned Behavior (TPB) in an attempt to predict human behaviour (Ajzen, 1991). It is a psychological theory that connects beliefs and behaviours. According to the theory, an individual's behavioural intentions are shaped by three key factors: attitude, subjective norms, and perceived behavioural control. Keeping in mind the operational definition of cybersecurity awareness in the present study, the most fitting Theory of Planned Behavior (TPB) framework used by Chandarman R. and Van Niekerk, B. (2017) in their study entitled “Students’ Cybersecurity Awareness at a Private Tertiary Educational Institution” has been adapted in the present study. Conceptual framework of the study is as follows.

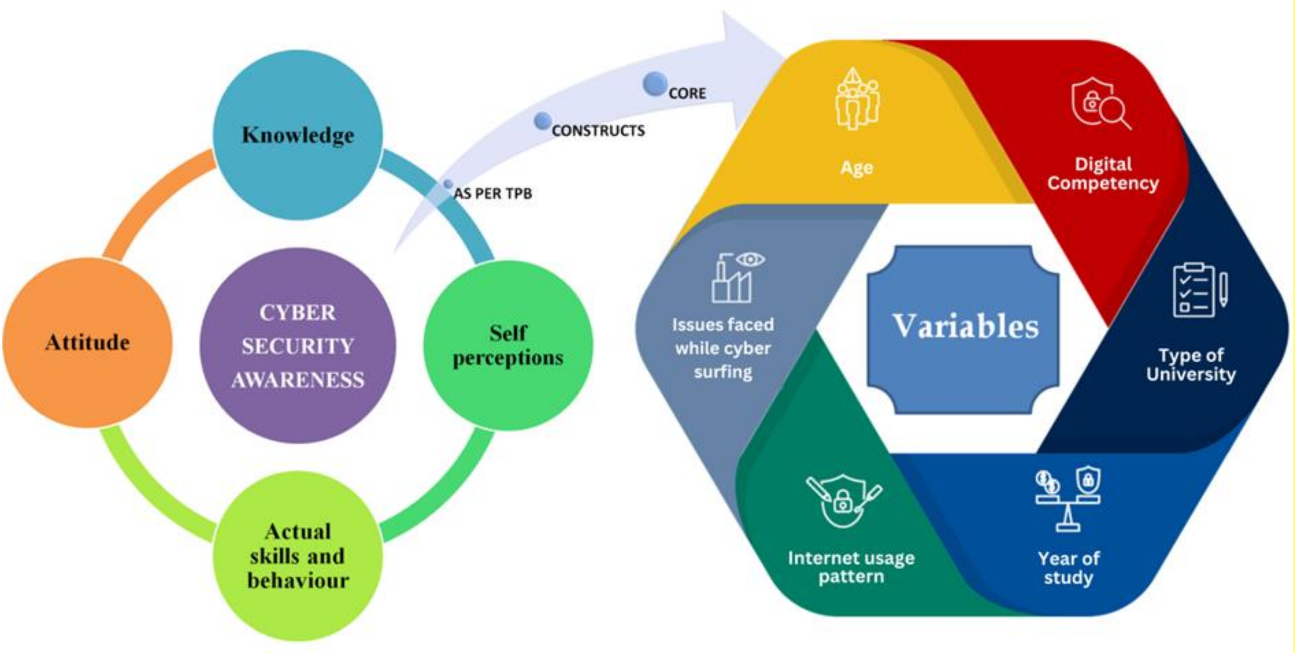

Figure 1. Conceptual Framework of the Study

This methodology section outlines the procedures utilised to carry out the present study:

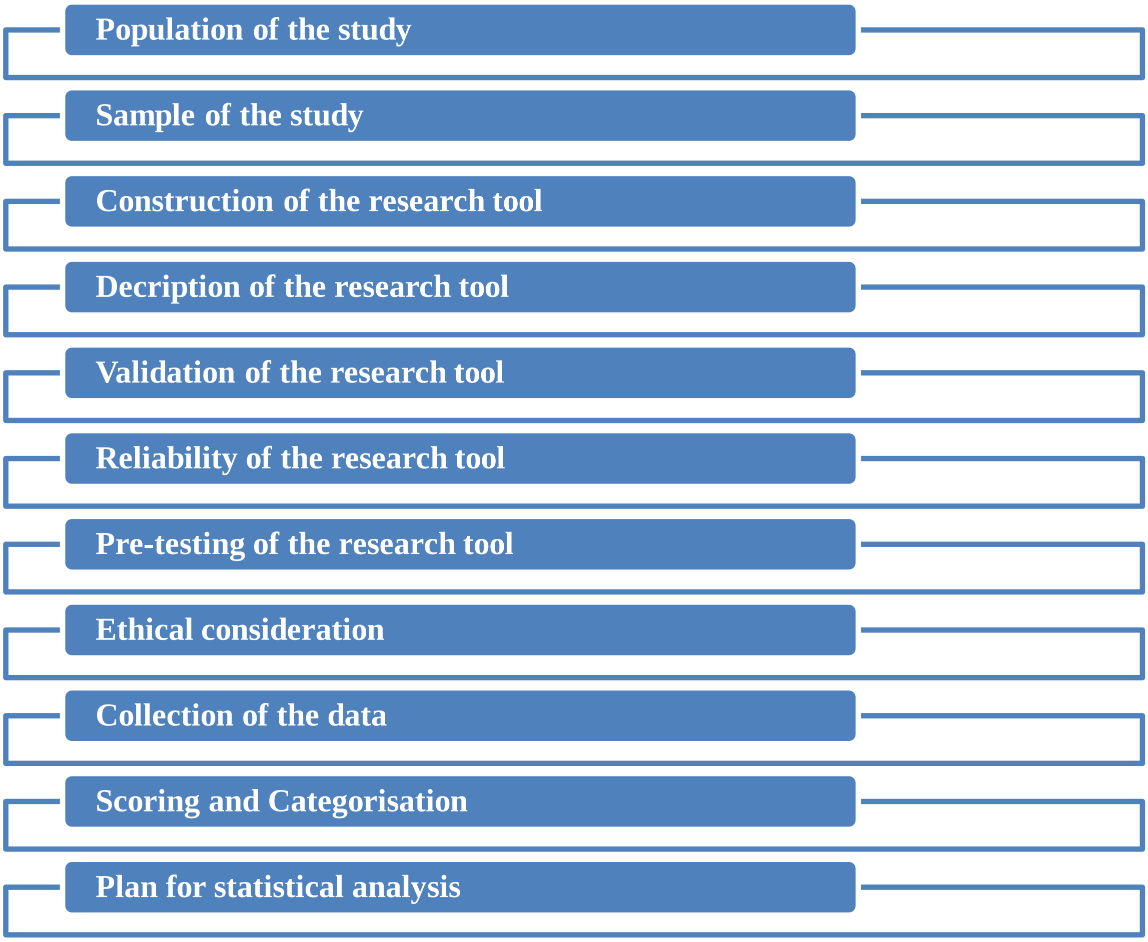
Population of the study
Sample of the study
Construction of the research tool
Decription of the research tool
Validation of the research tool
Reliability of the research tool
Pre-testing of the research tool
Ethical consideration
Collection of the data
Scoring and Categorisation
Plan for statistical analysis

