CYBERSECURITY AWARENESS AMONG THE UNIVERSITY STUDENTS OF THE VADODARA, 2022-23

April, 2023 **Manasi Nimbekar**

CYBERSECURITY AWARENESS AMONG THE UNIVERSITY STUDENTS OF THE VADODARA, 2022-23

A Dissertation

Submitted in partial fulfilment of the requirement

for the degree of Master of Science in

Faculty of Family and Community Sciences (F. C. Sc.)

The Maharaja Sayajirao University of Baroda, Vadodara

2023

Manasi Nimbekar
(Research Scholar)

Dr. Varsha Parikh
(Research Guide)

Department of Extension and Communication,
Faculty of Family and Community Sciences,
The Maharaja Sayajirao University of Baroda,
Vadodara, Gujarat.

Department of Extension and Communication

Faculty of Family and Community Sciences,

The Maharaja Sayajirao University of Baroda, Vadodara.

NOTE

The examiners are requested to keep in mind while evaluating the student's project report of either the dissertation or the action project.

The master students can choose dissertation work or action project for 10 credits. The written reports or a dissertation can be 120 to 130 pages, while the report of an action project can be 60 to 80 pages. The dissertation can have hypotheses and qualitative/ quantitative statistical analysis, while the action project can have field-type evaluation using only percentages.

An action project or research study must be accompanied by appendices, giving an account of physical proof of having conducted an actual project or study, e.g., maps, photographs, drawings, samples, attendance records, booklets, etc.

At the time of viva-voce examination, a student who has carried out an action project may present actual project models, charts, equipment, objects, etc., used in carrying out the projects as further proof of the project.

Dr. Avani Maniar

Head,

Department of Extension and Communication

Faculty of Family and Community Sciences

The Maharaja Sayajirao University of Baroda

Vadodara, Gujarat.

CERTIFICATE

This is to certify that the dissertation entitled **"Cybersecurity awareness among the university students of the Vadodara, 2022-23"** has been carried out by the investigator under my supervision and guidance for the partial fulfilment of the Degree of Masters of Science (Faculty of Family and Community Sciences). The matter presented in this dissertation has not been submitted for the award of any other degree or diploma.

Manasi Nimbekar
Research scholar

Dr. Varsha Parikh
Research Guide & Associate Professor
Department of Extension and Communication
Faculty of Family and Community Sciences
The Maharaja Sayajirao University of Baroda
Vadodara, Gujarat.

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the God, the Almighty, for his showers of blessings throughout my research work to complete the research successfully.

I would like to express my deep and sincere gratitude to my research Guide **Dr. Varsha Parikh, Associate Professor,** Department of Extension and Communication (EC), Faculty of Family and Community Sciences (FFCSc), The Maharaja Sayajirao University of Baroda (MSUB), Vadodara for her invaluable guidance and support throughout my study. Her expertise and encouragement helped me to complete this research work on time and write this thesis. Her patience, motivation, enthusiasm, knowledge, and immense support has greatly contributed to the success of this research study.

I express my genuine gratitude to **Dr. Avani Maniar**, Head of the Department (EC), FFCSc, MSUB, Vadodara for her constructive support and valuable suggestions in tool validation for the study. I am also sincerely thankful to **Prof. (Dr.) Anjali Pahad,** EC, FFCSc, MSUB, Vadodara, for her important inputs in the research tool as well as insightful recommendations at distinct stages of my research study.

I would like to acknowledge **Dr. Deepti Singh and Ms. Hetashree Brahambhatt** -Assistant professors, EC, FFCSc, MSUB, Vadodara for their kind support in facilitating data collection from the department students. I am also grateful to **Ms. Sapna Shah**, Assistant professor, FFCSc, Vadodara who spared her time to validate the research tool for the study.

I am also grateful to all the undergraduate and postgraduate students of MSUB and Parul University who have supported me in on/offline mode by participating and filling up my research tool, sparing their valuable time, with their responses.

I am extremely thankful to **Mr. Shardul Acharya** who supported me for my statistical analysis for my research study. I am also thankful to my classmates **Shiri Shah, Shivani Patel, Pritha Kansabanik, Chaitalee Chauhan and Drashti Gandhi** for the help in several ways. I would like to offer my thanks to **Riddhi Koley, Umesh Parmar, Aayush Keshwala and Daxay Patel** for their help, support and motivation in various ways in my study. Special thanks to **Harsh Patel, Rishikesh Dhatrak, Hardi Zanje, Shubham Parmar** for their help and motivation in many ways in my study.

I express my deepest gratitude, to my family, my mother and father for their constant support, encouragement, endless motivation, and appreciation during my research work.

Manasi Nimbekar

Abstract

The present study entitled “Cybersecurity awareness among the university students of the Vadodara, 2022-23” was conducted among the university students of Vadodara to assess their overall cybersecurity awareness. The Theory of planned behavior (TPB) framework was used to understand student's awareness level emphasizing their cybersecurity measures. Adapted TPB framework, which comprised constructs viz. knowledge, self-perception, actual skills and behavior, and attitude regarding cybersecurity was used in the study. A total of 242 students of selected universities of Vadodara were selected in the present study using a snowball sampling method. The data was collected in person as well as using an online platform, through Google form. The link for Google form was shared with the respondents using emails and WhatsApp. The Statistical Package for the Social Sciences (SPSS) programme was applied for the statistical analysis.

Major results of the study highlights that, majority of the students were in the category of young students (18-23 years). Little more than half of the respondents were female and were studying in Private University. High majority of the respondents were at the undergraduate level. Majority of the respondents were moderate internet users. High majority of the respondents were found with primary level of digital competency skills. Only 17% of the respondents responded that they have faced issues during cyber surfing. The study revealed that majority of the students had low awareness regarding cybersecurity. The study also revealed that majority of the respondents had lower level of knowledge and unfavorable perceptions regarding cybersecurity. Most of the students follow unsafe cybersecurity skills and behavior, while carrying negative attitude towards cybersecurity. Further, correlation between TPB constructs was also checked in the study.

Key words: Cybersecurity, University students, Theory of planned behavior, Digital competency, knowledge, self-perception, actual skills and behavior, attitude

INDEX

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1 Cyberspace

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 cyber world refers to this online environment.

1.1.1 Digital Development Scenario

National Information Centre (NIC) created India's cyberspace officially in 1975 to provide government information technology solutions. According to Internet and Mobile Association of India (IAMAI) and consultancy company Kantar, by 2025, India's internet user base will be close to 1 billion. Social commerce platforms were used to make more than 500 million digital transactions, representing more than half of the country's online shoppers. By 2025, there will be 50% of all students using online learning in some capacity. (Pramshu, 2022, May 17). Nine out of ten active users online spent a daily average of 107 minutes. The study found that in both rural and urban India, the three most popular applications of the internet were for social media, communication, and entertainment. (Statistics, (n.d.). ITU. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx) Thus, cyberspace, the online environment, has recently grown in popularity despite the fact that it lacks a formal, global structure for complete governance. Some countries functioning under the United Nations have recently tried to establish a global framework for internet regulation. India is actively working to create this framework for cyberspace governance. [Redmonster.In. (2022)].

1.2 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. Data must be accurate, and any changes must be obvious.
- Accessibility is crucial since data is only useful if it is **available**.

Figure 1: CIA Triad Model

In a way, CIA is a fundamental concept to build a comprehensive, effective cyber security plan, which though cannot eliminate problems, can aid in prioritising systemic cyber hazards so that they can be effectively dealt with. It can decrease the likelihood of needless exposure and lessen the severity of a cyberattack, even though it cannot completely avoid all sources of compromise (Wallace, J., & Wallace, J., 2022, July 5.). Therefore, it can be an effective benchmark for determining the necessity of the security controls that are considered when an organisation or individual develops a security agenda. On the other hand, when a security incident, such as information stealing or a security breach occurs, it is determined that an organisation or individual has failed to properly enforce one or more of these regulations. In such instances, disclosure, modification, and destruction occur which are the antithesis of confidentiality, integrity, and availability. Here,

- Disclosure means when someone with permission accesses your information.

- Alteration means the modification or alteration of data.
- Destruction means when information, software, or systems are lost or rendered unreachable. (https://www.knowledgehut.com/blog/security/cia-in-cyber-security)

1.3 Cyber security issues and challenges

Several industries soon digitalised their internal operations in response to the Indian government's initiatives to digitally modernise the country. Indeed, all of this technical progress has made it possible for organisations to operate more successfully, but it has also resulted in intellectual property theft and the disclosure of sensitive data.

Below shown the "Fishbone" (Ishikawa) diagram, invented by Dr. Kaoru Ishikawa in the 1960s, a visualisation tool highlights potential causes of a cyber issues and related challenges in the areas of five M's, viz, Man, Machine, Methods, Materials and Measurement.

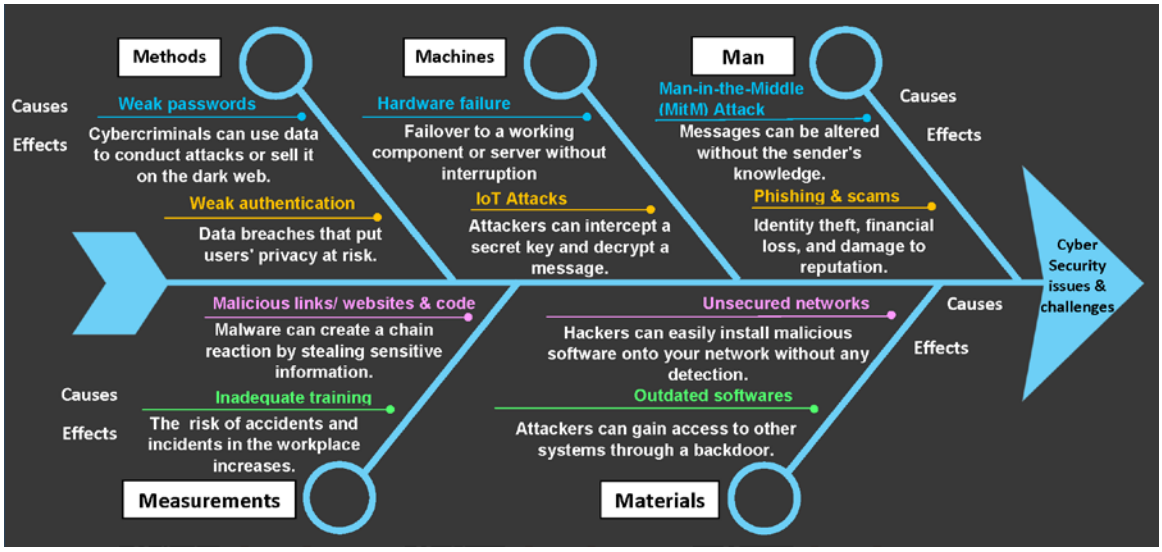


Figure 2: Fishbone diagram

- **Man** i.e., the individuals who are responsible for maintaining the devices. (personnel)
- **Machines** i.e., any component of a device needed to do the task, such as Firewalls, routers, computers, etc. (equipment)
- **Methods** i.e., the specific controls for carrying out the organization and its security process, such as policies, procedures, and norms. (Procedure)

- **Materials** i.e., the software needed to supply and safeguard the defences as well as the organization's processes. (tools)
- **Measurements** i.e., information produced by the security process, such as data, warnings, alerts, or other information, it has been used to evaluate the method's usefulness and effectiveness. (precision)

The Indian Computer Emergency Response Team (CERTIn) had received and monitored up to 12.67 lakh incidents of cyberattacks as of November 2022, according to their research, which found that the number of cyberattacks increased from 41,378 in 2017 to 14,02,809 in 2021, according to CERT-In statistics (Sanzgiri & Sanzgiri, 2022).

1.4 University vulnerability to cyber threats/ attack at global level and in India

Despite the fact that virtually every major industry faces serious cybersecurity concerns, higher education is particularly at risk because it involves many crucial components. 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 universally. Universities and colleges are convenient targets for the hackers.

1. **Educational institutions are still not secure enough -** The Security Scorecards 2018 report placed education worst among all industries in terms of cybersecurity. Universities/ Colleges struggle with their funds, especially public universities. Security expenditures are costly and sometimes put on the back burner in favour of other priorities.
2. **Numerous applications and open networks -** Universities and colleges have extensive networks that give staff and students access to a variety of data and apps. In order to remain competitive with other institutions, colleges are focusing on offering all the services necessary while also maintaining easy access for students. Unfortunately, that enables hacker easy access.
3. **Students are convenient targets -** Every year, a new class of students enrols at colleges, making it impractical to provide extensive cyber education. People in

their twenties usually lack experience, making them more susceptible to hacker frauds.

4. **Countless devices -** Bring Your Own Device (BYOD) is most prevalent on college campuses. All of their personal technology, including laptops, desktop computers, smart phones, and tablets, is interconnected. Hence, there is an opportunity with every gadget for hackers.
5. **Large campuses are welcoming to strangers -** There is no better environment for social engineering techniques, backdoors, or man-in-the-middle attacks than a college campus. It is simple for visitors to enter, get a security checkpoint, and plant Universal Serial Bus (USBs), monitor traffic, or damage labs and research spaces. **(**Townsend, A., 2022**)**
6. **Financial opportunities -** Money is the main factor in most hacking incidents. In 2018, 79% of attacks against educational institutions were driven by financial gain. Cybercriminals can steal money, hold college websites or data hostage for ransom, among many other crimes. (https://www.onelogin.com/blog/3-reasons-higher-ed-hacked)
7. **Personally Identifiable Information (PII) -** Higher education institutions are increasingly important suppliers of PII. In addition, they have data on many students who now have credit histories as well as former students, present workers, and other individuals. Numerous significant types of data are frequently stored in the system by universities, including details of loans, bank accounts, passports, social security numbers, and even medical information.
8. **Valuable confidential research -** Institutions are increasingly targeted by state and non-state actors seeking confidential and valuable research data. “The Massachusetts Institute of Technology” and “The University of Washington” were two among the twenty-seven universities that a Chinese hacker allegedly targeted. Educational institutions were targeted by cyber espionage 3.5 times more frequently in 2019 than in 2018. (Townsend, A., 2022). Due to the fact that educational institutions use the internet for research, they are vulnerable to cyberattacks, particularly the students who have insufficient cybersecurity expertise.

1.5 Significance of cyber security awareness

There has never been a more urgent need for cyber security than now as a result of educational institutions going online in response to the COVID-19 epidemic in 2020-2021. As after the COVID crisis, cybercrime has apparently increased in recent years, which has reportedly surged by almost 600%; hence, there has never ever been a more pressing need for cyber security than now. Several new threats occurred as a result of educational institutions going online in response to the COVID-19 epidemic in 2020–2021. As student data, personal information, and highly important research make universities appealing targets for hackers, and they have historically posed a serious threat to this crime. Hence, 75% of data breaches in the education industry can be attributed to universities alone. Attacks on colleges have increased since the disastrous security breach of 2018, when Iranian hackers targeted over 300 colleges. As a result, there is a significant need and desire to transform universities and other higher education institutions with utmost mechanisms. (Wilde, 2022).

When the COVID-19 pandemic began, students wishing to advance their education without attending classes or training facilities have 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 importance of cybersecurity awareness amongst the university staff, students in higher education institutions. (Ahaskar, 2021)

Therefore, in this situation, university students need to equip themselves with the right perception, attitude, and knowledge of cyber security as well as the necessary skills and behaviors to secure their devices and personal data. This is critical as cyber hackers continue to exploit weaknesses and present new vulnerabilities and hazards. Cybersecurity awareness programs are believed to be the first line of defence in preventing threat confrontation and security attacks. One of the major centres for higher education in Gujarat is Vadodara, which is home to numerous private and government universities. Many students come here to pursue higher education, not just from the nearby states but from across the country and outside. As researcher examine the

aforementioned vulnerability scenario in the context of universities through a number of conceptual and empirical studies, it is crucial to understand the following research questions:

(1) What level of cyber security awareness do university students have in this digital age?

(2) What is the attitude of university students who use extensive Internet of Things (IoTs) for various purposes?

(3) How well university students deal on cyber safety concerns?

(4) How do the university students perceive cybersecurity essential for their own data?

(5) How competent are university students while using protecting tool & techniques for themselves for online activities?

1.6 Statement of the Problem

A study on **"Cybersecurity awareness among the university students of the Vadodara, 2022–23"** was decided to be carried out in order to address the aforementioned research questions.

1.7 Justification of the study

The issue of cybersecurity is becoming more and more widespread. According to the research "Cyber Threats Attacking the Global Education, (2022)", "The USA, the UK, Indonesia, and Brazil all have seen more serious cyberattacks on higher education institutions and online platforms than India" (Pti, 2022, May 1). In light of this concern, following reasons justify need of the study.

1) **Academia's unique open culture -** Academics prefer to be more open and transparent than the majority of other industries, according to "Fred Cate, director of the Centre for Applied Cybersecurity Research at Indiana University (2013)" Colleges and universities "generally concentrate their efforts on making it as simple as possible for audience members, supporters, students, and instructors to connect with and be with us," the study claims (Campbell, 2017).

2) **Human error -** The most frequent error is double clicking on a potentially harmful Uniform Resource Locator (URL) or corrupted attachment, easy-to-guess passwords, misplaced mobile devices and laptops, default usernames and

passwords, and unintentional disclosure of confidential information by using an inaccurate email address are a few examples from the 2014 Cyber Security Intelligence Index. The average cost of a breach caused by human error is predicted to reach $4.63 million in 2021, and it was determined that 19 out of 20 digital risks would not occur at all if completely eliminated. As a result, it is crucial to establish a culture of cyber security awareness in order to protect students from online threats. (Martin, J.,2018)

3) **Free accessible public Wi-Fi -** Over the past ten years, public Wireless Fidelity (Wi-Fi) networks have proliferated, becoming more common in public spaces like transportation hubs, coffee shops, or next to well-known tourist attractions. However, as numerous other studies have shown, the majority of these networks are insecure, so when users connect, they expose themselves to security and privacy risks whether deliberately or unintentionally. A study done by **Sombatruang N., Sasse A. & Baddeley M. (2016)** claims that more than 90% of their participants expressed concerns about the security of public Wi-Fi, and among those, more than 50% continue to use these networks despite being aware of the risks. However, the most commonly quoted justification is that 'it is free'. University students, who typically have little funds for personal expenses and educational costs, frequently use free public Wi-Fi, putting them at risk for online threats. Due to the aforementioned factors, cyber security awareness is crucial amongst the university and higher education system and its contributors, since it guards against data loss and theft. So, carrying out the suggested study on students' levels of cyber security awareness can be quite helpful.

1.8 Justification for sample

The present research will comprise university students of Vadodara as sample of the study.

1) **Digitalisation in education and university students:** The proposed study focuses on the university students of Vadodara, where the samples for the study would be drawn from the public and private universities within Vadodara. In the post-pandemic era, young students use more internet and visit more websites for a variety of purposes, including searching for teaching-learning resources, library

resources, research projects, various training programs, downloading videos, images, and documents, and mostly using e-commerce websites. As a result, there is a higher chance that they will visit both safe and unsafe websites, which leaves them open to various cyber threats and risks. Since attackers continue to identify breaches and introduce new threats and flaws, this indicates that students should arm themselves with the knowledge they need to protect their gadgets and personal information to handle the challenges associated with using digital platforms for educational and research purposes while using IoTs. Therefore, this sample is selected to assess their awareness level regarding cyber security.