Figure 2. Methodology

2.1 Population of the study

The population of this study includes students from selected government and private universities accredited by the University Grants Commission (UGC) of Vadodara, Gujarat, India.

2.2 Sample of the study

The sample of this study is 242 students from government universities, i.e., Maharaja Sayajirao University of Baroda, and private universities, viz., Parul University of Vadodara.

2.3 Construction of the Research Tool

The researcher developed a structured questionnaire tool in the English language regarding cybersecurity awareness, which comprised background information, internet usage patterns, a scale for digital competency, a knowledge test, a self-perception scale, actual skill, and behaviour, as well as an attitude scale, to gather information for the present study's data collection. A Google form was also created for the data collection.

The tool was developed after reviewing relevant literature, books, and websites, as well as narratives from real-life incidents involving people regarding cyber security awareness.

2.4 Description of the tool

A questionnaire with seven (7) sections has been prepared to study cybersecurity awareness among selected university students in Vadodara. The questionnaire primarily consisted of two components:

Table 1. Research Tool Sections and Response System

Section	Parameters	Total No. of items	Tools	Response system
Section A	Demographic Profile of the respondents	9	Multiple choice questions	Selecting an appropriate option from a given list which best applies to the respondent and wherever it is instructed, fill in the blank with the right response.
Section B	Part A - Internet Usage Pattern	9	Multiple choice questions	Selecting an appropriate option from a given list which best applies to the respondent and wherever it is instructed, fill in the blank with the right response.
	Part B - Digital Competency	15	Interval scale	3 Point rating scale (Adapted from http://eprints.bournemouth.ac.uk/23477/)
Section B	Part C - Issues encountered during cyber surfing	7	Multiple choice questions & open-ended questions	Selecting an appropriate option from a given list which best applies to the respondent and wherever it is instructed, fill in the blank with the right response.
Section C	Student's cybersecurity knowledge	15	Multiple choice questions	Selecting an appropriate option from a given list which best applies to the respondent. One Correct Answer
Section D	Student's self-perception of cybersecurity skills	14	Interval scale	3 Point rating scale
Section E	Student's actual cybersecurity skills and behavior	10	Multiple choice questions	Selecting an appropriate option from a given list which best applies to the respondent. One Correct Answer
Section F	Student's cybersecurity Attitude	14	Interval scale	3 Point rating scale

2.5 Validity and Reliability of the research tool

The tool was given to seven experts, to assess the effectiveness of content based on relevance, logical order, use of language, and appropriateness of response systems. To assure internal and external consistency, the tool's reliability was assessed. The reliability of the questionnaire was evaluated with the test-retest method. The result of the reliability test was found to be 0.851.

Each of the TPB framework's constructs was examined for internal consistency using Cronbach's Alpha coefficient test. For high internal consistency the score must be over .7 and, in the present study, $\alpha = 0.914$, which shows the questionnaire is reliable and is significant and acceptable for further research.

2.6 Ethical Approval of the Study by IECHR Committee

The study was presented to IECHR Committee for ethical approval and was approved by the ethical committee with ethical approval number IECHR/FCSc/M.Sc./2022/18.

2.7 Data Collection

To study cyber security awareness among the university students of Vadodara, Gujarat the data was collected from 242 university students aged between 18-28 years of Vadodara by the researcher in person as well as using an online platform, i.e. Google form. The link for Google form was shared with the respondents' using emails and WhatsApp. 139 samples were collected through online mode, whereas 103 were collected offline mode. In total, 242 amongst which 116 male students and 126 female students submitted valid responses. Questionnaires which found incomplete, ambiguous were dismissed.

2.8 Statistical Analysis of the Data

Table 2. Different Statistical Measure Used for the Analysis of The Data.