2) **Internet addiction with lack of knowledge of cyber security:** Varghese et al. (2021) conducted a study on "the incidence of internet addiction among college-going students in India" and found that "from 20-40% percent of Indian college-bound students are at a high risk of acquiring an online addiction." University and college students frequently use the internet, particularly social media. Additionally, despite the fact that new Internet users sign up every day, a report by the "International Telecommunication Union of the United Nations" claims that they "lack sufficient understanding of security risks and the consequences of their online behavior." These illustrate the need for students who use the internet regularly to be up to date on security concerns, potential issues, and solutions in case those issues do occur. The current generation of students should also be able to recognise potential cyber hazards. Therefore, this study proposes to choose university students of Vadodara to determine the level of their cybersecurity awareness.

3) **Gen Z with least report of cybercrime:**

Millennials (aged 25 to 40) and Generation Z (18 to 24) were less likely than earlier generations to report cybercrime and become its victims, according to a survey by the National Cybersecurity Alliance in the US and the UK. As a result, the higher education system and universities are in an alarming state where Gen Z are major stakeholders, and there is a great need for solutions (By BL New Delhi Bureau, 2022).

1.9 Justification of Variables

1. **Age -** An individual's maturity and capacity to manage problems are typically correlated with age. As one grows old, they gather more life experiences. The adoption of technology may be significantly impacted by age. The age of a student affects their computer use, abilities, attitudes, self-efficacy, and anxiety.

   So, it is assumed that older age groups, though more exposed with technology, may be using Internet of Things (IoT) consciously and dealing with every situation maturely. Young students may be more exposed to technology as using it from early childhood, but ignorance regarding cyber threat/attack. According to Hasan et al. (2015), “Students between the ages of 18 and 23 had less perception and awareness than those between the ages of 24 and above”. This suggests that younger students, who use technology, may be less aware than the older group. Further, maturity level, inquisitiveness, and reporting of cybercrime may be the factors which may vary awareness of younger to older age group of the students. Hence, this variable is proposed in the present study.

2. **Gender –** It includes male, female and other, Gender has been considered as a variable in the present study. In addition, an individual's desire to use the internet, their online navigational skills, their risk-taking propensity, and their propensity to adopt new technologies may differ from one another, so depending on the students' gender, this may have an impact on their level of awareness of cybersecurity. Thus, it is included as a variable.

   According to one survey response, the majority of female students said they were less familiar with technology concerns than were male students. The results of a study on how gender influences cybersecurity practices and attitudes showed that, on a scale measuring how seriously students take cybersecurity, female college students performed on average better than male college students (Anwar et al., 2017); as a result, it is possible that women are more likely than men to feel cautious and anxious. Male students may be less concerned about the impact of strict cybersecurity legislation because of prevalent social expectations of masculinity (Anwar et al., 2017).

3. **Type of university -** The key difference between public and private universities is that government-funded institutions receive funding from the state, whereas private institutions are supported by donations, tuition fees, and private initiatives. Students expect a secure online environment at the university in this situation where India is currently experiencing a sharp rise in cybercrime patterns. Famous Indian universities' websites, including University of Delhi (DU), Aligarh Muslim University (AMU), Indian Institute of Technology Delhi, etc., have reportedly come under attack by pirates from Pakistan, according to "India Today Web Desk (2017)" (Desk, 2017).
4. **Year of Study –** Undergraduate (UG) students of first to fifth year may utilise the internet less frequently for academic purposes than postgraduate (PG) students do. Further, First and second-year postgraduate students may use the internet more frequently for a variety of tasks, increasing the likelihood that they will visit both safe and dangerous websites, such as finding teaching and learning resources, library resources, research projects, various training programs, downloading movies, photos, and documents, and visiting e-commerce websites. According to Filippidis et al. (2018), masters students have a higher prevalence of internet security awareness (ISA) than undergraduates (Daengsi et al., 2021c).

   Besides that, the present study has taken year of study as a variable because it may vary for UG students compared to the PG students depending on different factors like perceived usefulness, experience using the internet, devices they use to browse the internet, and self-behavioural control.
5. **Internet usage pattern-** The ways, individuals connect to the internet to accomplish particular aims are known as internet usage patterns. When it comes to students in this digital era, their world would be incomplete without the internet.

   A technology's perceived usefulness refers to a person's propensity to use it or not depending on how much they believe it will improve their ability to perform their tasks, and Davis (1989) found that these perceptions were highly predictive of a person's propensity to adopt a new technology.

In Seetharaman's (2012) study, 92.7% of 735 graduate medical students had internet access. Students surf the internet every day (46.2%), and the most frequently used Internet access is at home, dormitory, university library, internet cafe and friends. Students indicated that they use the Internet to search for information (62.9%) and had the highest perceived confidence in tasks involving using a word processor (77.3%) and creating PowerPoint presentations (75.5%). (https://doi.org/10.32381/JPR.2021.16.01.1)

Besides that, factors like net using frequency, place, and time spent on the internet, as well as perceived benefits, vary for each internet user, which in turn affects their vulnerability of the students. Thus, internet usage pattern is a key variable in the current study of cybersecurity awareness among university students in Vadodara, 2022–2033.

6. **Digital competency-** The importance of digital capabilities and technology is growing right now. Digital competence is the ability to use technology and systems creatively, critically, and confidently.

   People with high digital skills can successfully analyse and comprehend online learning materials, whereas those with low digital skills may find it difficult or objectionable. High cognitive strain, school burnout, and eventual abandonment of online learning are the results. (Lopez-Meneses et al., 2020) According to them, college students' performance in higher education depends on their ability to use technology effectively. (Silamut and Petsangsri, 2020). People's digital competency would increase if they were more aware of security issues. Henceforth, in the present study digital competency has been taken as a variable.

7. **Issues encountered during cyber surfing -** The information technology sector values cyber security. There is a serious problem with students of all ages and their peers using new forms of virtual communication excessively to the point that they harm one another over time physically, socially, or psychologically. (Khawrin, M. K. (2022) One of the biggest issues in modern life is information security. Cyberattacks, which are on the rise daily and despite all the precautions, cybersecurity still fills many people with a lot of fear (Dwarakanath, S., Ravi, K., & Vijayakumar, R., 2022)

Students are more vulnerable to many harmful websites and serious cyber threats/risks like ransomware attacks or phishing attacks as they visit more websites for their studies, social networking, entertainment, or e-commerce needs, among other problems encountered during cyber-surfing. Besides that, perceptions of susceptibility to threats, perceived threats, internet knowledge, and self-efficacy may differ between students who have experienced a cyberthreat or attack versus those who have not; consequently, differences in these perceptions, knowledge, skills, and attitudes can shed light on students' cybersecurity awareness level. (Reddy, G. N., & Reddy, G. J. U., 2014). Therefore, issues encountered while cybersurfing have been recognized as one of the key variables in determining students' cybersecurity awareness level.

1.10 Justification of Study in Context of Department of Extension and Communication

Higher education should adapt to the changing demands and challenges resulting from society's rapid social, technological, and other development because young people are the nation's future and the department has conducted number of studies with youth and university students on a range of development-related topics, so empowering them is crucial to building a prosperous country.

The department's curriculum also includes a variety of media & communication-related teaching, research, and community outreach efforts where computer, internet, and other new media-related activities are carried out because communication is a vital component of the department. The internet usage by department students for academic, entertainment, gaming and their purposes is well-known. The researcher decided to conduct this study on students' awareness of cybersecurity due to the study's direct relevance to the department's media and development communication component.

1.11 Objectives of the study

1. To prepare the profile of the selected university students of the Vadodara.
2. To assess the overall cybersecurity awareness among the selected university students of the Vadodara.

3. To assess the overall cybersecurity awareness among the selected university students of the Vadodara with reference to the following variables:
    e) Age
    f) Gender
    g) Type of university
    h) Year of Study
    i) Internet usage pattern
    j) Digital competency
    g) Issues encountered during cyber surfing.
4. To study the differences in the overall cybersecurity awareness of the selected university students of the Vadodara with reference to the selected variables.
5. To assess the cybersecurity awareness using Theory of Planned Behaviour (TPB) constructs viz, knowledge, self-perceptions, actual skills and behaviour and attitude among the selected university students of Vadodara.
6. 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 with reference to the selected variables.
7. To study the co-relations within the TPB constructs viz, knowledge, self-perceptions, actual skills and behaviour and attitude in the context of cybersecurity awareness.
8. To identify the readiness regarding cybersecurity awareness training program of the selected university students of Vadodara.

1.12 Null Hypotheses of the study

1. There will be no significant differences in the overall cybersecurity awareness of the selected university students of the Vadodara in relation to the selected variables.
2. There will be no significant differences in the TPB constructs viz, knowledge, self-perceptions, actual skills and behaviour and attitude among the selected university students of Vadodara with reference to the selected variables.
3. There will be no co-relation within the TPB constructs viz, knowledge, self-perceptions, actual skills and behaviour, and attitude in cybersecurity awareness.

1.13 Assumptions of the study

- Selected university students of the Vadodara will be familiar with cyber security mechanisms.
- Selected university students, Vadodara will vary in their cyber security awareness level according to the above selected variables.
- Selected university students, Vadodara will vary in their knowledge, self-perceptions, actual skills and behaviour and attitudes regarding cyber security according to the above selected variables.

1.14 Delimitations of the study

- The study will be delimited to the selected university of the Vadodara only.
- The study will be delimited to the cyber security awareness only.
- The study will be delimited to the selected and adapted TPB framework viz knowledge, self-perceptions, actual skills and behaviour and attitudes in relation to cyber security awareness only.

1.15 Operational Definition

- **Cyber security awareness:**

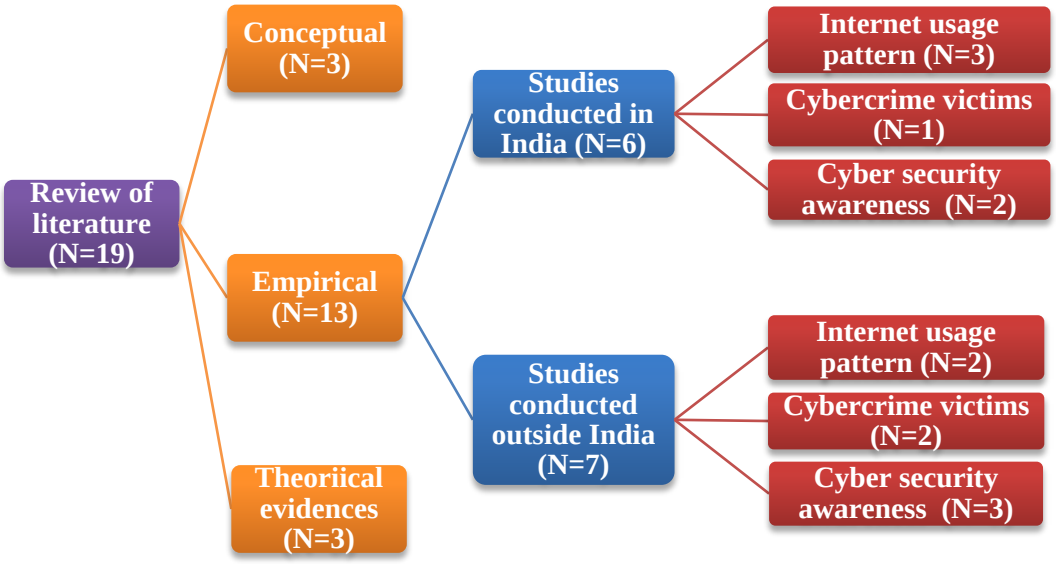
  In the present study, cyber security awareness comprised knowledge, perception, attitudes and actual skills of the students towards best cyber security activities. It refers to being aware of one's regular online actions, making sure one is aware of common hazards and the best strategies to avoid them. This also entails having a thorough awareness of how digital attacks may affect one's personal data, the position of their organisation, and their consumers.
  (https://aiict.edu.au/blog/what-is-cyber-security-awareness-and-why-is-it-important/

CHAPTER 2
REVIEW OF LITERATURE

CHAPTER 2

REVIEW OF LITERATURE

A current study was carried out to understand **"Cybersecurity Awareness among the university students in Vadodara, 2022–23".** The field of cybersecurity is vast and dynamic. In this study's literature review part, several cyber security awareness are connected to past work are covered. It expands on the Cyber Security Awareness (CSA) issues and awareness-related information, attitudes, and perceptions that had been investigated in past studies. This makes it easier to understand the overall relevance and goal and establishes a link between the current research study and past research on the issue.



2.1 Conceptual Reviews

The Indian Express (2022) in an article **"18 out of every 100 Indians victim of data breaches: Surf Shark"** mentioned that In a country with strict data protection laws where data breaches over the past 18 years have led to the loss of approximately 962.7 million people's contact information, The Indian

Express (2022) noted that "the first recorded digital attack and risk in 2004. India has become a center for cyber-attacks, ranking as the sixth most breached nation India's breach rate has increased from 5 to 42 hacked accounts per minute just two months into the quarter as of June 2022, a 740 percent increase over 2022 Q1. If there aren't enough protective measures in place within Indian jurisdiction, there could be a lot of data collection that results in even more security breaches throughout the country, the business stated in its research (T. Desk, 2022). (https://indianexpress.com/article/technology/tech-news-technology/18-out-of-every-100-indians-affected-by-data-breaches-surfshark-7967560/)

The Times of India (2022) reported that "India, the United States of America, the United Kingdom, Indonesia, and Brazil are the countries that are most frequently the target of cyberattacks on internet platforms and educational institutions. Remote learning is among the key triggers: Report." Ransomware attacks against prestigious organizations like Harvard University and the University of California are among them. In Asia and the Pacific last year, 58% of threats were made against academic institutions and online platforms in India or with ties to India. The United States accounted for 86% of the threats in North America, placing second overall in terms of impact. (Pti, 2022b). (https://timesofindia.indiatimes.com/india/indian-education-sector-biggest-target-of-cyber-threats-remote-learning-among-key-triggers-report/articleshow/91234420.cms)

According to a 2016, **Computer Weekly article** titled "Most Students Say Cyber Security Is a Growing Threat," which stated that "77% of college and university students understand the value of cyber security and believe that it is an increasing risk. Less than 20% of respondents indicated they are concerned about cyber security, and only 35% believe it is their responsibility to become knowledgeable about it. Less than 20% of respondents indicate they are concerned about cyber security, and only 35% believe it is their obligation to become knowledgeable about it. According to research from the digital education services company Jisc, undergraduates and other students in higher education are becoming more aware of cyber security as a result of media coverage of cyberattacks on significant corporations (McDonald, 2016).

(https://www.computerweekly.com/news/4500278781/Most-students-say-cyber-security-is-a-growing-threat)

2.2 Empirical Reviews

For the current study, the researcher looked over a variety of literature sources from both the national and international levels. Studies from Indian states viz, Delhi, Gujarat, Tamil Nadu, Karnataka, and West Bengal, as well as reviews from around the world viz, Saudi Arabia, Malaysia, California, Mogadishu, Nigeria, and Indonesia, were included as empirical reviews of studies carried out both inside and outside India in the current study. The following categories also apply to the studies mentioned as under -

(1) internet usage pattern

(2) cybercrime victims

(3) cybersecurity awareness

1. Studies related to Internet Usage Pattern

a) Studies conducted on Internet Usage Pattern in India

Nagpur A. (2020) conducted a study entitled **"Internet Addiction and Mental Health among University students during COVID-19 lockdown",** "to find out the difference in Internet Addiction & Mental Health among 166 undergraduate university students of professional courses across gender & semester. For data collection questionnaire was used. The findings showed that, in comparison to other groups, male respondents in their final semester were substantially more likely to develop an internet addiction, compared to students in the intermediate semester, university students in their final semester were more likely to experience mental health issues. The findings also indicated that male students had poor mental health and a significant level of Internet addiction. In the COVID-19 scenario, students from the previous semester performed very well for internet addiction and mental health concerns. This study found a connection between internet addiction and mental health problems only among male students."

Anand N. et al. (2018) conducted a study entitled **"Internet Use Patterns, Internet Addiction, and Psychological Distress among Engineering University Students: A Study from India."** In this study, "1086 students from Mangalore in southern India who were pursuing bachelor's degrees in engineering were examined for their internet use habits and Internet Addiction (IA) and their relationships with psychological discomfort, particularly depressive symptoms. The socio-educational and internet use behaviours were evaluated using the internet addiction test (IAT). The self-report questionnaire (SRQ-20) was used to measure psychological distress, specifically depressive symptoms, while the A data sheet was used to compile statistics on internet usage and demographics.

The study's findings showed that-

- Engineering students that matched the criterion for mild online addiction (27.1%), moderate online addiction (9.7%), and severe online addiction (0.4%).
- Male engineering students were more likely to engage in IA behaviours due to living in leased housing, using the internet, and experiencing psychological discomfort.
- Engineering students with IA can negatively affect their academic progress and professional ambitions.

  It is essential to recognise and treat IA and psychological discomfort in engineering students as soon as possible.Anand et al., 2018)."

  (https://journals.sagepub.com/doi/pdf/10.4103/IJPSYM.IJPSYM_135_18)

Eduljee N. and Kumar S. (2015) conducted a study entitled "**Patterns of Internet Use with Indian Students from Aided and Unaided Colleges"** in Mumbai, India "to understand patterns of internet usage with the 323 higher education institution students from aided and unaided colleges. Questionnaire was used for data collection.

The findings of the study revealed that;

- Compared to students at the aided college, unaided college students were more likely to assess their computer skills better and to have more confidence using computers.

- Internet usage among students from the unaided institution was much higher than that of students from the aided colleges, with both groups of students learning about the internet through independent research (45.7% and 47.6%) and from friends (21.4% and 26.8%, respectively) Less than 1 hour to 4 hours per day was spent by 89.7% of aided college students and 76.3% of unaided college students.
- While unaided students used the internet for learning (57.4%) and research (50.4%), students who received assistance used it for enjoyment (57.0%) and education (43.9%)."

b) Studies conducted outside India on Internet Usage Pattern

Bhatnagar N. & Pry M. (2020) conducted a study entitled **"Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study".** "The objectives of this investigation were to determine how students felt about social media privacy, whether security was important to college students, and whether academic institutions needed to do a better job of teaching students about cyber-security. At a regional campus of a prominent university in western Pennsylvania, 107 students from 10 courses and 18 different academic majors were given a paper-based survey. The study's conclusions showed that:

- The two most extensively used social media sites are Snapchat and Instagram.
- A high degree of security knowledge, with 72.6 percent of students understanding the dangers of having their online profiles publicly visible and 78.5% being aware of how to use the security tools offered by their social media provider.
- Most (71.03%) had not suffered a victimisation.
- The majority (78.09%) use security measures, which is in line with survey questions requirement that respondents indicate whether or not their social media accounts are private."

Hossain, M. , and Rahman, M. (2017) conducted a study entitled **"Comparative Study of Internet Usage Among University Students: A Study of the University of Dhaka, Bangladesh,"** aimed to compare internet usage and overall perception of the internet among students of different disciplines (such as business studies, sciences, and arts) at the University of Dhaka.