Sr. No.	Purpose	Statistical measures
1	Demographic profile of the students	Percentages
2.	Overall knowledge, Self-perceptions, actual skills and behavior, attitude (as per TPB framework) for Cybersecurity awareness of the students	Percentages
3.	Differences in the knowledge, self-perceptions, actual skills and behavior and attitude (as per TPB framework) regarding cybersecurity awareness of the students	Mann-Whitney U, Kruskal Wallis Test, t-test and ANOVA
4	Differences in the co-relation within TPB constructs viz, knowledge, self-perception, actual cybersecurity skills and behavior and attitude	Correlation

2.11 Formula used for Correlation base.

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

Where,

r = Pearson Correlation Coefficient

x_i = x variable samples y_i = y variable sample

$\bar{x}$ = mean of values in x variable $\bar{y}$ =mean of values in y variable

Table 3. Categorization of Scores in Correlation

Correlation	Range
Not correlated	< 0.1
Weak	0.1 – 0.2
Moderate	0.2 – 0.5
Strong	> 0.5

III. RESULTS AND DISCUSSION

3.1. Demographic profile of the respondents

Table 4. Variable-Wise Frequency and Percentage Distribution of the Selected University Students of the Vadodara (n=242)

Sr. No.	Variables	Categories		Frequency (n)	Percentage (%)
1	Age	Young(18-23yrs)		156	64.5
		Old(24-29yrs)		86	35.5
2	Gender	Male		116	47.9
		Female		126	52.1
3	Type of University	Government		106	43.8
		Private		136	56.2
4	Year of study	Undergraduate	First year	47	20.0
			Second year	66	27.0
			Third year	35	14.4
			Fourth year	20	8.0
			Fifth year	1	0.4
		Post-graduate	First year	31	13.0
			Second year	42	17.0

Demographic details of the respondents were as follows:

- The majority of the students, i.e., 64.5%, were in the category of young students (18–23 years).
- Little more than half of the respondents, i.e., 52.1%, were female.
- More than half of the respondents, i.e., 56.2%, were studying at private universities, and the rest were from government universities.
- The high majority, i.e., 70% of the respondents, were undergraduate students in their first to fifth years of study (20%, 27%, 15%, 8%, and 0.4%, respectively). The remaining 30% of the respondents were postgraduate students in their first and second years of study.

Table 5. Frequency and Percentage Distribution of the Selected University Students of the Vadodara According to the Variables Internet Usage Pattern and Digital Competency Level (n=242)

Sr. No.	Variables	Categories	Frequency (n)	Percentage (%)
5	**Internet usage pattern**	**Moderate users**	**147**	**60.7**
		Heavy users	95	39.3
6	Digital competency	Beginner	171	70.7
		Intermediate	71	29.3

- The majority of the respondents, i.e., 60.7%, were moderate internet users.
- The high majority (70.7%) of the respondents were found with a primary level of digital competency skills i.e., beginner, followed by 29.3% of them with advanced digital competency skills, i.e., intermediate.

Table 6. Frequency and Percentage Distribution of the Selected University Students of the Vadodara According to Cyber Victimization (n=242)

Sr. No.	Variable	Category	Frequency (n)	Percentage (%)
7	Cyber victimization	Yes	40	16.5
		No	202	83.5

- The high majority of the respondents, i.e., 83%, had not fallen victim to online crimes, whereas 17% of respondents had fallen victim to online crime.
- 17% of the respondents responded that they have faced issues during cyber surfing. Among them, 35% and 30% reported issues related to phishing emails and malware, respectively.

3.2. Theory of planned behaviour: core constructs

Table 7. Co-relations Between TPB Constructs Viz, Knowledge, Self-Perception, Actual Cybersecurity Skills and Behaviour and Attitude for Cybersecurity (n=242)

Correlation within TPB Constructs viz Knowledge, Self-perceptions, Actual skills and behavior and Attitude					
		Knowledge score	**Self-perception score**	**Actual cybersecurity skills and behavior score**	**Attitude score**
Knowledge score	Pearson Correlation	1	.401**	.345**	.399**
	Sig. (2-tailed)	-	0	0	0
	N	242	242	242	242
Self-perception score	Pearson Correlation	.401**	1	.327**	**.625****
	Sig. (2-tailed)	0	-	0	0

	N	242	242	242	242
Actual cybersecurity skills and behavior score	Pearson Correlation	.345**	.327**	1	.314**
	Sig. (2-tailed)	0	0	-	0
	N	242	242	242	242
Attitude score	Pearson Correlation	.399**	.625**	.314**	1
	Sig. (2-tailed)	0	0	0	-
	N	242	242	242	242
**Correlation is significant at the 0.01 level (2 tailed)					

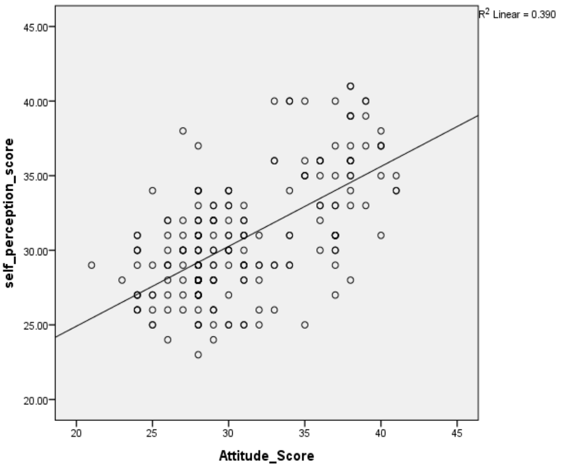

Figure 1. Co-relations between self-perception, and attitude for cybersecurity

a. CSA and overall knowledge of the respondents

- More than half (53.7%) of the respondents had less knowledge of cybersecurity, followed by less than half (46.3%) of them knowing cybersecurity.