- At the University of Dhaka, 100%, 92%, and 90% of students with backgrounds in business studies, science, and the arts, respectively, use the internet. • Of the respondents, 64% have backgrounds in business or science, 54% have backgrounds in science, and 36% have backgrounds in the arts.
- 34% of respondents with business studies backgrounds, 22% of respondents with science backgrounds, and 40% of respondents with arts backgrounds report spending 1-2 hours online daily.
- The majority of respondents with a business or science background use the internet for educational, communicative, recreational goals.

2. Studies related to Cyber Crime Victims

a) Studies related to cybercrime victims in India

Sen A. (2013) conducted a study entitled **"Linking Cyber Crime to the Social Media: A Case Study of Victims in Kolkata"** aimed "to identify main victims of cyber stalking, to explore issues of privacy in the electronic space and inquiries into the role of social networking sites in preventing cyber stalking and to seek insight into virtual community relationships and their features in relation to cyber stalking. It was a qualitative study. Focused group interviews and a semi-structured interview schedule were used to gather the data. Using purposive sampling method, 22 samples were collected from selected high school, graduate and postgraduate students of Jadavpur University, Kolkata.

- Due to the stalkers' anonymity and the disclosure of personal information in public accounts, several of the respondents have also been the targets of online stalking and harassment.
- There have been cases where the attackers continued to send the responders unwelcome messages even if they were not on the respondents' friend list.
- Along with that, unwelcome persons attempted repeated friend requests, made vulgar comments, and tried to force contact. Furthermore, it can be inferred from their perspectives, whether or not the victim ever really encounters the harasser, the psychological ramifications of cyberstalking can be devastating, resulting in verifiable psychological disaster and damage."

(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)

b) Studies related to cybercrime victims outside India

Igba I. D. et al. (2018) conducted a study on "**cybercrime among university undergraduates: Implications on their academic achievement**". "Online questionnaire was used to conduct a cross-sectional survey of education faculty students. 207 students from the faculty of education made up the study's sample. The findings revealed, among other things, that college students view cybercrime as a tool for self-improvement. It was noted that there was more work to be done to create a reliable, secure, and safe network environment. This suggests that in order to make undergraduates more valuable in life, value reorientation should be forced upon them. The end result should expose both students' and professors' eyes to the most advantageous methods of utilising internet services to take advantage of the globalised environment without necessarily abusing it."

Yu S. (2014) conducted a study on **"Fear of Cyber Crime among College Students in the United States: An Exploratory Study".**"This study covered a total of four cybercrimes: online fraud, cyberbullying, computer viruses, and digital piracy. Perceived victimisation risk, perceived crime severity, and prior victimisation were the three primary independent variables. They were all evaluated specifically for each crime. The control variables were age, gender, and race. The fear of cybercrime is the dependent variable. An online survey was carried out in an anonymous manner. College students enrolling in general education classes at an urban institution in the Midwest of the USA were recruited and a total of 270 valid responses out of 519 student responses were recorded for analysis. He concentrated on how three key factors—perceived crime seriousness, perceived victimisation risk, and victimisation experience—relate to the fear of crime and cybercrime. The study found that the predictors for fear of cybercrime varied depending on the offence. The fear of cybercrime is exacerbated by internet usage."

3. Studies related to cyber security awareness

a) Studies related to cyber security awareness in India

Senthilkumar. K. & Sathishkumar E. (2017) conducted a study entitled "**A Survey on Cyber Security awareness among college students in Tamil Nadu",** "to evaluate students' knowledge of internet security hazards while analysing their cybersecurity awareness in Tamil Nadu. The survey conducted using questionnaire in 5 major cities that are randomly taken. Sample size of the study was 379 students who were selected using purposive sampling.

The findings of the study were as follows;

- Over 70 percent of students across all cities were aware of the most common types of virus assaults and use antivirus software or Linux operating systems to protect their systems. The remaining students do not use antivirus software and are thus vulnerable to malicious viruses.
- Although 11% of the respondents are using antivirus software, they are not upgrading it. Over 97% of the respondents don't know where the infection came from.
- More than sixty percent of students across all cities reported receiving phishing emails or messages. However, the proportion of people who get phishing emails or messages differs by city.
- The Tamil Nadu college students are estimated to be 69.45% aware of cyber security, with men making up 38.6% and women making up 30.85%.
- According to the survey results, Tamil Nadu's college students have a higher than average degree of understanding of cyber-related threat issues, which can help them defend against cyberattacks."

Narahari A. & Shah V. (2016) conducted a study entitled **"Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India)".**

"The study's objectives were to determine the degree of online users' awareness of cybercrime and to develop a framework for sustaining online users' awareness campaigns to combat cybercrime and promote online security. In-depth interviews

and questionnaire were used respectively for data collection. The 100 Anand-based young internet users were chosen using the purposeful sampling method.

Findings of the study were;

- Cybercrime targets crucial infrastructures with political motivation, with 10% targeting educational institutions and 50% targeting the commercial sector.
- Nine out of ten respondents claimed to have had their identity stolen, whereas 91% of internet users disagreed.
- While 52% of respondents acknowledged they are cautious when sharing personal information, 48% of respondents admitted they disclose their personal information with people they don't know well.
- Of the respondents, 42% believe that posting photos on social networking sites is not risky, while 58% believe that it is.
- Sixty-seven percent of consumers report frequently receiving phishing emails requesting for sensitive information like their address, bank account number, or mobile number.
- Half of people have been the target of phishing phone calls.
- The study demonstrates that Anand internet users lack a thorough understanding of current cybercrimes and cyber security.
- The lack of understanding about securing PCs and laptops is serious, with nearly half of participants still suffering from viruses, not changing passwords, and sharing private data. If the government does not make serious efforts, ignorance about this issue may grow."

b) Studies related to cyber security awareness outside India

Alharbi, T., & Tassaddiq, A. (2021) conducted a study entitled **"Assessment of Cybersecurity Awareness among Students of Majmaah University"** aimed "576 undergraduate students at the University of Majmaah were investigated to explore and evaluate their degree of cybersecurity awareness and user compliance using a scientific questionnaire based on numerous internet usage safety aspects. The snowball sampling method was employed.

The study's main findings were;

- 41% of students automatically applied updates, while 17.6% chose to ignore or not upgrade, leaving their devices open to intrusions.
- 21 percent of respondents were unaware of the risks of downloading free software from reputable sources.
- Only 22% of the students did not know what two-factor authentication was or how it gave an additional layer of protection.
- The students had no idea how to send emails securely and safely.
- 75% of users' access emails from public Wi-Fi without protecting the connection or using a VPN.
- About 60% of users frequently check the security parameters and settings of their online browsers and are aware of how to identify unusual behaviour in their browser history.
- 56% of the students never posted their location publicly on social media and always kept it private.
- Nevertheless, more than 70% of those polled in this survey were able to disclose any threat they encountered.
- The respondents' understanding of cybersecurity was average."

Garba A. et. al (2021) conducted a study on **"An assessment of cybersecurity awareness level among North-eastern University students in Nigeria"** aimed "to identify the level of cybersecurity awareness of the 441 students in North-eastern Nigeria. Adamawa, Borno, Bauchi, Gombe, Taraba, and Yobe are among the states included in the survey.

Major findings of the study were as follow;

- 49.7% of students make sure they are familiar with the seller before making purchases, while 5.2% make an online payment without doing so.
- A sizable portion of students (40%) worry that their accounts will receive any kind of undesirable information.
- 42 percent of respondents said they would definitely examine any friend requests before accepting.
- About 50% of respondents agreed, while 50% disagreed, that making new internet acquaintances alone is a good idea.

- 56.2% of respondents stated they could meet a friend they made online with their parents' consent; this indicates that parents are aware of the dangers of meeting strangers and is a wise precaution to take in order to avoid kidnapping or harassment.
- Sixty-three percent of respondents agreed that it is inappropriate to criticise someone for posting a provocative image on social media, while only a small percentage of respondents (8.6%) disagreed with the question.

This study found that almost 60% of respondents expressed satisfaction with their use of the internet, suggesting that poor cybersecurity knowledge can lead to cyberattacks. It is important to receive good instruction on how to use the internet properly without falling victim to a cyber danger. It is urgently necessary to design and implement effective cybersecurity awareness programmes to address these issues and prevent students, particularly female students, from being victims of cyberattacks."

Moallem A. (2019) conducted a study entitled **"Cyber Security Awareness among College Students"** aimed "to investigate student awareness and attitudes towards cyber security and the resulting risks among the most advanced technology environment: California's Silicon Valley. The sample size for the study was 247 students. The data was gathered using questionnaire.

The findings of the study are as follows;

- Bank account information ranked first among the respondents' most private data (20%), then contact information (17%), photographs (15%), location (15%), and the IP address of the device (14%).

Again, there were no significant differences between the populations of women, men, and different age ranges.

- Fifty percent of the respondents responded that they have rejected the permission (54% females and 49% males),
- Sixty-two percent of respondents have reason to believe that they have been observed online without their consent.

When it comes to perceptions of data security in university systems, 8% believe their data is safe (5% women vs. 10% men) 57% believe data is relatively safe in

university systems (66% 53% men), 21% said it was unsafe (18% women and 25% men) and 13% were unsure.

According to the survey's findings, college students still do not have a good understanding of how to protect their data, even if they believe that they are watched when using the Internet and that even university networks are not secured."

2.3 Studies based on various theories and model

Moletsane, T., and Tsibolane, P. (2020) conducted a study titled "Mobile Information Security Awareness among Students in Higher Education.", in order to determine the effects of behavioral determinants on higher education students' awareness of mobile device security, specifically, information security knowledge, attitudes toward information security, normative views about information security, and intention for information security. This study provides a conceptual framework that incorporates ideas from the Knowledge-Attitude-Behavior (KAB) model and the Theory of Planned Behaviour (TPB) model for measuring mobile information security awareness and evaluated the factors influencing students' awareness of mobile security at a higher education institution in South Africa.

- The results showed a strong relationship between students' levels of security awareness and their understanding of and behavioral intentions toward information security issues.
- The less respondents appear to have favorable views towards mobile security, such as forming secure password habits, the more respondents claim to be aware of the risks associated with cyber-security.
- Despite learning about cyber-security issues, the students' opinions of their online vulnerability did not appear to change.
- After learning about cyber-security risks, students' intentions to exercise greater caution, such as adhering to the university's online safety rules, did not seem to improve.

- The study also showed the gap between knowledge of security and the absence of concurrent safety practices, which was associated with intentions to act more cautiously online

Alanazi, M., et al. (2022) conducted a study on "**Exploring the factors that influence the cybersecurity behaviour of young adults".** He stated that, Understanding how young adults use cybersecurity and identifying the policies and variables that can lessen cyberthreats are crucial. To forecast young adults' behavioural intent to engage in cybersecurity behaviors, it combined the main concepts of the theory of planned behavior (TPB) with additional characteristics, such as perceived awareness and knowledge. he results showed that the intentions of young adults to engage in cybersecurity behaviour (IPC) were significantly influenced by attitude (ATT), subjective norm (SN), and perceived behavioural control (PBC) after online surveys were used to collect information from 1581 young adults enrolled in Technical and Vocational Training Corporation (TVTC) colleges in Saudi Arabia.

Future research may benefit from examining socio-demographic and cultural factors that may affect CSB, as well as perceived awareness of the implications of cyberthreats and the necessity of cybersecurity behavior (PCST), which was also crucial for IPC. PBC was not directly related to engaging in cybersecurity behaviours, whereas PCST and IPC were associated with cybersecurity behaviours, although PBC was not."

Skinner, W. F., & Fream, A. M. (1997) conducted a study entitled **"A social learning theory analysis of computer crime among college students"**. Using a multistage sample of Southern University students, the researchers first looked at the lifetime, recent year, and recent month occurrences of five different illegal computer activities: using hacking software, guessing passwords to gain access, gaining access to browse the internet without authorization, gaining access to modify information, and writing or using programs that damage computer data, such as viruses. In addition, given the paucity of studies examining the causes of computer crime, researchers look at how well the social learning theory can account for these behaviors (Akers, 1985).A confidential self-administered

questionnaire was given to a sample of 581 undergraduate students at a major southern state university using a multistage sampling technique. Multivariate analysis showed strong support for social learning theory as a conceptual framework for understanding computer crime in general, but only weak support for the idea as an explanation for a few specific types of computer crime, such as gaining unauthorized access to browse other people's computers (Skinner & Fream, 1997).

(https://journals.sagepub.com/doi/abs/10.1177/002242789703400405?journalCode=jrca)

2.4 Trend Analysis

2.4.1 Overall Trends Analysis

- The reviewed studies were from the duration of 1997-2022
- International studies referred were from countries viz, Bangladesh, Saudi Arabia, Malaysia, USA, Somalia, Nigeria, South Africa and Indonesia; whereas from within India the researcher could come across majority of the studies from eastern and southern region, viz, Delhi, Gujarat, Tamil Nadu, Karnataka, Maharashtra, West Bengal were referred for the present study.
- In the reviewed studies sample size was ranging from 100 to 1597.
- The referred studies have used quantitative and qualitative research approaches. The methods used to collect data were through survey, interview and focus group discussion.
- In majority of the studies have used purposive and snowball sampling technique.
- The majority of the reviews from the referred articles suggest that cybercrimes and attacks are becoming more common in India and globally each and every day.
- The majority of the reports show that students and the general public are not aware of cybersecurity issues.
- The referred literature revealed that education sector particularly higher education institutions are most targeted than other organizations for cyber-attack.

2.4.2 Trend Analysis of studies related to Internet Usage Pattern

Within India as well as outside India trend shows that, out of the referred studies,

- to access internet students use their smartphone.
- spent more than three hours online each day.

- majority of the students used the internet for their enjoyment, education, educational, social, recreational, and financial purposes.

2.4.3 Studies related to Cyber Crime Victims

Within India as well as outside India trend shows that, out of the referred studies,

- majority of the studies revealed that students accept friend request of stranger person.
- majority of the studies revealed that total number of cybercrime victims are increasing in India.
- a few of the participants had experienced cyberstalking.
- cyberbullying has been identified as the most concerning issue throughout the time

2.4.4 Trend Analysis of studies related to need for cyber security awareness

Within India as well as outside India trend shows that, out of the referred studies,

- respondents were aware of hacking, but very few were also aware of other cyberattacks including phishing, cyberstalking, and defamation.
- uninformed of the risks associated with installing free software from untrustworthy and unidentified sources.
- they were using an antivirus but did not updating the software; careful in case of sharing personal information.
- students had absolutely no idea what two-factor authentication was.
- students kept their location confidential and also never disclosed it publicly on social media.
- students knew how to report any threat they faced.
- students believed that their data is secure in university systems.

2.5 Research Gaps

After an assessment of the available research, the following research gap was found:

- Out of the referred studies within India the majority of the studies have been seen only from eastern and southern India and few from northern & western India except i.e., from Delhi and West Bengal.

- While reviewing the literature, the researcher did not come across any studies regarding cyber security awareness among university (government and private) students conducted in Gujarat state.
- The review of the literature revealed that there is a high need for cybersecurity awareness among the people, particularly youth and students who use the internet the most. Researcher has not come across the research so far regarding cyber security awareness conducted in Vadodara city.

2.6 Conclusion

Although studies on internet usage patterns were conducted in Gujarat, it was found that none specifically focused on cyber security awareness among university students, especially in the Vadodara. In the current world, where social media platforms and internet usage are increasing daily, the current research shows that cyber security awareness among university students is a growing concern. So, a study on "**Cybersecurity Awareness among the University Students in Vadodara, 2022–2023**" would help to identify university students' internet usage patterns and their awareness level regarding cybersecurity.

CHAPTER 3
METHODOLOGY

CHAPTER 3

METHODOLOGY

This study aims to investigate the "**Cybersecurity awareness among the university students of Vadodara, 2022-2023."**

Icek Ajzen developed the Theory of Planned Behavior (TPB) in an attempt to predict human behavior (Ajzen, 1991). It is a psychological theory that connects beliefs and behaviors. 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 operational definition of the cybersecurity awareness in the present study, the most fitted Theory of Planned Behavior (TPB) framework used by Chandarman R. & Van Niekerk, B. (2017), in their study entitled "Students' Cybersecurity Awareness at a Private Tertiary Educational Institution" has been adapted in the present study. (https://doi.org/10.23962/10539/23572)

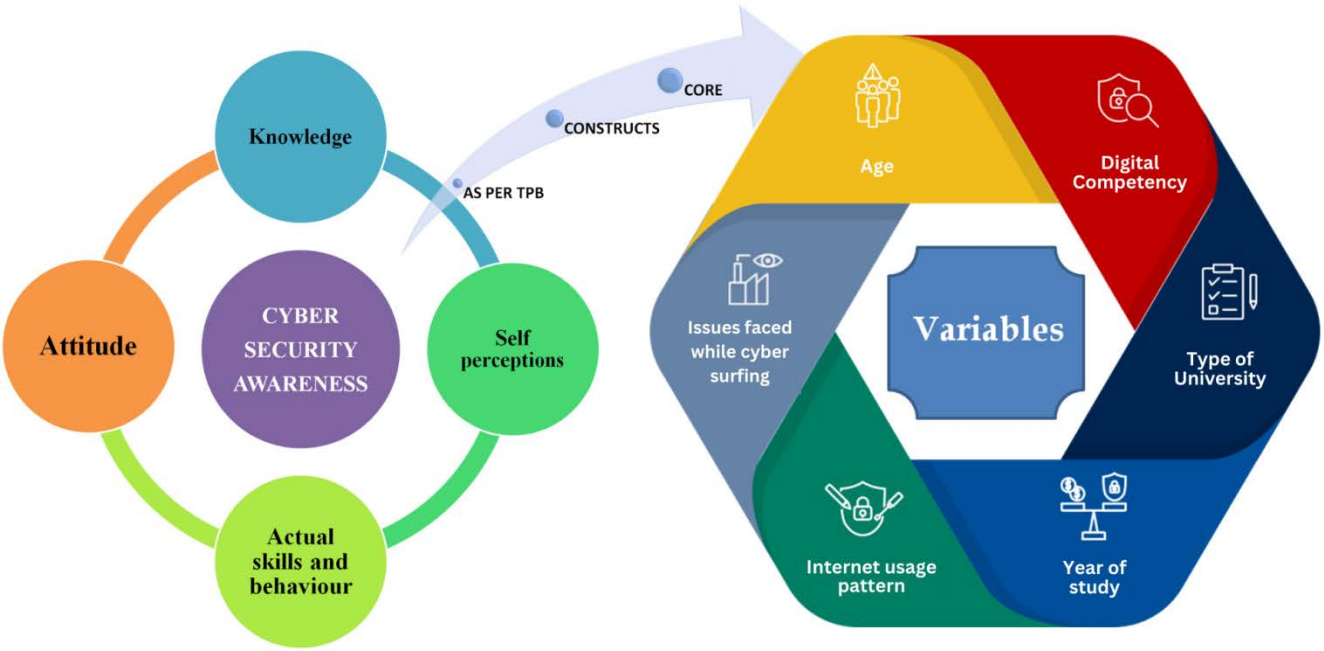
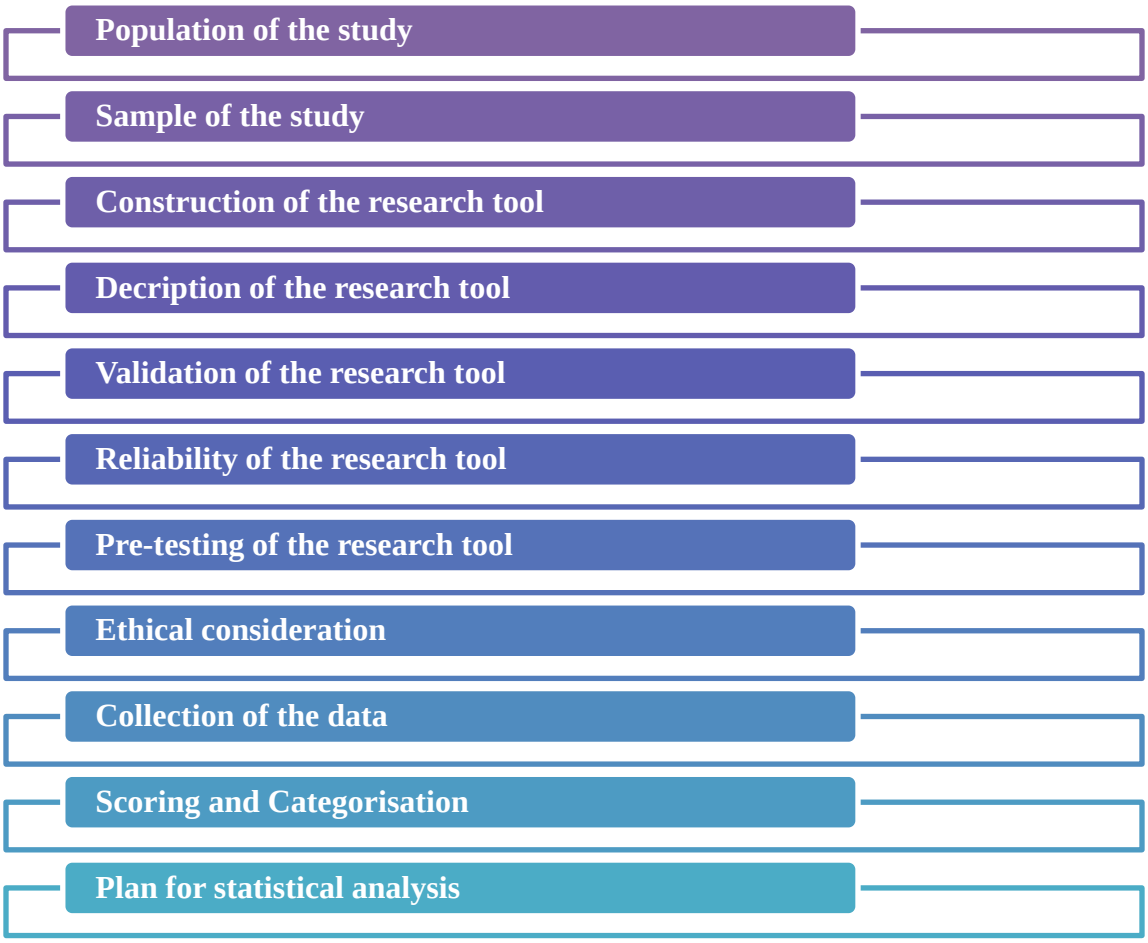


Figure 3: Conceptual framework of the present study

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



3.1 Population of the study

The population of this study include students from selected government and private universities accredited by the University Grants Commission (UGC) of Vadodara for 2021-2022.

3.2 Sample of the study

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

3.2.1 Selection of the sample

This study is exploratory in nature. In order to investigate cybersecurity awareness among selected university students in Vadodara, the survey method was adopted. Data is

collected using a non-probability sampling method known as the snowball sampling technique. To obtain a sample of 242 people, the researcher contacted all known respondents by phone, WhatsApp and in person.

3.2.2 Criteria for selection of the sample

- **Inclusion criteria**

  a. Those students who study in the selected U.G.C. recognized government and private universities of Vadodara city only in the year 2022-23.

  b. Those students who give consent for the study.

  c. Those students who are using the internet.

- **Exclusion criteria**

  a. Those who do not give consent.

  b. Those students who are not studying at selected universities in Vadodara city.

  c. Those who do not have access to a digital device.

  d. Those who do not have access to the internet.

3.2.3 Sampling unit

The geographical area from which the sample is collected is referred to as the sampling unit. Undergraduate and postgraduate students were taken as a sample for the current study from the selected government and private higher education universities of Vadodara city, Gujarat.

3.2.4 Sample size

The research sample consisted of 242 respondents from the above selected universities. The university population was gathered from the two universities' official websites, The Maharaja Sayajirao University of Baroda, and Parul University of Vadodara, in order to determine the sample size for the study. With a total population size of 75,245 of both the selected universities of Vadodara city, 95% confidence level, and 6.3% marginal error, the sample size of 242 is planned. To calculate sample size “Cochran’s sample size formula” has been used:

$\boldsymbol{n = z^2 \times \frac{(pq)}{e^2}}$ Where, $\boldsymbol{n}$ = sample size

$\boldsymbol{z}$ = standard error associated with the chosen level of confidence

p = the (estimated) proportion of the population

e= is the desired level of precision (i.e. the margin of error), ***q***= 1 – p.

3.3 Construction of the Research Tool

The researcher developed a structured questionnaire tool in the English language regarding cybersecurity awareness which sought information related to demographic profile, internet usage pattern, a scale for digital competency, a knowledge test, a self-perception scale, actual skill and behavior as well as an attitude scale for the present study's data collection. A google form was also created for the data collection.

The questionnaire was developed after referring relevant literature, books, and websites, situational narratives on real-life incidents from the students /people, as well as using readymade tools from previous research regarding cyber security awareness.

3.4 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: (I) Demographic details and (II) The subscales of the Theory of planned behavior (TPB) model.

(I) Demographic information included age, gender, year of study, internet usage pattern, and digital competency. The tool of digital competency was adapted using the "modified version Digital Competence Assessment Framework (DIGCOMP) by Evangelinos G & Holley D(2015)" used for the current study. (http://eprints.bournemouth.ac.uk/23477/)

(II) The sub-scales of TPB constructs viz a knowledge test, self-perception scale, actual skill and behavior as well as attitude scale items were prepared based on the CIA (Confidentiality, Integrity, and Availability) Triad model. In all four constructs, cyber security dimensions viz., password security, network security, website security, system security, social networking site security, and operational security related questions and statements were covered in the questionnaire. Moreover, the question regarding the readiness of participants to take cybersecurity awareness training was also included. A detailed description of each of the seven sections is given below.

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
	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 behaviour	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
Section G	Student's readiness regarding cybersecurity awareness training.	4	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.

Details of research tools prepared and used for data collection from selected university students of Vadodara city are as follows;

(I) Demographic and other details

Section A – Demographic profile of the respondents

This section was comprised of questions that give information about the university student's background, which includes their age, gender, name of the university, type of university in which they study, and year of study. These were also the independent variables for the present study. However, information related to their email ID, mobile number, stream or specialization, and program in which they study was also sought as other background information.

Section B: Part I – Internet Usage Pattern

In today's digital era, the most common daily regular activity is using the internet. Daily, majority of the people of all ages, nationalities, backgrounds, and social status use the Internet. To know more about how university students use the internet, this section includes information on their internet usage patterns. This section comprised nine (9) multiple-choice questions, in which the respondents were asked for information about how long they had been using the internet, the devices they used to connect, the locations where they accessed it, the types of accessibility available, how often they used it, why they used it, the information they collected, accessed, or stored for easy access to daily tasks, and information specific to their social networking accounts.

Section B: Part II – Digital Competency

A set of abilities known as digital competency is necessary for the proper, critical, and creative use of digital technology to accomplish goals in the fields of education, employment, leisure, and inclusion or participation in society. The tool of digital competency was adapted from the modified version "Digital Competence Assessment Framework '(DIGCOMP)' framework by Evangelions G & Holley D, 2015" (http://eprints.bournemouth.ac.uk/23477/) and used for the current study. This framework comprised information on five different sections, viz, literacy in information and data, cooperation and communication, production of digital material, safety, and problem-

solving. Below given are several dimensions contained in each of DIGCOMP framework section.

Table 2: Digital competency areas and dimensions

Sr. No.	Area	Dimensions
1.	Information and data literacy	• Browsing, searching and filtering data, information and digital content
		• Evaluating data, information and digital content
2.	Communication and collaboration	• Interacting through digital technologies
		• Sharing through digital technologies
		• Engaging in citizenship through digital technologies
		• Collaborating through digital technologies
3.	Digital content creation	• Developing digital content
		• Integrating and re-elaborating digital content
4.	Safety	• Protecting devices
		• Protecting personal data and privacy
5.	Problem solving	• Solving technical problems
		• Identifying needs and technological responses
		• Creatively using digital technologies
		• Identifying digital competence gaps

[Adapted from modified version of "DIGCOMP by Evangelions and Holley, 2015" (http://eprints.bournemouth.ac.uk/23477/)**]**

This section consisted of fifteen (15) statements. The level of digital competency was evaluated using a three-point rating scale.

Section B: Part C – Issues encountered during cyber surfing

Cybersecurity is a top concern in every sector. Today, one of the biggest difficulties faced by modern society is information security. The overuse of different forms of virtual communication by students of different age groups and their peers, which harms individuals physically, socially, or psychologically through repeated and persistent actions, is a grave issue.

This section is comprised of questions related to issues encountered during cyber surfing by the respondents. It consisted of a total of seven (7) questions regarding cyber victimization, issues faced while surfing, reporting of cyber victimization, and the possibility of being victimized in the future.

This has been considered as one of the variables initially when the study was framed, however after data collection due to skew data this particular variable has been dropped as a variable and information has been considered as other background information.

Subscales of the Theory of Planned Behaviour

Section C – Student's cybersecurity knowledge

Knowledge of cybersecurity is a key part of protecting oneself against malicious attacks, data breaches, and other cyber threats. This part of the questionnaire included a knowledge test on cybersecurity awareness. To assess the degree of comprehension among university students in the city of Vadodara, researcher developed a cybersecurity awareness knowledge test. This section consisted of fifteen (15) MCQs (Multiple Choice Questions) related to cybersecurity, ensuring CIA Triad model base focusing on six main security elements as stated above.

Section D – Student's self-perception of cybersecurity skills

Students' self-perceptions of cybersecurity skills, have a significant impact on the types of activities they participate in, the number of efforts they put into them, and the likelihood they will participate in those activities in the future. A single security breach might expose the confidential data of billions of people.

Therefore, this section consisted of statements to ascertain the self-perceived cybersecurity skills among the selected university students of Vadodara city. The statements in this section included both positive and negative perspectives about

cybersecurity actions involving digital devices owned/used by the individual or family, cybersecurity acts for academic, entertainment, and social purposes, and others. However, it revolved around the CIA Triad Model and also emphasized the key security components, including operational security, network security, website security, system security, and security for passwords.

The measurement of self-perception was done using a three-point rating scale that consisted of fourteen self-perceived statements about cybersecurity skills. The 3-point Likert-type scale, with a scale from 1 (less extent) to 3(to a great extent), was applied for positive statements. Items with negative wording got a reversal score. Scores that are higher indicate that the reporting self-perceptions more under one's control.

Section E – Student's actual cybersecurity skills and behaviour

This section comprised information regarding actual cybersecurity skills and behaviour if students were to face those situations.

The questions in this section focused on the student's actual cybersecurity skills and behaviour while utilizing internet of things. Situation based multiple-choice questions (MCQs) about cybersecurity were developed after reviewing many websites, books, articles, narratives collected from victims in real-life situations, and previous research studies. Situations were framed in the different dimensions of cybersecurity keeping in mind the CIA Triad model.

Section F – Student's cybersecurity attitude

Student's attitude about cybersecurity may influence their awareness. With certain level of awareness when one gets engage in a specific act, an individual's attitude might be either positive or negative. Therefore, the statements in this section were used to ascertain the attitude of cybersecurity awareness among the selected university students in Vadodara. The statements in this section included both positive and negative attitudes on cybersecurity acts. However, the items were prepared to keep in mind CIA Triad Model and also emphasized the above state six key security components.

A three-point rating system was created to evaluate attitudes toward cybersecurity awareness. The data were scaled on a 3-point Likert-type scale with a range of 1 (less

extent) to 3 (great extent). Items with negative wording received a reversal score. A positive attitude towards cybersecurity was indicated by higher scores.

Section G - Student's readiness regarding cybersecurity training

This section comprised questions on students' readiness to undertake cybersecurity training. To identify the students' readiness regarding the cyber security awareness training program, open-ended questions and MCQs (Multiple Choice Questions) were included which contain four (4) questions related to readiness regarding cybersecurity training in this section.

3.5 Validation of the research tool

The tool was given to seven experts, amongst which three (3) were teaching faculties from the Department of Extension and Communication, two (2) were teaching faculties from the Faculty of Family and Community Sciences, and two (2) were from the field of computer science. This tool is provided to the experts to assess the effectiveness of content based on relevance, logical order, use of language, and appropriateness of response systems. Suggested modifications were made in the tool as per feedback received from experts.

3.6 Reliability of the research tool

To assure internal and external consistency, the tool's reliability was assessed.

- The Cronbach's Alpha coefficient test was used to measure internal consistency.

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 internal consistency of the questionnaire is reliable, significant and acceptable for further research.

- The test-retest method was used to assure external consistency.

The reliability of the questionnaire was evaluated with the test-retest method.16 students from Vadodara city's universities, both government and private, were the given the research tool.

The same tool was provided to the same sixteen (16) students of Vadodara's government and private universities again after ten days to assess the tool's reliability.

Karl Pearson's formula was used to determine the correlation coefficient.

$r = \frac{\Sigma XY}{\sqrt{\Sigma x^2 \Sigma y^2}}$Where, X= Responses of the respondents to whom the questionnaire was administered for the first time.

Y= Responses of the respondents to the questionnaire was re-administered.

The result of the reliability test was found to be 0.851.

3.7 Pre-testing of the Research Tool

Ten university students from Vadodara City cooperated in the tool's pre-testing. In order to evaluate the questionnaire's clarity, a pre-test of the tool was conducted. It was done to evaluate the language's clarity and determine how long it would take to complete the form. The tool was made simple and understandable by removing ambiguous items which were found. On average, 13–15 minutes were needed to complete the questionnaire.

3.8 Ethical Approval of the Study by IECHR Committee

The study was presented to IECHR Committee for ethical approval on 24th November 2022. It was approved by the ethical committee with ethical approval number IECHR/FCSc/M.Sc./2022/18.

3.9 Data Collection

To study cyber security awareness among the university students of Vadodara city, 2022-23, the data was collected from 242 university students aged between 18-28 years of Vadodara city by the researcher from 25th of November to 13th December 2022. The data was collected 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. Out of total 252 distributed questionnaires, total 10 incomplete/ invalid questionnaires were excluded and considered 242 valid tools for formal data analysis. 139 samples were collected through online mode, whereas 103 were collected using offline mode. In total, 116 male students and 126 female students submitted valid responses.

Questionnaires were excluded in further analysis which found incomplete, ambiguous were dismissed.

3.9.1 Difficulties faced while collecting the data

a. Respondents required constant repeated reminders.

3.9.2 Tabulation of Data

a. Data were coded in accordance with the conclusions on the response scores, as discussed below.

b. The researcher created excel spreadsheet for the same purpose.

3.10 Scoring and Categorization of the Data

3.10.1 Scoring and Categorization of Variables

The various components contained under the various parts of the tools were given varying weightage using various scoring procedures.

Table 3: Categorization of variables of the study

Sr. No.	Variables	Basis		Categories
1.	Age	18-23		Young
		24-29		Old
2.	Gender	Male		Male
		Female		Female
		Other		Other
3.	Type of University	Government (as per UGC list)		Government
		Private (as per UGC list)		Private
4.	Year of study	Undergraduate	First year	First year
			Second year	Second year
			Third year	Third year
			Fourth year	Fourth year
			Fifth year	Fifth year
		Post-graduate	First year	First year
			Second year	Second year
5.	Internet usage pattern	Below mean		Moderate users
		Mean and Above mean		Heavy users
6.	Digital competency	Lower level of competency		Beginner
		Medium level of competency		Intermediate
7.	Issues encountered during Cyber surfing	Dropped as a Variable after data collection		

3.10.2 Scoring and categorization of Internet usage pattern

To measure student's internet usage pattern multiple questions were prepared. For each response score was given. Following was the procedure for scoring internet usage pattern in the study:

Table 4: Scoring of data for Internet usage pattern

Type of statements	Minimum score	Maximum score
Multiple choice questions	9	50
Total	**9**	**50**

Hence, the minimum and maximum score for the internet usage pattern were 9 and 50 respectively. Each student's overall score was determined. The respondents were then categorised as follows depending on their final scores.

Table 5: Categorization of scores in internet usage pattern

Variable	Range	Basis	Categories
Internet usage pattern	9-29	Below mean	Moderate use
	30-50	Mean and Above mean	Heavy use

Respondents who scored below the mean are moderate users, and a high score, i.e., above the mean, represents heavy use of the internet.

3.10.3 Scoring and categorization of digital competency

A 3-point rating scale was developed to measure the competency level of selected university students in the city of Vadodara on the Internet of Things (IoT). The scoring pattern for statements was as follows:

Table 6: Scoring of data for Digital Competency

Total no. of items	Minimum score	Maximum score
15	15	45

Total score was fifteen. The lowest and highest score was 15 - 45.

Table 7: Categorization of scores in digital competency

Variable	Range	Basis	Categories
Digital Competency	15-30	Mean and Below mean	Beginner
	31-45	Above Mean	Intermediate

In this section, respondents who scored between 15-30 (mean & below mean) were categorised at beginner level and those who scored between 31-45 i.e., above mean, were at intermediate level.

3.10.4 Scoring and categorization of student's overall cybersecurity awareness

To measure student's overall cybersecurity awareness, the scores of constructs of adapted theory of planned behaviour framework viz. knowledge, self-perception, attitude, including actual cybersecurity skills and behaviour towards cybersecurity was calculated. The categorization of the respondents was done based on their achieved scores.

Table 8: Categorization of scores in student's overall cybersecurity awareness

Variable	Range	Basis	Categories
Student's overall cybersecurity awareness	61-85	Mean and Below mean	Low awareness
	86-110	Above Mean	High awareness

Respondents with scores between 61 and 85, or mean and below the mean, were regarded to have low cybersecurity awareness, while those with scores between 86 and 110, or above the mean, were considered to have high cybersecurity awareness.

3.10.5 Scoring and categorization of student's cybersecurity knowledge

The respondents' cybersecurity knowledge was assessed using a knowledge test. The test's scoring process was as follows: One point was given for each correct response, and zero points for each erroneous response:

Table 9: The possible scores of the knowledge test

Type of statements	Minimum score	Maximum score
Multiple choice questions	0	20
Total	**0**	**20**

The maximum and minimum scores for the knowledge test are 20 and 0, respectively. The final score for each student was calculated. The responders were then categorised based on the results they had received.