Differences in the knowledge of the selected university students of Vadodara regarding cybersecurity concerning the selected variables.

- There was a significant difference found in the respondents' knowledge regarding cybersecurity in relation to the variable, viz, digital competency.
- There were no significant differences in the cybersecurity knowledge of the respondents in relation to their age, gender, type of university, internet usage pattern, and year of study.

b. CSA and overall Self-perceptions of cybersecurity skills of the respondents

- The majority of the respondents, i.e., 67.4%, had unfavourable perceptions, whereas one-third of the respondents, i.e., 32.6% had favourable perceptions.

Differences in self-perception of the selected university students of Vadodara regarding cybersecurity skills in relation to the selected variables

- There were significant differences found in the self-perception regarding the cybersecurity skills of the respondents in relation to the variables, viz., gender, type of university, and internet usage pattern.
- There were no significant differences found in the self-perception of cybersecurity skills of the respondents in relation to variables viz. their age, digital competency, and year of study.

c. CSA and overall Actual skills and behaviour of the respondents

- Almost the majority of the respondents, i.e., 58.3%, used to follow unsafe cybersecurity skills and behaviours in the real world, followed by little more than one-third, i.e., 41.7% of them, following safe cybersecurity skills and behaviours.

Differences in the actual skills and behaviour of the selected university students of Vadodara regarding cybersecurity in relation to the selected variables

- There were significant differences found in the actual cybersecurity skills and behaviour of the respondents in relation to the variables viz, age, type of university, and digital competency.
- There were no significant differences found in the actual cybersecurity skills and behaviour of the respondents in relation to their gender, internet usage pattern, and year of study.

d. CSA and overall Attitude of the respondents

- The majority of the respondents, i.e., 68.2%, had a negative attitude, whereas little less than one-third of the respondents, i.e., 31.8%, had a positive attitude.

Differences in the attitude of the selected university students of Vadodara regarding cybersecurity in relation to the selected variables

- There were significant differences found in the attitude regarding cybersecurity of the respondents in relation to the variables viz, gender, type of university, and digital competency.
- There were no significant differences found in the attitude regarding cybersecurity of the respondents in relation to their age, internet usage pattern, and year of study.

3.3. Differences in the co-relationships between TPB constructs, viz, knowledge, self- perception, actual cybersecurity skills and behaviours, and attitude

- All four TPB constructs in the present study, viz., knowledge, self-perception of skills, actual skills, and behaviour and attitude, revealed positive connections with one another.
- The association between self-perception of skills and attitude of CSA has been found to have the strongest positive correlation; however, the rest of the three constructs showed a moderate association with one another.

The study revealed that the majority of the respondents had low awareness regarding cybersecurity. While daily technological breakthroughs make our society more linked than ever and simplify our daily lives, they also increase the risks to our privacy by putting our personal information at risk, making it crucial for everyone to be aware of cyber security. In cybersecurity, human error is responsible for data breaches that are either unintentional or the result of negligence. It includes activities like downloading infected software and using a password that is too easy to guess. The obligation to respond rapidly to the increasing number of cybersecurity threats is placing academic organizations under pressure when they're targeted the most. Higher education organizations are compelled to develop a vulnerability management life cycle because attackers have been employing an attack life cycle. University students still don't have a good understanding of how to protect their data, although they think they are monitored online and that even on institutional systems, it is not secure. Additionally, it appears that educational institutions do not actively work to boost university students' awareness of these problems and their understanding of how to safeguard themselves against future cyberattacks, such as identity theft or ransomware.

This implies that a complete solution is required since the root reasons for university students' poor cybersecurity knowledge, negative self-perception, unsafe or dangerous cybersecurity skills and behaviours, and negative attitudes may be complicated.

IV. CONCLUSION

In nutshell, the findings of the present study regarding the constructs of the TPB framework exhibit positive results in the current investigation. The association between knowledge, one's impression of one's talents, i.e., self-perception, one's real skills and behaviour, and one's attitude towards cybersecurity is nonetheless good. This suggests that improving students' understanding and skill sets may have a positive impact on their actual abilities, behaviours, and attitudes related to cybersecurity.

Ultimately, there may not be enough mentors or role models in the field of cybersecurity for students to look up to and learn from. By setting up awareness campaigns and seminars, it is crucial to teach students more about the value of cybersecurity and the necessity of protecting their digital devices as well as their data. It can be beneficial to make materials on cybersecurity accessible, such as social media, blogs, online courses, and other resources, to increase awareness and encourage safe conduct. University students can be protected from cyber dangers and assist in creating a safer online environment by raising their level of understanding of cybersecurity. The study on cybersecurity awareness among university students concludes that more education and training are required in this area. Hence, following types of research can be undertaken in the upcoming times : 1. This study can be taken up on a larger scale by including parents and teachers along with students to measure CSA; 2. The needs and expectations of school and university students for CSA can be studied; 3. A comparative study assessing cybersecurity awareness of government school-going children versus private school children can be conducted in Gujarat and other states of India; 4. A research study on designing and developing cybersecurity training interventions for students' cybersecurity awareness in Gujarat or other states of India can be conducted; 5. A comparative study assessing cybersecurity awareness for various audience settings can be conducted in rural, tribal, and urban areas of Gujarat and India; 6. A comparative study assessing cybersecurity awareness of working women Vs housewives can be conducted in Gujarat and India.