Table 10: Categorization of scores in student's cybersecurity knowledge

Variable	Range	Basis	Categories
Cybersecurity Knowledge	0-10	Mean and Below Mean	Less Knowledgeable
	11-20	Above Mean	Knowledgeable

Those who had scores above the mean were regarded as knowledgeable, whereas those who received scores between 0 and 10, or in the mean or below the mean, were regarded as less knowledgeable.

3.10.6 Scoring and categorization of student's self-perception of cybersecurity skills

Selected university students' self-perceptions of cybersecurity were evaluated using a Likert scale. It was constructed using a 3-point scale. The following table shows the scores for both positive and negative statements:

Table 11: Scoring pattern according to the nature of statement regarding student's self-perception of cybersecurity skills

Statements	Great Extent	Some Extent	Less Extent
Positive statements	3	2	1
Negative statements	1	2	3

Table 12: Scoring of data for student's self-perception of cybersecurity skills

Total no. of items	Minimum score	Maximum score
14	14	42

There were 14 statements in total. The range between the lowest and highest possible scores is 14–42.

Table 13: Categorization of scores in student's self-perception of cybersecurity skills

Variable	Range	Basis	Categories
Self-perception of cybersecurity skills	14-28	Below mean	Unfavourable
	29-42	Mean and Above Mean	Favourable

Those who scored between 14 and 28 (below the mean) were classified as having unfavourable perceptions, while those who scored between 29 and 42 (mean and above mean) were classified as having favourable perceptions.

3.10.7 Scoring and categorization of student's actual cybersecurity skills and behavior

The questions have been prepared in order to measure the actual skills and behaviors of students in terms of cybersecurity. For each of the correct actions, 1 point is awarded and zero on the wrong doers and the scoring pattern for the test is as follows:

Table 14: The possible scores of student's actual cybersecurity skills and behavior

Type of statements	Minimum score	Maximum score
Multiple choice questions	0	24
Total	**0**	**24**

Hence, a student's actual cybersecurity skills and behaviour could receive a maximum total score of 24 or a minimum score of 0. Each respondent's overall score was calculated. The respondents were then assessed based on the scores they obtained.

Table 15: Categorization of scores in student's actual cybersecurity skills and behavior

Variable	Range	Basis	Categories
Actual cybersecurity skills and behaviour	0-11	Mean and Below mean	Unsafe
	12-24	Above Mean	Safe

Respondents with scores between 12 -24 (above mean) were classified as possessing safe cybersecurity skills and behaviour, whereas those with scores 0-11 (mean and below mean) considered into the unsafe category.

3.10.8Scoring and categorization of student's cybersecurity attitude

A three-point likert scale was developed to measure attitudes towards cybersecurity among selected university students at Vadodara. The following table shows the scores for both positive and negative statements:

Table 16: Scoring pattern according to the nature of statement regarding student's cybersecurity attitude

Statements	Great Extent	Some Extent	Less Extent
Positive statements	3	2	1
Negative statements	1	2	3

Table 17: Scoring of data for student's cybersecurity attitude

Total no. of items	Minimum score	Maximum score
14	14	42

There were fourteen statements in all. The range between the lowest and highest possible scores is 14–42.

Table 18: Categorization of scores in student's cybersecurity attitude

Variable	Range	Basis	Categories
Student's cybersecurity attitude	14-28	Below mean	Negative Attitude
	29-42	Mean and Above Mean	Positive Attitude

Those who scored between 29 - 42 (mean and above mean) fell into the category of respondents with a positive attitude, while those who scored between 14 - 28 fell into the category of respondents with a negative attitude (below the mean).

3.10.9 Correlation base

Correlation was calculated to analyse the relation within the four TPB constructs in the present study in relation to variables. The range for the correlation was as follows;

Table 19: Categorization of scores in correlation

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

Pearson correlation coefficient formula:

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

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

3.11 Plan for Statistical Analysis of the Data

Microsoft Office Excel was used to clean, tabulate, and enter the data. The Statistical Package for the Social Sciences (SPSS) software was used for the statistical analysis. The statistical measurement that was examined was as follows.

Table 20: Different statistical measure used for the analysis of the data

Sr. No.	Purpose	Statistical measures
1	Demographic profile of the students	Percentages
2.	Internet usage pattern of the students	Percentages
3.	Digital competency of the students	Percentages
4.	Overall cybersecurity awareness of the students	Percentages
5.	Variable wise overall cybersecurity awareness of the students	Percentages
6.	Differences in the overall cybersecurity awareness of the students with respect to variables	t-test and ANOVA

Sr. No.	Purpose	Statistical measures
7.	Overall knowledge, Self-perceptions, actual skills and behaviour, attitude (as per TPB framework) for Cybersecurity awareness of the students	Percentages
8.	Differences in the knowledge, self-perceptions, actual skills and behaviour and attitude (as per TPB framework) regarding cybersecurity awareness of the students	Mann-Whitney U, Kruskal Wallis Test, t-test and ANOVA
9	Differences in the co-relation within TPB constructs viz, knowledge, self-perception, actual cybersecurity skills and behaviour and attitude	Correlation
10	Readiness of students regarding cybersecurity awareness training program	Percentages

Statistical Measures and formula used for the analysis of the data

The formula used for the t-test

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{Sp^2}{n_1} + \frac{Sp^2}{n_2}}}$$

$$Sp^2 = \frac{(n_1 - 1)S_{12} + (n_2 - 1)S_{22}}{n_1 + n_2 - 2}$$

Where,
$\bar{x}_1$ = mean of group 1
$\bar{x}_2$ = mean of group 2
n_1 = number of groups 1
n_2 = number of groups 2
$df = n_1 + n_2 - 2$
S_1 = SD of group 1
S_2 = SD of group 2
Sp = pooled variance

The formula used for the ANOVA

$$F = \frac{\text{Large Variance}}{\text{Small Variance}} \quad \text{or} \quad F = \frac{\text{Between -group variance}}{\text{Within-group variance}}$$

Where, Between-group variance = Variance in the mean of each group for the total mean of all variance groups and, Within-group variance = Average variability of scores within groups.

The formula used for the Mann-Whitney U test

$$U_1 = R_1 - \frac{n_1(n_1+1)}{2} \quad \text{or} \quad U_2 = R_2 - \frac{n_2(n_2+1)}{2}$$

Where, *R* is the sum of ranks in the sample, *n* is the number of items in the sample.

The formula used for the Kruskal Wallis test

$$H = \left(\frac{12}{n(n+1)}\sum_{i=2}^{k}\frac{{R_i}^2}{n_i}\right) - 3(n+1)$$

Where, k = number of comparison groups,

n = total sample size,

n_i = sample size in the i^{th} group,

R_i = sum of the ranks in the i^{th} group.

CHAPTER 4
FINDINGS AND DISCUSSION

CHAPTER 4

FINDINGS AND DISCUSSION

4.1 Profile of the students

4.2 Internet Usage Pattern of the students

4.3 Digital Competency of the students

- 4.3.1 Overall digital competency of the students

4.4 Cybersecurity awareness among the students

- 4.4.1 Overall cybersecurity awareness among the students
- 4.4.2 Variable-wise cybersecurity among the students
- 4.4.3 Differences in the cybersecurity awareness in relation to selected variables

4.5 Cybersecurity awareness as per constructs of Theory of Planned Behaviour

- 4.5.1 Overall Cybersecurity awareness among the students in relation to each construct of TPB model viz. Knowledge, Self-perceptions of cybersecurity skills, actual skills and behaviour and attitudes
- 4.5.2 Differences in relation to each construct of TPB model viz. Knowledge, Self-perceptions of cybersecurity skills, actual skills and behaviour and attitudes in relation to selected variables

4.6 Readiness to undergo training on cybersecurity

Section A: 4.1 Demographic profile of the respondents

Table 21: 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		156	64.5
		Old		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

Variable-wise frequency and percentage distribution of the selected university students of the Vadodara (n=242)

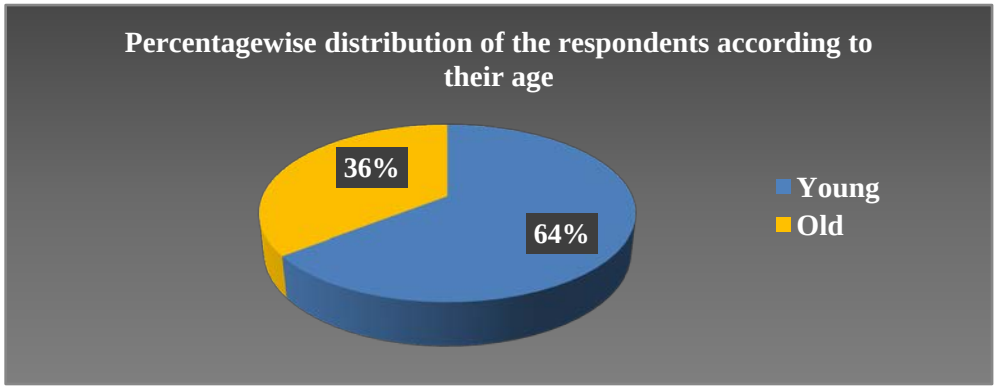


Figure 4 - Percentage distribution of the selected university students of the Vadodara according to their age

Table 21 & figure 4 reveals the percentage distribution of the selected university students of the Vadodara city according to their age. It represents that majority of the students i.e. 64.5 %, were in the category of young students (18-23 years) and only 35.5% were older students (24-29 years).

(n=242)

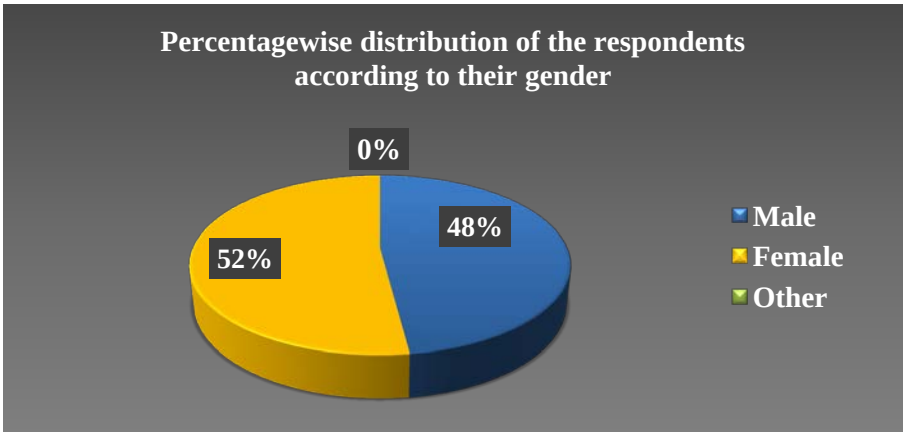


Figure 5 - Percentage distribution of the selected university students of the Vadodara city according to their gender

Table 21 & figure 5 also reveals that little more than half of the respondents, i.e., 52.1% were female, and the remaining 47.9% were male.

(n=242)

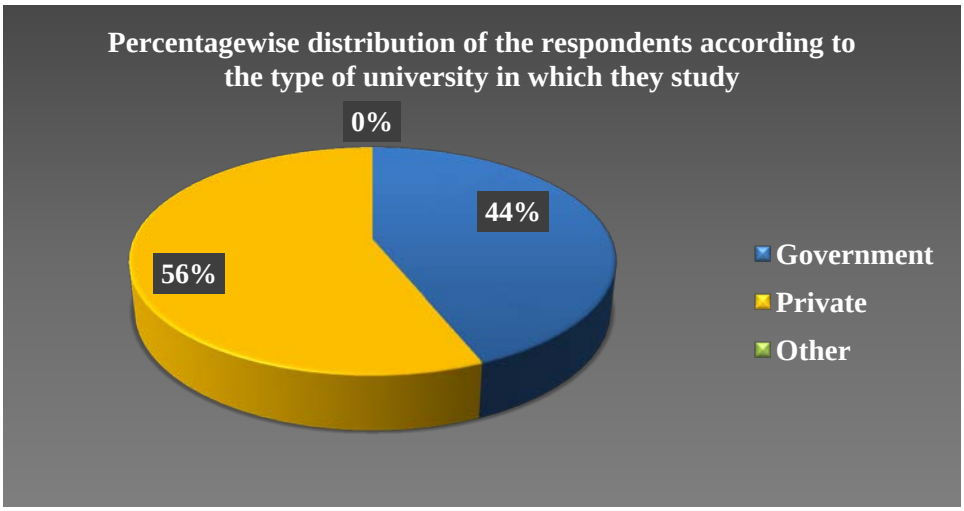


Figure 6 - Percentage distribution of the selected university students of the Vadodara city according to the type of university in which they study

Table 21 & figure 6 reveals that more than half of the respondents, i.e., 56.2% were from private university, and the remaining 43.8% were from government university.

(n=242)

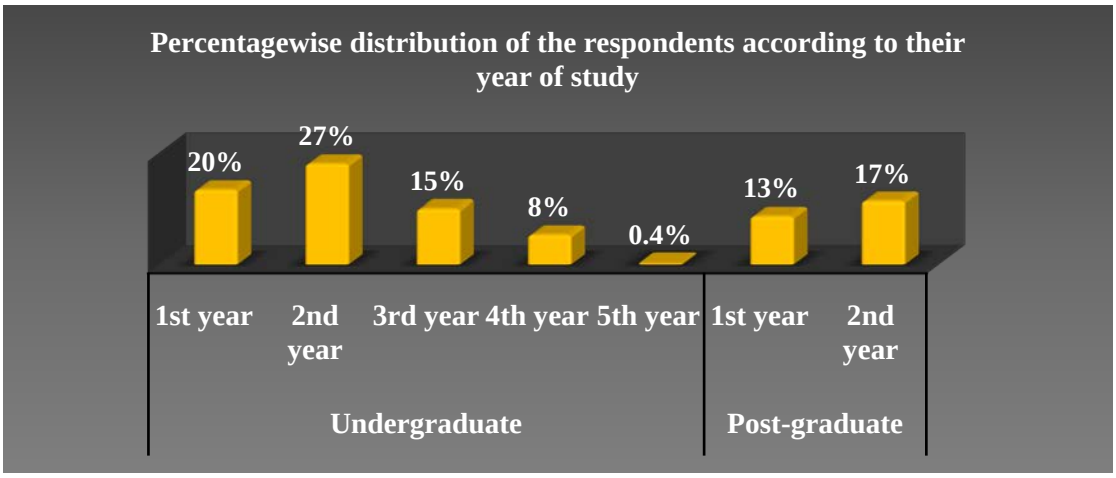


Figure 7 – Percentage distribution of the selected university students of the Vadodara city according to their year of study

Table 21 & figure 7 show that 70% of the respondents were undergraduate students in their first to fifth years of study (20%, 27%, 15%, 8%, and 0.4%, respectively). Remaining 30% of the respondents were postgraduate students in their first and second years of study (13% and 17%, respectively).

4.2 Section B

4.2.1 Part A– Internet usage pattern of the selected university students of the Vadodara

Table 22: – Internet usage pattern of the selected university students of the Vadodara city **(n=242)**

Sr. No.	Variables	Categories	Frequency (n)	Percentage (%)
5	Internet usage pattern	Moderate users	147	60.7
		Heavy users	95	39.3

(n=242)

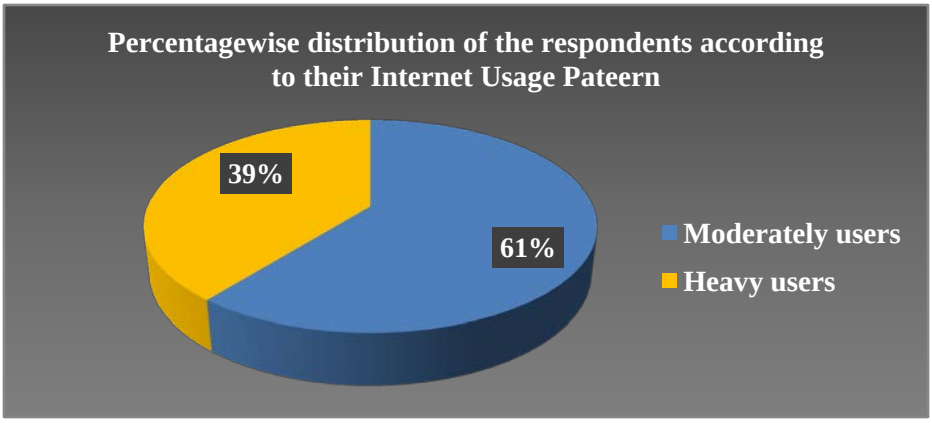


Figure 8 - Percentage distribution of the selected university students of the Vadodara city according to their internet usage pattern

Table 22 & figure 8 reveals that majority of the respondents, i.e., 60.7% were moderate internet users, and the remaining 39.3% were heavy internet users. Detailed usage pattern is described as follows.

Table 23: Frequency and percentage distribution of the selected university students of the Vadodara city according to different elements of internet usage pattern

(n=242)

Internet usage pattern	Frequency (n)	Percentage (%)
Years of using internet		
Less than or equal to 5 Years	85	35.1
>5 to 10 years	140	57.9
More than 10 years	17	07.0
Devices for connecting to the internet		
Smartphone	240	99.2
Laptop	137	56.6
Desktop	75	31.0
Other	3	01.2
Places where students use the internet daily		
At home	229	94.6
At college	207	85.5
At library	70	28.9
Other	197	81.3

Internet usage pattern	Frequency (n)	Percentage (%)
Internet Access		
Mobile Network	228	94.2
Private Wi-Fi	117	48.3
University Wi-Fi	100	41.3
Broadband (wired/ unwired at home)	91	37.6
Other	65	26.8
Hours spent on the internet		
4 hours or more	146	60.3
3-4 hours	46	19.0
2-3 hours	36	14.9
1-2 hours	10	04.1
1 hour or less	4	01.7
Reasons to use internet		
Entertainment	215	89.6
E-payment	188	78.3
Education	162	67.5
E-commerce	142	59.2
To communicate	93	38.8
Other	89	37.1
Stored, accessed or collected information as a part of daily tasks		
Aadhaar card number	148	71.2
My PRN/ college unique ID	113	54.3
Bank account information	84	40.4
PAN card	84	40.4
Voter ID	79	38.0
Driving License	68	32.7
Other	154	74.0
Usage of social networking sites		
WhatsApp	226	93.4
Instagram	203	83.9
YouTube	190	78.5
Snapchat	143	59.1
Other (Facebook, Linked-In)	80	33.0

Table 23 revealed that –

- About 60% of the selected university students had been using the internet for more than five to ten years.

- Almost hundred percent (99.2%) of college students use smartphone, followed by more than half of the respondents (56.6%) using a laptop, followed by 31% of them was using a desktop to connect for internet of things.
- Higher percentages of university students use internet at home, college and other than these places (i.e.94.6%, 85.5%, 81.3% respectively).
- Nearly half of the respondents (48.3%) use private Wi-Fi to access the internet, which is followed by a very large majority of the respondents (94.2%) who use mobile networks.
- The majority of students (60.3%) used the internet for more than four hours per day.
- High majority (89.6%, 78.3%) of the students reported using the internet for entertainment and for online payments respectively followed by, 67.5% for education, and 59.2% for e-commerce.
- A high majority (71.2%) of the students used to store, collect, access their Aadhaar card number followed by a little more than half (54.2%) for college ID/ PRN in their devices as a part of their daily tasks.
- A high majority of the respondents uses WhatsApp (93.4%), Instagram (83.9%) and YouTube(78.5%), followed by almost majority of them (59.1%) using Snapchat.

4.2.2 Part B– Digital competency of the selected university students of the Vadodara city regarding cybersecurity

Table 24: Digital competency of the selected university students of the Vadodara city (n=242)

Sr. No.	Variables	Categories	Frequency (n)	Percentage (%)
6	Digital competency	Beginner	171	70.7
		Intermediate	71	29.3

(n=242)

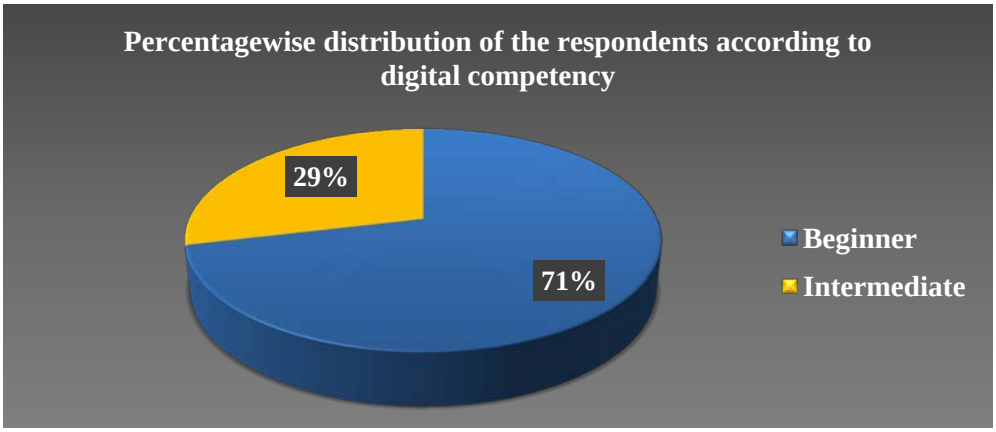


Figure 9 - Percentage distribution of the selected university students of the Vadodara city according to digital competency

Table 24 and figure 9 show that a large majority of respondents (70.7%) were found to have primary level, or beginner, digital competency skills, while 29.3% of them had intermediate level skills.

This indicates that, higher percent of the respondents in the current study were familiar with information and data literary, safety, and problem solving parameters of digital competency and remaining were better with communication and collaboration, and digital content creation areas of digital competency, on the basis of their self-report.

Table 25: Frequency and percentage distribution of the selected university students of the Vadodara city according to digital competency (n=242)

Sr. No.	Statements	Great Extent		Some Extent		Less Extent	
		n	%	n	%	n	%
	Information and Data literary						
1.	use a variety of search engines to access information	83	34.3	94	**38.8**	65	26.9
2.	use variety of filter process to evaluate the accuracy and liability of information	51	21.1	125	**51.7**	66	27.3
3.	download data from the internet in a variety of forms	68	28.1	110	**45.5**	64	26.4
	Communication and Collaboration						
4.	use a variety of online communication platforms,	71	29.3	90	**37.2**	81	33.5
5.	use collaboration tools to create/ manage materials	77	31.8	101	**41.7**	64	26.4

Sr. No.	Statements	Great Extent		Some Extent		Less Extent	
		n	%	n	%	n	%
	Communication and Collaboration						
6.	actively engage in online forums/ use a variety of online services	66	27.3	106	**43.8**	70	28.9
7.	use the internet to pass on information to others	60	24.8	108	**44.6**	74	30.6
	Digital Content creation						
8.	the creation of complex digital material in a range of media, including text, tables, photos, and audio files.	66	27.2	106	**43.8**	70	28.9
9.	use many tools for advanced formatting features using the internet.	64	26.4	108	**44.6**	70	28.9
	Safety						
10.	check whether security software installed on the device(s) which access the internet	43	17.8	121	**50.0**	78	32.2
11.	use the cloud's data storage services	67	27.7	102	**42.1**	73	30.2
12.	activate or configured/ change security settings in my digital devices	51	21.1	120	**49.6**	71	29.3
	Problem Solving						
13.	use licenses/ copyrights information when creating online content	50	20.7	99	**40.9**	93	38.4
14.	find or deal with solutions to the more common issues that come up using digital technologies	48	19.8	132	**54.5**	62	25.6
15.	find support from computer professional when a technical issue in digital device arise	36	14.9	121	**50.0**	85	35.1

Table 25 makes it clear that all respondents had some degree of digital competency when it came to handling internet-related items, indicating that university students had less of this proficiency and could only handle internet-related items at a novice level.

The statements, such as locating or resolving solutions to the more frequent problems that happen with digital technologies (54.5%), utilising a range of filter processes to evaluate the truth and liability of information (51.7%), checking to see if security software is installed on the device(s) that access the internet (50%), and seeking assistance from computer professionals when a technical issue with a digital device arises (50%), were comprehended to some extent by between half and more than half of the respondents.

4.2.3 Part C– Issues encountered during cyber surfing

Table 26: Frequency and percentage distribution of the selected university students of the Vadodara city according to cyber victimization (n=242)

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

Table 26 shows that while 17% of respondents had experienced an online crime, most of the respondents, or 83%, had not. This was originally planned as one of the variables, but during data analysis due to skewed responses, this particular variable was dropped as a variable and information was taken into account as additional background data.

Table 27: Frequency and percentage distribution of the selected university students of the Vadodara city according to issues encountered during cyber surfing (n=242)

Sr. No.	Variables	Categories	Frequency (n)	Percentage (%)
7	Issues encountered during cyber surfing	Phishing emails	14	35.0
		Identity fraud	2	5.0
		Malware	12	30.0
		Denial of Service	2	5.0
		Sensitive content	1	2.5
		Online blackmail	2	5.0
		Other	7	17.5

(n=40)

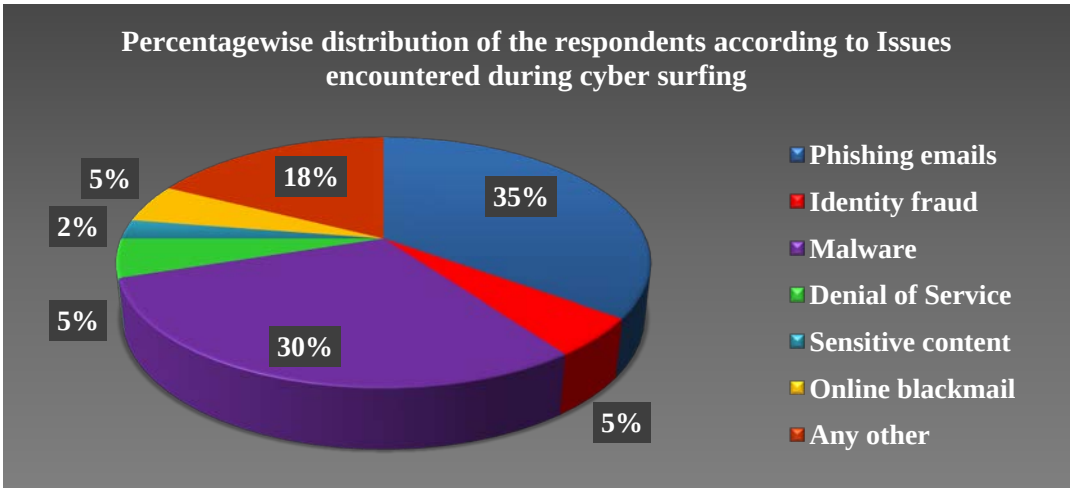


Figure 10 - Percentage distribution of the selected university students of the Vadodara city according to issues encountered during cyber surfing

Table 27 and figure 10 show that 16% of respondents said they have encountered problems while online. Of those, 35% and 30%, respectively, reported problems with malware and phishing emails. Only 5%, 2%, and 1% of respondents, respectively, said they had problems with identity fraud, online blackmail, denial of service, and sensitive content. The other 18% had experienced problems with social media account hacking.

4.4 Overall cybersecurity awareness of the selected university students of the Vadodara city

Table 28: Frequency and percentage distribution of the selected university students of the Vadodara city according to their overall cybersecurity awareness (n=242)

Sr. No.	Student's Cybersecurity Awareness	f	%
1	Low awareness	152	62.8
2	High awareness	90	37.2

(n=242)

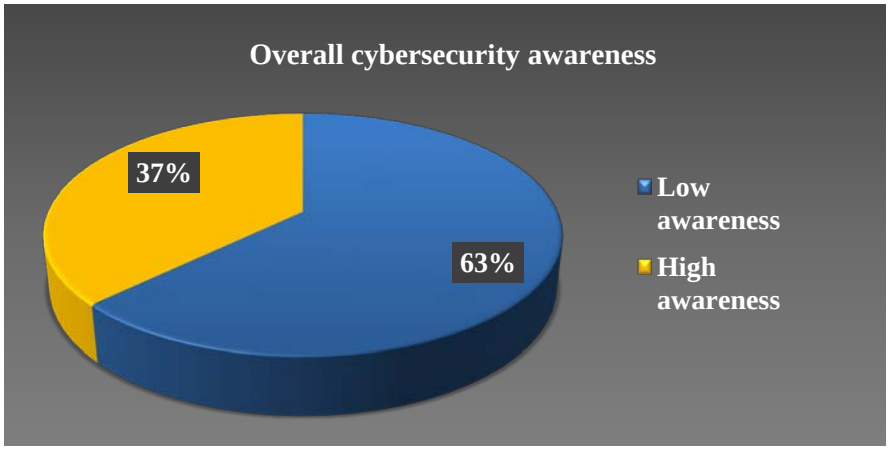


Figure 11 - Percentage distribution of the selected university students of the Vadodara city according to their overall cybersecurity awareness

Table 28 shows the frequency and percentage distribution of Vadodara city's selected university students' level of overall cybersecurity awareness (CSA). It shows that the majority of students (62.8%) have low cybersecurity awareness, followed by less than forty percent (37.2%) having a higher level of CSA. Hence, it can be inferred from the above finding that individuals in this study revealed overall low CSA in the context of their knowledge, self-perceptions towards cybersecurity skills, actual cyber security skills and behaviour and attitude. So, it can be interpreted that the respondents may lack in their knowledge, may be unable to perceive cyberspace activities beyond their thoughts, or might not be able to understand how their feelings, acts, and behaviors are affecting them as well as others and may have anxious even aggressive attitude while online.

This low level of CSA may result them to unable to pinpoint the precise issues that upset them the most when they become present online, which could eventually put them at a higher risk of cyberattack or becoming a victim of one. Today, when the internet is omnipresent and has become essential almost in every spheres of life, and when the majority of students use it frequently, poor cybersecurity awareness among them raises severe concerns.

This is a worrisome finding because students who stay online for maximum hours and use the internet for a variety of activities showed low awareness, suggesting that they would not be able to assess the gravity of online problems. Further, current study's

findings in the category of other than background information demonstrate that, nearly all respondents (99.2%) use smartphones; internet connectivity is readily available at home (94.2%) and away from home (84.2%); use online connectivity for more than four hours; and using the internet to access, store, and gather personal data (71.2%), cyber victim were 16.5% of the respondents and reporting by cyber victim to cyber cell/ police station were done by less than forty percent of the respondents(37.5%). It supports that, “risks which are higher for activities or technology that has the potential to harm more people. This is because, even while some activities very seldom have an effect on individuals, they can nonetheless have a significant impact on a huge number of people”. (Mumpower, Shi, Stoutenborough, & Vedlitz, 2013; Adams, 2012).

The possible reason could be this Gen Z have grown up with technology where self learnt cyberspace usage is observed in this age groups, which indicates cognitive vulnerability by having lack of formal cybersecurity training among them. According to Pew Research Center, Generation Z, which it defines, as everyone born after 1996, is the first generation to have grown up with digital technology. A new technology is constantly available to this young group. In spite of these advantages, the National Cybersecurity Alliance (NCSA) has discovered that generation Z is more likely than other generations to become a victim of a cyberattack. The aforementioned dissemination lead to state that ignorance is one of the causes of their online victimisation.

Another reason could be as stated by “The National Institute of Standards and Technology (NIST)” that “Gen Z spend more time online, which may makes them to become security fatigued. This can cause users to lower their guard and release information without thinking of the consequences. The National Cybersecurity Alliance (NCSA) also reported that, ‘40% of respondents lacked” motivation to implement security measures, despite the fact that 37% of respondents of all ages believed they could. Security weariness and uncertainty about what needs to be done most can both contribute to a lack of motivation. This is a big difference’. According to Moallem A. (2019), “despite their view that they are completely aware of their problems or can fix them on their own, university students do not appear to be particularly concerned about the security of their data,”

The arguments listed above indicate that, on one hand there is a security risk that cyberthreats represent to a nation and on the other how high internet penetration rates, which immediately generate a compelling demand for CSA. Given the prominence of susceptible Gen Z, this is especially true. Due to technological improvements, where more people are using more gadgets and producing more data, most of it sensitive or confidential, it is imperative to understand the growing relevance and necessity for cybersecurity understanding today. This will protect people from the increasing number of sophisticated cybercriminals and their attack methods. This is implied to be significant on both a national and global level by the above arguments. Paraphrase

The aforementioned information suggests that the government, at the policy level, must enforced the adoption and implementation of a robust curriculum on CSA from the central to all levels of the educational system, from elementary school students, or members of Generation Alpha, to college students, or members of Generation Z, especially in this digital age when online teaching-learning systems have now become an integral part of academic institutes following the epidemic, introduction of NEP20 as well as launching of 5G in India. This investment in CSA will assist in setting up a secure future for the country.

4.4.1 Variable wise overall cybersecurity awareness of the selected university students of the Vadodara city

Table 29: Frequency and percentage distribution of the respondents according to their overall cybersecurity awareness (n=242)

Sr. No.	Variables	Category		Overall cybersecurity awareness			
				Low		High	
				f	%	f	%
1.	Age	Young		97	62.2	59	37.8
		Old		55	**64.0**	31	36.0
2.	Gender	Male		84	62.8	32	37.2
		Female		68	**72.4**	58	27.6
3.	Type of university	Government		48	54.0	58	46.0
		Private		104	**62.8**	32	37.2
4.	Year of study	Undergraduate	1st Year	28	59.6	19	40.4
			2nd Year	40	60.6	26	39.4
			3rd Year	26	**74.3**	9	25.7
			4th Year	13	65.0	7	35.0
			5th Year	0	0.0	1	**100.0**
		Post-graduate	1st Year	21	**67.7**	10	32.3
			2nd Year	24	57.1	18	42.9
5.	Internet usage pattern	Moderate users		98	**66.7**	49	33.3
		Heavy users		54	56.8	41	43.2
6.	Digital competency	Beginner		118	**69.0**	53	31.0
		Intermediate		34	47.9	37	52.1

Table 29 reveals the percentage distribution of the selected university students of Vadodara city according to their cybersecurity awareness in relation to selected variables.

It can be seen from the above table that cyber security level varies across selected variables, viz, age, gender, type of university, year of study, internet usage pattern, and digital competency.

According to Table 29, the Vadodara city university students that were selected had lower cybersecurity awareness in more of the following categories:

- ✓ IIIrd year undergraduate students (74.3%)
- ✓ Females (72.4%),
- ✓ Beginners (69.0 %)
- ✓ Older students (64.0%)
- ✓ Moderate users (66.7 %)
- ✓ Students from private universities (62.8%)

Table 29 shows that a majority of respondents (62.2% and 64%) in the present of were younger (18-23) and older (24-29) students, respectively, and they had a low level of cyber security awareness (CSA). In contrast to the younger students, the older group of students had a marginally greater percentage, according to CSA data. This can be interpreted that, because the majority of the respondents, regardless of their age group, have low CSA, the consequences of their cyber-acts could be risky where they may be deliberately sabotaging their online presence for instances like enabling ransomware, or clicking on a type of virus that encrypts files and prevents the host from accessing data, or other attack on their systems. So, present study demonstrates that, younger and older group of the students had equal chances of susceptibility to become cyber victim.

Genderwise, majority (72.4%) of female students revealed a lower level of CSA compared to male students. Similar finding supported by Garba A. et.al.(2020) in their study, “where the majority of men have a fundamental understanding of cybersecurity, while very few women have cybersecurity understanding”.

According to the variable of type of university, the majority of students (62.8%) who were enrolled in private institutions demonstrated a lower awareness level compared to those who were from a government university. The reason could be, because private colleges may have greater financial resources than government universities, they may be able to afford better systems to protect against cyberattacks and threats. As a result, students at private universities may feel safer than students at government universities.

This may have contributed to their lower level of cybersecurity awareness. According to Security Scorecards 2018 study, stated that, “in education sector, particularly in higher education system, public universities/ colleges, struggle with finances. There security expenditures are frequently underfunded and sacrificed in favour of other objectives.” (https://www.onelogin.com/blog/3-reasons-higher-ed-hacked). Thus, students from government university were compelled to be proactive and vigilant as their university lacks robust infrastructure which can prevent them from any kind of cyber threats or attacks. So, for government university students it’s essential to comprehend several preventive strategy while they use to be online within campus too.

When compared to undergraduate (UG) and postgraduate(PG) students, statistics on CSA, by year of study showed that a significant majority (74.3%) of third-year undergraduate students had low cybersecurity awareness as compared to rest of the students. According to a study by Pramod and Raman (2014), “college students are aware of the security concerns provided by cell phones, but they do not fully understand the security solutions.”

As per the variable, internet usage pattern, current study data shows that majority of the moderate internet users (66.7%) had low CSA as compared to heavy internet users. The probable reason could be that students might not be aware of the potential consequences of their online acts, such as identity theft, financial fraud, or reputational harm. Hence, it is quite normal for moderate users to have low cybersecurity awareness as they are not more engaged in internet-related activities compared to heavy users.

Regarding the respondents' level of digital competency, the majority (69%) of the beginner group had a lower CSA than the respondents with an intermediate level of digital competency. The most likely reason is that, despite the numerous benefits the digital age has provided us, people in society have not been able to adapt this learning at the same rate as digital technology transforming. Hence, lag behind in different security measures. Students, especially those in higher educations, too may be left unprepared or unprotected in this area as a result of this mismatch; those with having basic digital skills could be more susceptible to cyber-risks.

Therefore, the aforementioned argument implies that in order to protect university students from cyberthreats, continuous measurement of this awareness is essential. This

is especially true with regard to the aforementioned study variables, particularly to the above defined categories of respondents. Students constitute the third entity of the higher education system, and since many of them were unfamiliar with online affairs and were using various platforms for the first time, it is the responsibility of higher education institutions to protect their students by providing them with up-to-date information about technological developments in Indian society. Continuous mapping of this CSA is essential for defending university students from cybercrime.