REFERENCES

1. Adamu, A. G., Siraj, M. M., and Othman, S. H. (2022) 'Cybersecurity Awareness Evaluation Among Students at Northeastern University in Nigeria', International Journal of Electrical and Computer Engineering, 12(1), pp. 572.
2. Ahaskar, A. (2021, February 8) '60% Surge in Cyber Threats Masquerading as Online Learning Platforms in H2 2020', Mint. [Online] Available at: https://www.livemint.com/technology/tech-news/cyber-threats-disguised-as-online-learning-platforms-grew-by-60-in-h2-2020-11612784120540.html
3. Alanazi, M., Freeman, M., and Tootell, H. (2022) 'Factors Influencing the Cybersecurity Behaviours of Young Adults', Computers in Human Behavior, 136, p. 107376.
4. Alharbi, T., and Tassaddiq, A. (2021) 'Assessment of Cybersecurity Awareness Among Majmaah University Students', Big Data and Cognitive Computing, 5(2), pp. 23.
5. Almarabeh, T., Majdalawi, Y. K., and Mohammad, H. (2016) 'Internet Usage, Challenges, and Attitudes Among University Students: Case Study of the University of Jordan', Journal of Software Engineering and Applications, 9(12), pp. 577-587.
6. Alqahtani, M. A. (2022) 'Cybersecurity Awareness Based on Software and Email Security with Statistical Analysis', Computational Intelligence and Neuroscience, 2022.
7. Alzubaidi, A. (2021) 'Measuring the Level of Cybersecurity Awareness for Cybercrime in Saudi Arabia', Heliyon, 7(1), e06016. [Online] Available at: https://doi.org/10.1016/j.heliyon.2021.e06016
8. Anand, N., Jain, P., Prabhu, S., Thomas, C., Bhat, A., Prathyusha, P. V., Bhat, S., Young, K. S., and Cherian, A. V. (2018) 'Internet Use Patterns, Internet Addiction, and Psychological Distress Among Engineering University Students: A Study from India', Indian Journal of Psychological Medicine, 40(5), pp. 458–467. [Online] Available at: https://doi.org/10.4103/ijpsym.ijpsym_135_18
9. Anwar, M., He, W., Ash, I. K., Yuan, X., Li, L., and Xu, L. (2017) 'Gender Difference and Employees' Cybersecurity Behaviours', Computers in Human Behavior, 69, pp. 437–443. [Online] Available at: https://doi.org/10.1016/j.chb.2016.12.040
10. Aswathi, P., and Mohamed Haneefa, K. (2019) 'Attitude towards Information Technology and Digital Divide: A Study Among Students in Universities in Kerala, India'.
11. Bada, M., and Nurse, J. R. (2020) 'The Social and Psychological Impact of Cyberattacks', in Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press, pp. 73-92.
12. Barnicoat, C. A. (2014) 'Perceptions of Cyberbully Victimization Among College Students: An Examination Using Routine Activities Theory', Doctoral Dissertation, Middle Tennessee State University.
13. Benson, V., and McAlaney, J. (Eds.). (2019) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press.
14. Bhatnagar, N., and 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), pp. 48-58.
15. Bogdanovskaya, I., Koroleva, N., and Uglova, A. (2020) 'Digital Competence and Information Security in Adolescents', in Ceur Workshop Proceedings, pp. 63-72.

16. Chandarman, R., and Van Niekerk, B. (2017) 'Students' Cybersecurity Awareness at a Private Tertiary Educational Institution', The African Journal of Information and Communication, 20, pp. 133-155.
17. Chasanah, B. R., and Candiwan, C. (2020) 'Analysis of College Students' Cybersecurity Awareness in Indonesia', SISFORMA, 7(2), pp. 49-57.
18. Daengsi, T., Pornpongtechavanich, P., and Wuttidittachotti, P. (2022) 'Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks', Education and Information Technologies, 27(4), pp. 4729–4752. [Online] Available at: https://doi.org/10.1007/s10639-021-10806-7
19. Debb, S. M., Schaffer, D. R., and Colson, D. G. (2020) 'A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults', International Journal of Cybersecurity Intelligence & Cybercrime, 3(1), pp. 42-55.
20. Dwarakanath, S., Ravi, K., and Vijayakumar, R. (2022) 'A Study on the Emotions of an Employee After a Cyber Security Attack in Their Organization'.
21. Eduljee, N. B., and Kumar, S. S. (2015) 'Patterns of Internet Use with Indian Students from Aided and Unaided Colleges', Asian Journal of Multidisciplinary Studies, 3(7), pp. 32-43.
22. Evangelinos, G., and Holley, D. (2015) 'A Qualitative Exploration of the DIGCOMP Digital Competence Framework: Attitudes of Students, Academics, and Administrative Staff in the Health Faculty of a UK HEI', EAI Endorsed Transactions on e-Learning, 2(6).
23. Fatokun, F. B., Hamid, S., Norman, A., and Fatokun, J. O. (2019) 'Impact of Age, Gender, and Educational Level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical Investigation on Malaysian Universities', Journal of Physics: Conference Series, 1339(1), 012098. [Online] Available at: https://doi.org/10.1088/1742-6596/1339/1/012098
24. Funke, J. (2017) 'How Much Knowledge Is Necessary for Action?' in P. Meusburger, B. Werlen, & L. Suarsana (Eds.), Knowledge and Action, Springer International Publishing, pp. 99–111. [Online] Available at: https://doi.org/10.1007/978-3-319-44588-5
25. Ghosh, S., and Tripathy, B. K. (2022) 'Cybersecurity Awareness and Practices Among Postgraduate Students of Management Institutes: An Empirical Study', Journal of Critical Reviews, 9(4), pp. 425–433.
26. Goncalves, R., Silva, R., Fonseca, B., and Cunha, M. A. (2021) 'Cybersecurity Knowledge and Practices: A Study on Portuguese University Students', International Journal of Cybersecurity Intelligence & Cybercrime, 4(2), pp. 29–49.
27. Gupta, N., Kapoor, N., and Swami, S. (2018) 'Security Awareness in Social Media and Smartphone Applications Among College Students in India', Computers in Human Behavior, 87, pp. 19–27.
28. Haghighi, P. D., and Hyun, S. S. (2016) 'The Impact of Internet on the Academic Performance of Iranian College Students', Proceedings of the European Conference on E-Learning, pp. 300-308.
29. Hassan, Z., Hashem, I. A. T., and Tahir, A. B. (2016) 'Students' Attitudes and Acceptance of Mobile Learning in Higher Education Institutions', The Electronic Library, 34(2), pp. 302-318.
30. Jawahar, K., and Devi, S. N. (2022) 'Cybersecurity Practices and Awareness Among Engineering College Students in Tamil Nadu', Materials Today: Proceedings, 58, pp. 1087–1090.
31. Kang, M. (2019) 'Global Perspectives on Cybersecurity Education', in Handbook of Research on Curriculum Development and Experiential Learning in Modern Business, IGI Global, pp. 1-25.
32. Kavitha, S., and Uma, G. (2020) 'Security Awareness Among College Students in Tamilnadu: An Empirical Study', Materials Today: Proceedings, 26(4), pp. 3484–3487.