4.4.2 Differences in overall cybersecurity awareness of the selected university students of the Vadodara city in relation to the selected variables

Table 30:'t' test showing differences in overall cybersecurity awareness of the selected university students of the Vadodara city in relation to the selected variables

(n=242)

Sr. No.	Variables	Category	N	Mean	S.D.	T-Value	p-Value	Remarks
1.	Age	Young	156	82.0	11.6	0.59	0.557	Not Significant
		Old	86	81.1	11.4			
2.	Gender	Male	116	79.7	10.4	2.67	0.008	Significant
		Female	126	83.6	12.2			
3.	Type of university	Government	106	85.1	13.2	4.15	0.000	Significant
		Private	136	79.1	9.2			
4.	Digital competency	Beginner	171	79.6	11.0	4.63	0.000	Significant
		Intermediate	71	86.8	11.1			
5.	Internet Usage Pattern	Moderate users	147	80.0	10.7	2.96	0.003	Significant
		Heavy users	95	84.4	12.2			

*p value significant at < 0.05

Table 30 clearly indicates that there were significant differences found in the respondents' overall CSA, according to the variables viz, gender, type of university, digital competency, and internet usage patterns. It implies that there were considerable

differences between the mean scores of the respondents, regardless of whether they were male or female, attend a public or private university, have beginner or intermediate levels of digital skill, or use the internet moderately or heavily.

In light of this, the null hypotheses stating that, there will be no significant differences in the overall level of CSA among the selected university students from the city of Vadodara based on the variables of gender, type of university, digital competency, and internet usage pattern are rejected. So, it can be inferred from these results that student CSA varies depending on gender, type of university, digital competency, and internet usage pattern.

Regarding variable gender, the study's findings showed that females' mean scores were higher than those of their male counterparts, indicating that the study's female participants had a better level of CSA. It implies that compared to male counterparts, females were more cautious, aware of, and protective of online activities.

Regarding the variable type of university, the study's findings showed that students who attend private universities scored poor in terms of the students who attend public universities, indicating that the private university students who participated in the research had lower levels of cybersecurity awareness.

Regarding variable digital competency, the study's findings showed that digitally proficient beginner group's mean scores was lower than those of intermediate-level students, indicating a lower level of cybersecurity awareness among the beginner's digital proficient group in the study. A finding seems obvious as intermediate students had relatively better digital skills than beginner respondents. So, may be novice with their digital skills may not be competent to handle unexpected cyber breaches when occur, however, those with intermediate digital skills may recognize and actively handle so could be less possibilities of cyberthreats encounters while online.

Bogdanovskaya (2020) highlighted in her research that a lack of digital literacy is one of the things that lowers information security and may put people at danger.

Regarding varying internet usage patterns, the study's findings showed that moderate users' mean scores were lower than those of heavy internet users. It indicates a lower level of cybersecurity awareness among the respondents with moderate internet users.

The possible reason could be understood and justified as stated by Mishra's (2014) research, that most computer users believe security software to be an effective form of defence and mistaken firewalls and antivirus software for one and the same, Similar finding was also revealed by Mensch and Wilkie (2011)'s research that installing security solutions may provide consumers a false sense of security while really leaving them open to other risks including phishing and identity theft.
(https://www.researchgate.net/publication/322455127_Students'_Cybersecurity_Awareness_at_a_Private_Tertiary_Educational_Institution [accessed Mar 12 2023].)

So, moderate internet users of the present study may have such erroneous sense of cyber security, which makes them more vulnerable than their counterparts.

Thus, above findings implies that the components of students' cybersecurity awareness levels at higher education institutions are significantly influenced by variables such as gender, university type, digital competency, and internet usage habits in the current study. The previous table also makes it evident that there were no significant differences in the respondents' ages and overall cybersecurity awareness. So, it can be inferred that respondents' overall cybersecurity awareness level did not significantly differ based on their age. So, null hypothesis of the study, that there will be no significant differences in the overall cybersecurity awareness of the selected university students from Vadodara city with respect to their ages is accepted.

Younger generations might become overconfident in their ability to use the internet properly, which would lead to an increase in unsafe behavior. On the other hand, older generations can still lag behind in terms of cybersecurity understanding and procedures, which could make them more susceptible to online dangers. Therefore, in a way, regardless of ages, the students lack awareness, which is why no significant differences were found.

Therefore, even though younger people may be more aware of cybersecurity due to increased access to information and technology, it's still important to teach them about safe online practices, and the same is true for older groups of students. It’s a call to action for nation, where a population of 1.38 billion, India's National Cyber Coordination Centre (NCCC), a functioning government organization that focuses on raising cybersecurity awareness, may not be enough. In order to increase cyber security awareness throughout

all levels of the educational system, from elementary to higher education, greater participation is required from multi-stake holders such as the academic, industrial, political and government sectors.

Table 31: One way ANOVA test showing differences in overall cybersecurity awareness of the selected university students of the Vadodara city in relation to the selected variable of year of study (n=242)

Sr. No.	Year of study	Sum of Squares	df	Mean Square	F	Sig.	Remarks
1.	Between Groups	358	4	90	0.7	0.611	Not Significant
2.	Within Groups	31513	237	133			

Table 31 clearly indicates that there were no significant differences in the overall cybersecurity awareness of the respondents in relation to their year of study. So, it can be inferred that irrespective of categories of first year, second year, third year, fourth year and fifth year of undergraduate or first and second year of post-graduate students, their overall cybersecurity awareness were not significantly different.

Hence, the null hypothesis stating that there will be no significant differences in the overall cybersecurity awareness of the selected university students of the Vadodara city with respect to the variable year of study is accepted. The most likely reason could be that they all whether UG or PG students irrespective of their year of study, fall in the category of GenZ who have grown up with digital technology hence they all were at the same level of awareness, so, overall comprehending has not much differences and hence, no significant differences were foundfor this variable of the study.

A study conducted by Fatokun, F. B., et. Al. (2019), on the, cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities revealed similar finding and reported that, “there is a need for higher education institutions to educate students on the most recent and widespread cyberthreat breakouts in order to familiarise them since both undergraduate and graduate students are unfamiliar with some of the major cyberthreats.”

4.5 Theory of Planned Behaviour Framework Elements

4.5.1 Section C: Student's Cybersecurity Knowledge

4.5.1.1 Knowledge of the selected university students of the Vadodara city regarding Cybersecurity

Table 32: Frequency and percentage distribution of the selected university students of the Vadodara city according to their cybersecurity knowledge (n=242)

Sr. No.	Cybersecurity Knowledge	f	%
1	Less Knowledgeable	130	53.7
2	Knowledgeable	112	46.3

(n=242)

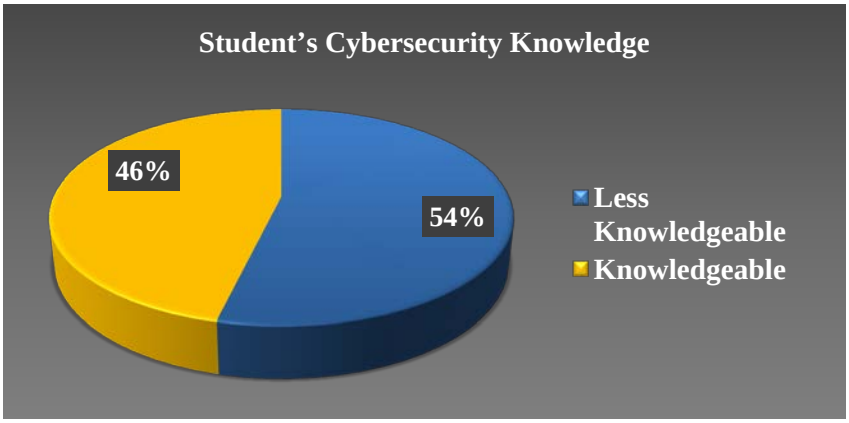


Figure 12 - Percentage distribution of the selected university students of the Vadodara city according to their cybersecurity knowledge

Table 32 and figure 12 shows the frequency and percentage distribution of the respondents, according to their level of cybersecurity knowledge. It demonstrates that little less than half (46.3%) of the students were having knowledge of CSA whereas and little more than half (53.7%) of the respondents were having less knowledge about CSA. So, it can be inferred that, though the higher education system has undergone a digital transition as a result of the Digital India initiative and the Internet, provided students with a variety of online venues, however, the reach of technology has been only considered throughout in terms of access and reach, not in terms of secured reach. It further also suggests a lack of attention or complacent attitude on the part of academic institutions

towards improving students' cyber-security measures. A contrast findings found in the Moallam A. (2019), study which reported that,“60% of respondents in a survey on cybersecurity awareness among university students were knowledgeable about cybersecurity, however, 40% of them, were unaware of cyber security.”

In the study of Garba, A., Sirat, M. B., Hajar, and Dauda, (2020), on “university students' knowledge of cyber security, Kruger, Drevin, and Steyn (2010) stated that, human behaviour and knowledge of information security were significantly correlated. This makes it quite evident that if people are aware of security, the frequency of attacks may be significantly reduced.”

The ability to spot contradictions in one's own knowledge or expertise demands a particular level of knowledge or skill, which individuals who sense this impact do not possess. Psychologists David Dunning and Justin Kruger claim that because most individuals try to "choose what they think is the most rational and ideal alternative," oblivious people frequently find themselves at a disadvantage because they are unaware of their limitations. According to the proverb (Charles Darwin), ignorance is preferable to knowledge and that lack of knowledge might be dangerous.

(https://www.britannica.com/science/Dunning-Kruger-effect)

Knowledge is referred to as the facts, information, and skills that a person has learnt via experience and education. With the right information, one may make the appropriate modifications to go forward and succeed. However, it's not just what someone knows that matters; it's also how they use it. There may not be a direct correlation between the degree of precise information and action, according to studies on the prevention of cyberattacks. Above findings implies that, knowledge must be taught to higher education students in order for them to make the best decisions. Students must be aware of the negative effects of cyber-related problems while lacking security awareness due to the grim realities and challenges brought on by cyberattacks as well as the rising frequency of hacking attacks on the data frameworks in the academic area. This suggests that university students should have access to a mandatory course on CSA with the latest CS knowledge are made.

Table 33: Frequency and percentage distribution of the respondents according to their knowledge level regarding cybersecurity

(n=242)

Sr. No.	Factors	Questions	Correct %	Incorrect %
1.	Password Security	Which of the following passwords are more secure? (can select > 1 option)	35.3	**64.7**
2.		Which of the following is a proper precaution for social networking account security? (can select > 1 option)	41.4	**58.6**
3.	Network Security	Which of the following does not contribute to email security being maintained?	**63.2**	36.8
4.		Which of the following act is not done by Trojans?	50.0	50.0
5.		____ is sending spam or unsolicited emails to any target victim's inbox.	50.0	50.0
6.	Website Security	In ____ phishing, the construction of a fake webpage is done for targeting definite keywords & waiting for the searcher to land on the fake webpage.	**60.3**	39.7
7.		When you visit a website, ____ are small files that are downloaded to your computer.	**62.4**	37.6
8.		Identify secure URL	33.3	**66.7**
9.	System Security	The built-in security app called the ____ by Microsoft is intended to filter network data from your Windows system and prohibit hazardous communications or the apps that are starting them.	43.0	**57.0**
10.		Turn on ____ just when you need to use it; otherwise, turn it off for security reasons.	**60.7**	39.3
11.		Which of the following actions won't spread the virus?	50.0	50.0
12.	System Security	There are three standard measures used to safeguard information accessibility:	**61.6**	38.4
13.	Social Networking Site Security	A number of social media platforms and services offer ____ to properly verify accounts.	**53.7**	46.3
14.	Operational Security	What is software piracy?	**52.5**	47.5
15.		_____ is an online fraud run by cybercriminals, in which the user is digitally persuaded to provide sensitive information.	47.5	**52.5**

(n=242)

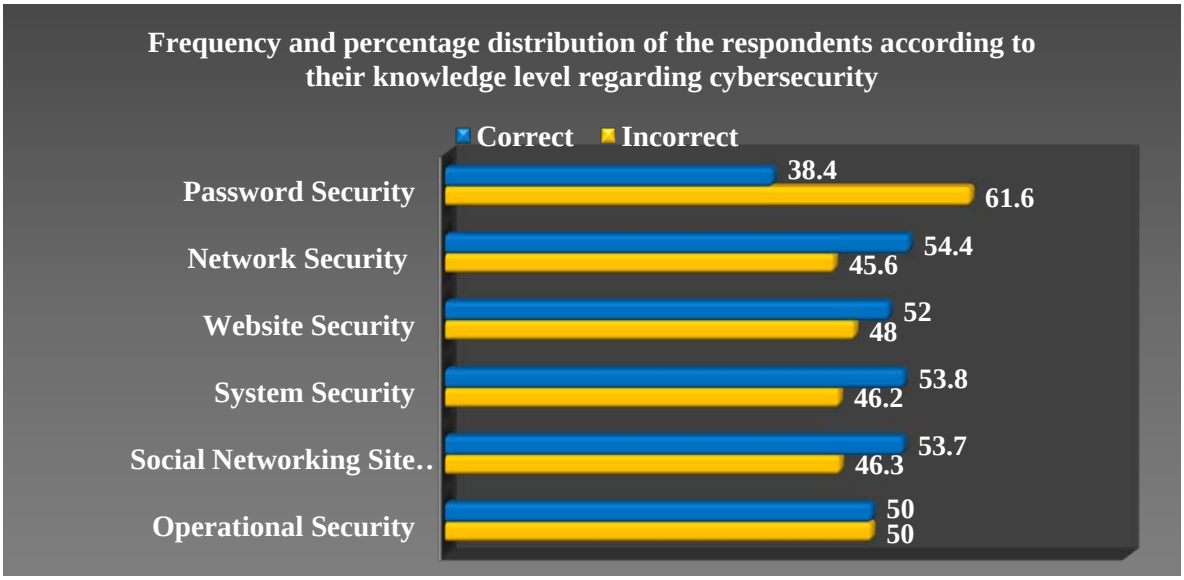


Figure 13 - Frequency and percentage distribution of the respondents according to their knowledge level regarding cybersecurity

Table 33 reveals the frequency and percentage distribution of the respondents according to their knowledge level regarding cybersecurity as mentioned below.

- Fewer than half of the respondents (46.2% and 46.3%) had incorrect knowledge about social networking site security, whereas more than half of the respondents (53.9% and 53.7%) had the right knowledge about system security.
- The majority of respondents, or 61.6%, had inaccurate knowledge about password security management, while only 38.4% had correct password knowledge.
- Regarding network security, a little more than half (54.4%) of the respondents had accurate information, while a little less than half (45.6%) of them had an inaccurate understanding.
- Nearly half (52%) of the respondents knew about website security, but 48% of them knew the wrong thing.
- Regarding operational security, equal percent i.e. half of the respondents had accurate and incorrect knowledge. Since actual knowledge isn't always true belief, it's important to make a distinction between the two. The information in the table above demonstrated how certain knowledge is influenced by both prior knowledge and environmental influences.

(https://link.springer.com/chapter/10.1007/978-3-319-44588-5_6)

- Less technical questions, such as identifying secure URLs (33.3%) and secure passwords (35.3%), had the least accurate answers, but preserving email security (63.2%) and downloading files from websites to computers (62.4%) scored better with reference to CSA. The findings showed that even while people use digital gadgets frequently, they are not always aware of the risks involved.
- The results of the above table indicate that students' knowledge of issues like "more secure passwords," "precaution for social networking account security," "secure URLs," and "online fraud operated by cybercriminals where the user is digitally persuaded to provide sensitive information" was deficient. Given that these are the fields where people with technical skills required, and thus this presents a worrying image. However, there are directly under human control.
- According to the research done by Van B. et al. (2019), human error accounts for close to one-fourth of all cybersecurity failures (Waldrop, 2016). The current study findings with above lack of basic knowledge support this.
- So, it can be concluded that, the aforementioned circumstance endangers not only the users personally but also the entire academic organisations. However, in light of the rise in internet usage and significance of digital technologies in the classroom, it shouldn't be allowed for resistance to stop the beginner individual from embracing technology in this digital age. Instead, one needs to be better prepared and equipped in order to solve problems successfully. Higher education students must acquired hands-on cybersecurity training in order to promote personal accountability and successfully counteract cyberthreats.

4.5.1.2 Differences in the knowledge of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variables

Table 34: Mann-Whitney U test showing differences in knowledge of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variables (n=242)

Sr. No.	Variables	Category	N	Mean rank	Mann-Whitney U	p-Value	Remarks
1.	Age	Young	156	118.7	6269.0	0.398	Not Significant
		Old	86	126.6			
2.	Gender	Male	116	124.0	7020.5	0.596	Not Significant
		Female	126	119.2			
3.	Type of university	Government	106	124.3	6908.0	0.577	Not Significant
		Private	136	119.3			
4.	Digital competency	Beginner	171	115.0	4961.5	0.025	Significant
		Intermediate	71	137.1			
5.	Internet Usage Pattern	Moderate users	147	115.6	6112.5	0.101	Not Significant
		Heavy users	95	130.7			

*p value significant at < 0.05

According to the above table 34, there were significant differences between the respondents' knowledge of cybersecurity and the variable referred to as digital competency. It shows significant difference between the mean rank of the respondents who were at the beginner than the intermediate level of digital competency. The mean rank of beginner respondents exhibited a lower level of cybersecurity knowledge than that of their counterparts.

Hence, the null hypothesis stating that there will be no significant differences in the overall cybersecurity knowledge of the selected university students of the Vadodara city with respect to the variable viz. digital competency was rejected.

The probable reason could be that persons with limited digital proficiency may not be aware of the vulnerabilities offered by the internet and may not be able to recognise cyberattacks that were designed to disrupt online transactions or operational processes, or to obtain unauthorized access to an operating system, destroy sensitive data. As a result, beginners were more at risk than their peers who were relatively better digital competencies may be able to comprehend IoT on how to protect oneself from such cyber threats.

This finding suggests that in order to create an effective cyber security literacy program or awareness interventions that assist students in coping with various levels of cyber activities, it is necessary to assess knowledge gaps that should be filled.

The above table 34 clearly indicates that there were no significant differences in the cybersecurity knowledge of the respondents in relation to their age, gender, type of university and internet usage pattern. So, it can be inferred that irrespective of categories of young or old, male or female, government or private university and moderate users or heavy users their knowledge regarding cybersecurity were not significantly different.

Hence, the null hypotheses stating that there will be no significant differences in the overall cybersecurity knowledge of the selected university students of the Vadodara city with respect to the variable viz. age, gender, type of university and internet usage pattern were accepted.

The probable reason could be that, students who fall in Gen Z as per their age could be more impulsive and inquisitive in nature in general irrespective of younger and older age-group category hence; get affected equally on cyberthreats which makes them vulnerable as far as CSA knowledge was concerned. Hence, there was no significant difference found with CSA knowledge of the respondents according to their age.

Daengsi, T & et. al (2022) stated that, age is a significant variable that explains differences in human behaviour in digital culture and online material consumption, according to Bordonaba-Juste et al. (2020). The distinctions between previous generations can be attributed to the shared values, beliefs, and attitudes that people who share comparable experiences and who lived during the same time period will exhibit.

(Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with

Phishing Attacks. Educ Inf Technol 27, 4729–4752 (2022). https://doi.org/10.1007/s10639-021-10806-7)

Regarding type of university, the reason could be the due to the cohort which comes in the university were rarely undergo with deep dive on the cybersecurity concept formally which deficit them on CSA knowledge irrespective of government or private university students, hence there were no significant differences in stated categories of CSA was seen for this variable.

Despite the fact that the majority of individuals seek increased internet security and privacy, they rarely employ the available tools and approaches to achieve their goals. So, referring to internet usage pattern variable, showing no significant differences found for overall CSA.