33. Kavitha, S., and Uma, G. (2020) 'Security Awareness Among College Students in Tamilnadu: An Empirical Study', Materials Today: Proceedings, 26(4), pp. 3484–3487.
34. Kim, B., and An, J. (2019) 'Cybersecurity Awareness and Training for Employees: A Research Note', International Journal of Information Management, 44, pp. 141–147.
35. Kolahi, J., Khazaei, S., Salahi-Moghaddam, A., Soori, H., and Molaeipoor, L. (2014) 'Factors Influencing the Use of Information Technology in Nursing Education: A Study in Iran', Journal of Advances in Medical Education & Professionalism, 2(4), pp. 169–174.
36. Kumar, N., and Joseph, J. (2017) 'A Study on the Security Awareness of E-Banking Users in Selected Areas of Kerala', Journal of Emerging Technologies and Innovative Research, 4(2), pp. 33-39.
37. Kurubacak, G., Erdur-Baker, O., and Sunar, D. (2009) 'Cyberbullying: A New Face of Peer Bullying', The Eurasia Proceedings of Educational & Social Sciences, 1(1), pp. 96-100.
38. López, R., Zhang, H., Saldaña, M., Zhou, J., Aung, Z., Zhang, J., and Chen, X. (2019) 'Understanding Students' Cybersecurity Behaviors: A Case Study', in Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication, ACM, pp. 1-8.
39. Lu, H. H., Lu, L. Y., and Yu, C. S. (2013) 'Factors Affecting Cybersecurity Knowledge Sharing Intention among Employees', Management Decision, 51(10), pp. 2029–2045.
40. Lublóy, Á., and Kaczmarek, M. (2021) 'Perceived Cybersecurity Risks and Individual Cybersecurity Behaviors: Empirical Evidence from Europe', Journal of Organizational and End User Computing (JOEUC), 33(1), pp. 16-38.
41. Madakam, S., Ramaswamy, R., and Tripathi, S. (2015) 'Internet of Things (IoT): A Literature Review', Journal of Computer and Communications, 3(2), pp. 164-173.
42. Manogaran, G., Lopez, D., and Thota, C. (2017) 'A Survey of Big Data Architectures and Machine Learning Algorithms in Healthcare', Journal of King Saud University - Computer and Information Sciences. [Online] Available at: https://doi.org/10.1016/j.jksuci.2017.01.015
43. Marchiori, E., Moustakas, E., Katos, V., and Arief, B. (2013) 'Digital Forensic Process Ontology', Journal of Digital Forensics, Security and Law, 8(2), pp. 25-40.
44. Mehmood, A., and Pearson, S. (2014) 'Fog Computing: Focusing on Mobile Users at the Edge', ACM SIGCOMM Computer Communication Review, 44(5), pp. 1-2.
45. Mentz, J., and Cilliers, L. (2021) 'Digital Forensics Education for Employability', Future Generation Computer Systems, 115, pp. 198-207.
46. Mitnick, K. D., and Simon, W. L. (2002) The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons.
47. Mokhtarian, P. L., Salomon, I., and Singer, M. E. (2015) 'What Moves Us? An Interdisciplinary Exploration of Reasons for Travel Behavior', Transportation Research Part A: Policy and Practice, 77, pp. 96-112.
48. Moallem, A. (2019). Cybersecurity awareness among college students. In Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21–25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9 (pp. 79–87). Springer International Publishing.
49. Moletsane, T., and Tibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. 2020 conference on information, communications, technology, and society (ICTAS) (pp. 1–6). IEEE.

50. Moshirpour, M., and Dargahi, T. (2021) 'A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Directions', Journal of Network and Computer Applications, 178, p. 102987.
51. Mylrea, M. F., Gupta, L., and Yuan, Y. (2014) 'New Market Opportunities for Digital Forensics in the Cloud', Digital Investigation, 11(3), pp. 215-224.
52. Nagaur, A. (2020). Internet addiction and mental health among university students during the CVOID-19 lockdown. MuktShabd J, 9, 684-692.
53. Narahari, A. C., & Shah, V. (2016). Cyber Crime and Security: A Study on Awareness among Young Netizens of Anand, Gujarat State, India. IJARIIE, 6(2), 1164–1172.
54. Nasser, A., Minoli, D., and Jain, R. (2013) 'Cloud-Based Wireless Networks: Technologies, Risks, and Scenarios', IEEE Wireless Communications, 20(2), pp. 10-17.
55. Niemantsverdriet, K., and Russell, M. A. (2018) Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices, IGI Global.
56. Nyikes, Z., &Baimakova, K. V. (2016). An Examination of the Relationship between Security Awareness and Digital Competence.
57. Ozdamli, F., and Zunboylu, H. (2015). M-learning adequacy and perceptions of students and teachers in secondary schools: M-learning adequacy and perceptions. British Journal of Educational Technology, 46(1), 159–172. https://doi.org/10.1111/bjet.12136
58. Pham, H., Brennan, L., & Richardson, J. (2017, June). Review of behavioural theories in security compliance and research challenges. Informing Science and Information Technology Education Conference, Vietnam (pp. 65–76). Santa Rosa, CA: Informing Science Institute
59. Reddy, G. N., & Reddy, G. J. U. (2014). A study of cyber security challenges and emerging trends in the latest technologies. arXiv. https://doi.org/10.48550/arXiv.1402.1842
60. Safarpour, F., Kurd, N., and Ghazanfari, Z. (2021). A Study on Internet Usage Patterns among Students at the Medical University of Ilam and Influential Factors. Biomedical Journal of Scientific and Technical Research, 33(2), 25761-25765.
61. Sanzgiri, V., &Sanzgiri, V. (2022). 12.67 lakh cyber-attacks were reported in India by November 2022, according to the IT Ministry in Parliament. MediaNama.https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/
62. Second International Conference of the South Asian Society of Criminology and Victimology (SASCV), 11–13 January 2013, Kanyakumari, Tamil Nadu, India. (n.d.). Google Books. https://books.google.co.in/books?hl=en&lr=&id=Do1Kl2OyQdgC&oi=fnd&pg=PA378&dq=studies+on+cybercrime+victims+within+college+students+in+india&ots=S3lsbbieAj&sig=RuMykUvXLoDVGiE3nG90ik17iKM&redir_esc=y#v=twopage&q=studies%20on%20cybercrime%20victims%20within%20college%20students%20in%20india&f=true
63. Senthilkumar, K., and Eswaramoorthy, S. (2017, November). A survey on cyber security awareness among college students in Tamil Nadu. In IOP Conference Series: Materials Science and Engineering (Vol. 263, No. 4, p. 042043). IOP Publishing.
64. Skinner, W., & Foam, A. M. (1997). A Social Learning Theory Analysis of Computer Crime among College Students. Journal of Research in Crime and Delinquency, 34(4), 495–518. https://doi.org/10.1177/0022427897034004005
65. Slusky, L., &Partow-Navid, P. (2012). Students' information security practices and awareness. Journal of Information Privacy and Security, 8(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664

66. Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public wi-fi? An investigation of behaviour and factors driving decisions. Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 61–72. https://doi.org/10.1145/3046055.3046058
67. Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human-Computer Studies, 123, 29–39.
68. Wang, X., Zhang, R., Wang, Z., & Li, T. (2021). How does digital competence preserve university students' psychological well-being during the pandemic? An investigation from self-determined theory. Frontiers in Psychology, 12. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.652594
69. Yen, S. C., Lo, Y., Lee, A., & Enriquez, J. (2018). Learning online, offline, and in-between: comparing student academic outcomes and course satisfaction in face-to-face, online, and blended teaching modalities. Education and Information Technologies, 23, 2141-2153.
70. Yu, S. (2014). Fear of cybercrime among college students in the United States: An exploratory study. International Journal of Cyber Criminology, 8(1), 36.
71. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge, and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97.

WEBILIOGRAPHY

72. BL New Delhi Bureau. (2022, March 15). Indian Gen Z spends average 8 hours a day online: report. [Online] Available at: https://www.thehindubusinessline.com/news/variety/indian-gen-z-spends-average-8-hours-a-day-online-report/article65227021.ece
73. Bournemouth University Research Online [BURO]. A Qualitative Exploration of the DIGCOMP Digital Competence Framework: Attitudes of students, academics, and administrative staff in the health faculty of a UK HEI. (n.d.). [Online] Available at: http://eprints.bournemouth.ac.uk/23477/
74. Bureau, B. N. D. (2022, March 15). Indian Gen Z spends average 8 hours a day online: Report. [Online] Available at: https://www.thehindubusinessline.com/news/variety/indian-gen-z-spends-average-8-hours-a-day-online-report/article65227021.ece
75. Campbell, S. (2017). Cybersecurity in Higher Education: Problems and Solutions. Toptal Insights Blog. [Online] Available at: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education
76. CIA Triad in Cyber Security: Definition, Examples, Importance. (n.d.). [Online] Available at: https://www.knowledgehut.com/blog/security/cia-in-cyber-security
77. Cybercrime in India: An overview. (n.d.). [Online] Available at: https://legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
78. Cyber security awareness and why it is important | Australian Institute of ICT. (n.d.). [Online] Available at: https://aiict.edu.au/blog/what-is-cyber-security-awareness-and-why-is-it-important/
79. Cyber space and the various challenges attached to the regulation of information and communication technology. - Lawpanch. (2022, March 2). [Online] Available at: https://lawpanch.com/cyber-space-and-the-various-challenges-attached-to-the-regulation-of-information-and-communication-technology-%ef%bf%bc/

80. Cybersecurity awareness is about both “knowing” and “doing.” (2014, October 1). Security Intelligence. [Online] Available at: https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/
81. Cybersecurity in higher education: Problems and solutions | Toptal. (n.d.). Toptal Insights Blog. [Online] Available at: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education
82. Delhi University, AMU, IIT-BHU websites hacked; “Pakistan Zindabad”, pro-Kashmir messages seen. (n.d.). India Today. [Online] Available at: https://www.indiatoday.in/india/story/delhi-university-amu-website-pakistan-zindabad-kashmir-kashmiri-youths-indian-army-973492-2017-04-25
83. Desk, I. T. W. (2017, April 25). Delhi University, AMU, IIT-BHU websites hacked; 'Pakistan Zindabad', pro-Kashmir messages seen. India Today. [Online] Available at: https://www.indiatoday.in/india/story/delhi-university-amu-website-pakistan-zindabad-kashmir-kashmiri-youths-indian-army-973492-2017-04-25
84. Desk, T. (2022, June 13). 18 out of every 100 Indians victim of data breaches: SurfShark. The Indian Express. [Online] Available at: https://indianexpress.com/article/technology/tech-news-technology/18-out-of-every-100-indians-affected-by-data-breaches-surfshark-7967560/
85. Dunning-Kruger effect | Definition, examples, & facts | Britannica. (2023, March 27). [Online] Available at: https://www.britannica.com/science/Dunning-Kruger-effect
86. Economic Diplomacy Division. India to have nearly 1 billion internet users by 2025: Report. [Online] Available at: https://indbiz.gov.in/india-to-have-nearly-1-billion-internet-users-by-2025-report/
87. Education report cybersecurity. (n.d.). Security Scorecard. [Online] Available at: https://resources.securityscorecard.com/all/education-report-cybersecurity
88. Facts and figures 2021. (n.d.). [Online] Available at: https://www.itu.int/itu-d/reports/statistics/2021/11/15/youth-internet-use
89. Indian education sector biggest target of cyber threats, remote learning among key triggers: Report. (2022, May 1). The Times of India. [Online] Available at: https://timesofindia.indiatimes.com/india/indian-education-sector-biggest-target-of-cyber-threats-remote-learning-among-key-triggers-report/articleshow/91234420.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
90. Lara. (2018, February 24). Answer to "What’s the difference between “knowledge of sth” and "perception of sth “?” English Language & Usage Stack Exchange. [Online] Available at: https://english.stackexchange.com/a/432673
91. Matters, S. M. (n.d.). Patterns of internet usage among youth in India. Social Media Matters. [Online] Available at: https://www.socialmediamatters.in/internet-usage-among-youth-in-india
92. Measuring digital development: Facts and Figures 2022. (n.d.). ITU Hub. [Online] Available at: https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/
93. Murnane, K. (n.d.). How men and women differ in their approach to online privacy and security. Forbes. [Online] Available at: https://www.forbes.com/sites/kevinmurnane/2016/04/11/how-men-and-women-differ-in-their-approach-to-online-privacy-and-security/
94. Pramshu. (2022, May 17). India to have nearly 1 billion Internet users by 2025: Report - IndBiz | Economic Diplomacy Division. IndBiz | Economic Diplomacy Division. [Online] Available at: https://indbiz.gov.in/india-to-have-nearly-1-billion-internet-users-by-2025-report/

95. Pti. (2022, May 1). Indian education sector biggest target of cyber threats, remote learning among key triggers: Report. The Times of India. [Online] Available at: http://timesofindia.indiatimes.com/articleshow/91234420.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

96. Redmonster.In. (2022). Cyber Space and the various Challenges attached to the regulation of Information and Communication Technology. - LawPanch. LawPanch - Let's Spread Law. [Online] Available at: https://lawpanch.com/cyber-space-and-the-various-challenges-attached-to-the-regulation-of-information-and-communication-technology-%EF%BF%BC/

97. Sanzgiri, V. (2022, December 15). 12.67 lakh cyber-attacks reported in India by November 2022: IT Ministry in Parliament. MediaNama. [Online] Available at: https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/

98. Security Culture Report. (n.d.). Knowbe4. [Online] Available at: https://www.knowbe4.com/hubfs/Security-Culture-Report.pdf

99. Statistics. (n.d.). ITU. [Online] Available at: https://www.itu.int:443/en/ITU-D/Statistics/Pages/stat/default.aspx

100. The benefits of cyber security awareness training within universities. (2022, July 19). Open Access Government. [Online] Available at: https://www.openaccessgovernment.org/the-benefits-of-cyber-security-awareness-training-within-universities/139452/

101. The State of Cybersecurity Education in K-12 Schools. (n.d.). cyber.org. [Online] Available at: https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

102. Townsend, A. (2021, February 26). 3 reasons higher education is a cyberattack favorite. OneLogin Identity Management Blog. [Online] Available at: https://www.onelogin.com/blog/3-reasons-higher-ed-hacked

103. Utilizing the technology acceptance model to assess employee adoption of information systems security measures - ProQuest. (n.d.). [Online] Available at: https://www.proquest.com/openview/561019e2cb80f662d4308633147e172c/1?pqorigsite=gscholar&cbl=18750

104. Wallace, J. (2022, June 2). What is the CIA triad? Definition & examples in cybersecurity. Coretelligent. [Online] Available at: https://coretelligent.com/insights/what-is-the-cia-triad-and-why-does-your-cybersecurity-position-depend-on-it/

105. Wilde, N. (2022). The benefits of cyber security awareness training within universities. Open Access Government. [Online] Available at: https://www.openaccessgovernment.org/the-benefits-of-cyber-security-awareness-training-within-universities/139452

106. Yu, S. (2014). Fear of cybercrime among college students in the United States: An exploratory study. International Journal of Cyber Criminology, 8(1), 36.