Above all having a presence on new media platforms is currently associated with a status symbol, which is one of the driving forces for students using them. Unfortunately, the majority of students are unaware of effective strategies for combating online fraudsters and their activities. A majority of them either ignore such information or at most delete it. According to the National Sample Survey Organization's survey, more than 88% of adults over the age of 14 lack the skills necessary to send emails properly. So, it can be concluded that ethical attackers and defenders still have asymmetric information.

Table 35: Kruskal Wallis test showing differences in knowledge of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variable of year of study. (n=242)

Variable	N	Mean	Std. Deviation	p-value	Remarks
Year of study	242	9.51	3.562	0.743	Not significant

*p value significant at < 0.05

Table 35 above makes it evident that there were no significant differences in the respondents' knowledge regarding cybersecurity in relation to their year of study. Therefore, it can be inferred that respondents' cybersecurity knowledge did not differ considerably depending on whether they were in the first, second, third, fourth, or fifth year of their UG or PG studies in the university. Hence, the null hypothesis, stating there

will be no significant differences in the cybersecurity knowledge of the selected university students from Vadodara city with respect to the variable year of study, was therefore accepted.

This finding of the present study is at contrasts with the results from a study by “Hong et al. (2023), which found that there were notable knowledge gaps across undergraduates in different academic years, postgraduate students, and working graduates.”

However, a study conducted by Gavett et al., (2017), also corroborates this finding and mentioned that both young and old adults were suspicious about phishing attacks in approximately equal numbers.

Above scenario suggests that a lack of information makes students less confident in their ability to deal with suspicious cyber act and also lead them to poor choice of decision, or in-appropriate action. So, in order to reduce these possibilities or university students could become the target of such cyber assaults, it is essential to disseminate cybersecurity knowledge through specially designed programmes for university students as a whole, whether in the public or private setups. Cyber security education must be more widely available in order for more people to not only be aware of but also to be informed about the presence of cyber threats and attacks. There is a strong need of knowledge empowerment of these students to make them enable to recognise potential threats.

According to Luker (2003), educating the students can change their beliefs about cybersecurity. In addition to raising student awareness of the issue on campus, making cybersecurity a required course for all students could eventually result in a decline in cyberattacks against college students.

This implies that universities can foster a cybersecurity culture by launching special cyber cell and promoting cybersecurity best practices and encouraging students to take cybersecurity seriously, which involve promoting the use of password managers, multi-factor authentication, and other security solutions, as well as emphasizing the significance of refraining from harmful online cyber acts. Universities can also collaborate with cybersecurity firms and groups to offer students networking opportunities and industry insights, to offer, students a platform to learn more about cybersecurity as careers avenues.

4.5.2 Section D: Student's Self-Perception of Cybersecurity Skills

4.5.2.1 Self-Perception of the selected university students of the Vadodara city regarding cybersecurity skills

Table 36: Frequency and Percentage Distribution of the selected university students of the Vadodara city according to their self-perception regarding cybersecurity skills (n=242)

Sr. No.	Student's Self-Perception of Cybersecurity Skills	f	%
1	Unfavorable	163	67.4
2	Favourable	79	32.6

(n=242)

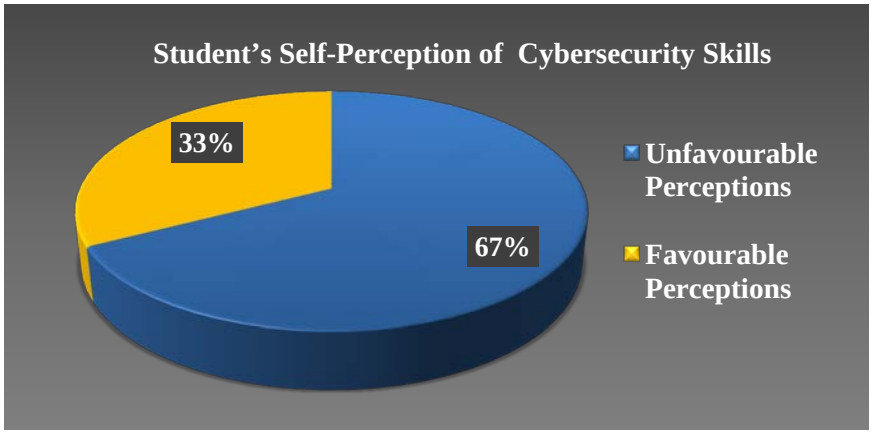


Figure 14 - Percentage distribution of the selected university students of the Vadodara city according to their self-perception regarding cybersecurity skills

Table 36& figure 14 reveals the frequency and percentage distribution of the respondents according to their self-perception regarding cybersecurity skills. It shows that majority of the respondents i.e. 67.4% had unfavorable perceptions, whereas one third of the respondents i.e., 32.6% had favorable perceptions. It is a matter of concern to see that majority of students had unfavorable perceptions which can be interpreted as more vulnerable and susceptible to cyber threats.

Understanding perception, it does not have a necessarily concrete and reliable basis as it is derived from one's own thoughts and ideas rather than learning and experience. Perception may lead to knowledge but not necessarily, it can even lead into the

opposite.(https://english.stackexchange.com/questions/432668/whats-the-difference-between-knowledge-of-sth-and-perception-of-sth)

Accordingly, the most likely explanation for why university students have negative perceptions of CSA is that when students perceive something, they may judge the risk based on their reasoning, using analytical and rational processes, and on how they may feel, as emotions are involved in the perception, management, and acceptance of risk. In addition, moods may change the background against which people's perceptions and ideas about danger change. A student who is feeling good, for example, will be less conscious of the threats surrounding them and will perceive those risks as being less likely to materialise. Instead, s/he will concentrate on the advantages of riskier actions. The results of detailed percentagewise analysis in the present study showed that, nearly Half (49.2%) of the respondents had less favorable perceptions of the statements that passwords on all digital devices should be changed frequently to lessen vulnerability to cyber threats and that it is risky to accept requests or messages from strangers on social networking sites. So it can be inferred that students in this study perceive cyberthreats very lightly. This suggests that respondents' unfavorable perceptions towards cyber security skills enhance vulnerability fuel, which may cause them to become a victim of cybercrime.

Similar results were reported by “Benson V. et al. (2019), who also noted that the key to understanding students' reactions to malicious cyber-attacks lies in the fact that students do not seem to see such attacks as a threat to themselves. Students are more likely to react to the occurrence (such as a service interruption) than the cyberattack itself.”

This implies that, perceived cyber threats need to be enforced amongst the students. For that they need to accept that cyber threat is existing and can affect to anyone.

Table 37: Frequency and percentage distribution of the selected university students of the Vadodara city according to their self-perceptions of cybersecurity skills

(n=242)

Sr. No.	Cyber-security dimensions	Statements	Great Extent		Some Extent		Less Extent	
			n	%	n	%	n	%
1.	Password Security	Passwords on all digital devices should be changed on a frequent basis to reduce vulnerability to cyber threats.	22	9.1	100	41.3	119	**49.2**
2.		Using old passwords is safe while changing passwords.	17	7	112	46.3	113	**46.7**
3.	Network Security	A phishing mail is simple to identify.	28	11.6	129	**53.5**	84	34.9
4.		Users' privacy can be protected through a Virtual Private Network (VPN).	29	12	128	**52.9**	85	35.1
5.		It's safe to conduct online transactions using public Wi-Fi.	35	14.5	104	**43**	103	42.6
6.	Website Security	It's safe to clear your browser history while using a computer at a cybercafé, college, or another location.	50	20.7	108	**44.6**	84	34.7
7.	Website Security	While looking on various educational websites, it is imperative that you read the cookie access authorization policies carefully.	28	11.6	116	**47.9**	98	40.5
8.	System Security	It's safe to share digital devices with close friends.	42	17.4	135	**55.8**	65	26.9
9.		You can continue watching movies, web series, or listen to music using authorized programmes after getting a warning message.	59	24.4	115	**47.5**	68	28.1
10.	Social Networking Site Security	Publicly posting a live location on social media is not detrimental.	67	27.7	134	**55.4**	41	16.9
11.		One becomes easily popular by sharing private images on social media.	66	27.3	118	**48.8**	58	24
12.		It is dangerous to accept requests/ messages from strangers on social networking sites.	35	14.5	101	41.7	106	**43.8**

Sr. No.	Cyber-security dimensions	Statements	Great Extent		Some Extent		Less Extent	
			n	%	n	%	n	%
13.	Social Networking Site Security	On social media threats/ suspicious activities are informal and do not need to be reported to the cyber cell.	69	28.5	104	**43**	69	28.5
14.	Operational Security	USB plugging at a college computer lab raises the possibility of drives getting viruses.	21	8.7	121	**50**	100	41.3

From the above table, it is evident that, all the cyber security acts were perceived by the respondents either to some or less extent. So, it can be inferred that, cyber acts have been conducted recklessly by the university students without thinking about its repercussions.

The present study results showed that there were not many disparities in how the selected universities' students perceived their security and resilience. The assertions were understood to some extent by forty or fifty percent of the respondents, for statements i.e. A phishing mail is simple to identify (53.5%), Users' privacy can be protected through a Virtual Private Network (VPN) (52.9%), It's safe to share digital devices with close friends(55.8%), Publicly posting a live location on social media is not detrimental (55.4%), and USB plugging at a university computer lab raises the possibility of drives getting viruses (50%), whereas 40% and more than that of the respondents had a less favourable perceptions for the statements i.e. Passwords on all digital devices should be changed on a frequent basis to reduce vulnerability to cyber threats (49.2%), Using old passwords is safe while changing passwords (46.7%), It's safe to conduct online transactions using public Wi-Fi (43%), It's safe to clear your browser history while using a computer at a cybercafé, college, or another location (44.6%), While looking on various educational websites, it is imperative that you read the cookie access authorization policies carefully (47.9%), You can continue watching movies, web series, or listen to music using authorized programmes after getting a warning message (47.5%), One becomes easily popular by sharing private images on social media (48.8%), It is dangerous to accept requests/ messages from strangers on social networking sites (43.8%), and on social media threats/ suspicious activities are informal and do not need to be reported to the cyber cell (43%).

Such negative impressions of cybersecurity could be the result of internet users' ignorance, arrogance, or lack of knowledge. Divergent viewpoints among the respondents may be attributed to substandard learning conditions, a lack of security resources for everyone, or wrong perceptions or insufficient cyber skills that ultimately causes them to become susceptible. The findings indicated that there is a pressing need to increase respondents' technical competence, understanding of the virtual world, and capacity to learn from digital platforms with reference to cybersecurity awareness, with current perspectives.

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

Table 38:'t' test showing differences in self-perception of the selected university students of the Vadodara city regarding cybersecurity skills in relation to the selected variables

(n=242)

Sr. No.	Variables	Category	N	Mean	S.D.	T-Value	p-Value	Remarks
1.	Age	Young	156	30.6	3.9	0.26	0.979	Not Significant
		Old	86	30.6	3.8			
2.	Gender	Male	116	29.7	3.3	3.55	0.00	Significant
		Female	126	31.4	4.2			
3.	Type of university	Government	106	31.6	4.4	3.89	0.000	Significant
		Private	136	29.8	3.2			
4.	Digital competency	Beginner	171	30.4	3.9	1.43	0.155	Not Significant
		Intermediate	71	31.1	3.7			
5.	Internet Use Pattern	Moderate users	147	29.9	3.8	3.71	0.000	Significant
		Heavy users	95	31.7	3.7			

*p value significant at < 0.05

Table 38 indicates that there were significant differences in the self-perception regarding cybersecurity skills of the respondents in relation to the variables viz, gender, type of university and internet usage pattern. It shows that the mean scores of the respondents who were male or female, study in government or private university, whether they were moderate internet users or heavy users differ significantly.

Therefore, the null hypotheses stating that, there will be no significant differences in the self-perception of cybersecuity skills of the selected university students of the Vadodara city with respect to the variables gender, type of university and internet usage pattern were rejected.

The study's findings regarding gender variation showed that female's mean scores were higher than male, indicating that females in the study had more favorable perceptions of CSA as compared to their counterparts. It indicates that, compared to male, female had more favourable perceptions of cybersecurity.

The most likely explanation is that women value their privacy more than men did in the virtual and real worlds, respectively. According to survey conducted by HMA (Hide My Ass) in US, result showed that, when using the internet, women (62%) are more inclined than men (49%) to make use of personalised privacy settings.

(https://www.forbes.com/sites/kevinmurnane/2016/04/11/how-men-and-women-differ-in-their-approach-to-online-privacy-and-security/?sh=4ffcf2547d88)

Thus, female may perceive the cybersecurity primary setting may be offer security zone, hence having low perceptions.

"In the study on Gender difference and employees' cybersecurity behaviours by Anwar, et.al. (2017) Ifinedo (2014) discovered that men seemed to have less motivation to follow security policy than women, and he advises practitioners to consider how gender affects security policy compliance in the workplace. Most earlier studies, including "Hearth and Rao (2009)," "Ifinedo (2014)," "Hoy and Milne 2010," "Laric et al. 2009," and "Sheehan 1999," have shown that women are typically more concerned about privacy (perceived vulnerability) than men and, as a result, more likely to follow security policies."

With reference to variable internet usage pattern, the study findings revealed that, the mean score of heavy users who have high level of internet usage shows higher mean score than moderate users showing their favorable perception among the university students in the present study.

The probable reason could be that cybersecurity is complex, elusive and ever evolving field. So, moderate internet users may not be really to forming risk perception towards cyber security skills, which may lead them to as have unfavourable perception.

Another reason could be the moderate internet users may have impression that, cybercrime may not really the crime for which s/he as an individual needs to bother, as such things may be taken care either by host university or government. “Cybercrime isn’t something that I need to be concerned about” The large perception gap between how the public views cybercrime and the threat it actually poses is a major impediment to the adoption of new online mindsets and behaviours.
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/684609/BT_CYBER_AWARE_V11_280218.pdf)

Regarding the variable, type of university, the study's findings showed that students in government universities had higher mean scores than students in private universities, indicating that they were having favorable perception towards cyber security skills than their counterparts of private university students.

The probable reason could be that, in private university due to layers of security zones, the respondent may perceive themselves that protecting ownself from cyber crime is optional, hence could be carefree which may lead them to the unfavourable perception toward cybersecurity skills.

The above table 38 clearly indicates that there were no significant differences in the self-perception of cybersecurity skills of the respondents in relation to their age and digital competency. So, it can be inferred that irrespective of categories of young or old and beginner or intermediate their self-perceptions regarding cybersecurity skills were not significantly different. Hence, the null hypotheses stating that, there will be no significant differences in the self-perception regarding cybersecurity skills of the selected university students of the Vadodara city with respect to the variable viz. age and digital competency were accepted.

In the study on ‘The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates’ conducted by Hong, W. C. H. et.al. (2023) stated that, according to Hwang et al., (2017) " the more highly educated and knowledgeable internet users (such as university students) who enter society, the more likely it is that their Internet Security Awareness (ISA) will be influenced by less educated co-workers. This is because peers have a significant influence on behaviour.

So, in nutshell, it indicates that, the perception among moderate internet users is troublesome, and it's unclear what exactly it is generating. So may be detailed investigation can be done. However, it appears that other societal influences are what are shaping students' perception toward CS skills.

Table 39: One way ANOVA test showing differences in self-perception of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variables of years of study (n=242)

Sr. No.	Year of study	Sum of Squares	df	Mean Square	F	Sig.	Remarks
1.	Between Groups	55	4	14	0.9	0.451	Not Significant
2.	Within Groups	3540	237	15			

The above table 39 clearly indicates that there were no significant differences in the self-perception of the respondents regarding cybersecurity skills in relation to the year of study.

It shows that the mean scores of the respondents who were at first year, second year, third year, fourth year or fifth year, whether in UG or PG studies did not differ significantly.

Thus, the variable year of study did not make any difference in the self-perceptions of the respondents regarding cybersecurity skills. Therefore, null hypothesis stating that there will be no significant differences in the self-perception of the selected university student of Vadodara city of the Gujarat state regarding their responses to self-perception of cybersecurity skills with respect to the variable year of study was accepted.

The implication is that such perceived discrepancies do result in actual cyber security disparities. "The self-perception illustration above suggests that risk perceptions are crucial in cyber models because they can anticipate the use of precautions (Huang, Rau, Salvendy, Gao & Zhou, 2011; Boss, Galletta, Lowry, Moody & Polak, 2015)."

Thus, it is recommended to run a systematic awareness campaign in regional and national languages with the goal of increasing respondents' awareness based on their knowledge

deficits as well as the danger zone which influence their wrong perceptions. This can be done using various mass and digital media, especially for GenZ as well as for the society.

4.5.3 Section E: Student's Actual Cybersecurity skills and behavior

4.5.3.1 Actual skills and behavior of the selected university students of the Vadodara city regarding cybersecurity

Table 40: Frequency and percentage distribution of the selected university students of the Vadodara city according to actual cybersecurity skills and behavior

(n=242)

Sr. No.	Student's Actual Cybersecurity skills and behavior	f	%
1	Unsafe	141	58.3
2	Safe	101	41.7

(n=242)

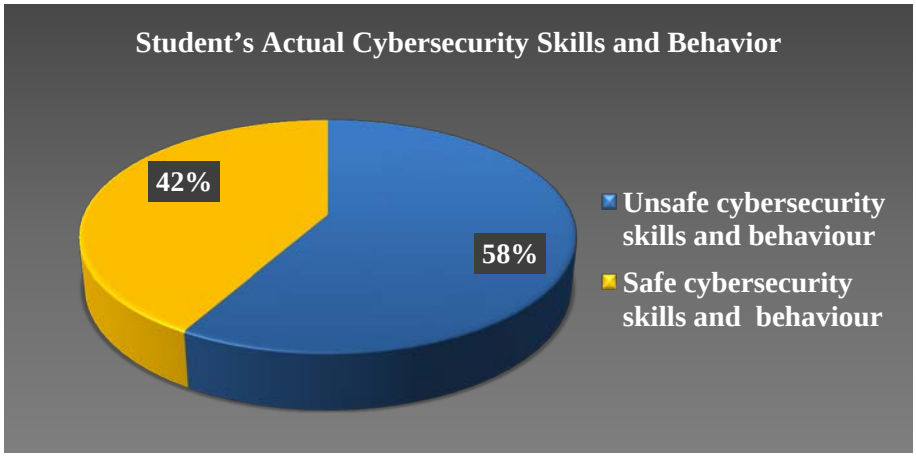


Figure 15 - Percentage distribution of the selected university students of the Vadodara city according to their actual cybersecurity skills and behavior

Above table 40 and figure 15 reveals the frequency and percentage distribution of the respondents according to their actual cybersecurity skills and behavior. It shows that almost majority of the respondents i.e. 58.3% follow unsafe cybersecurity skills and behavior in reality followed by little more than one third i.e., 41.7% of them actually following safe cybersecurity skills and behavior.

So, it can be inferred that students in the current study may get engage in wrong CS skills & behavior and they were not very careful, thus, did not bother to take precautions while using internet at public places or personal devices.

“According to Aliyu et al. (2010), university students in Malaysia seemed major violators of computer ethics and security as they were usually careless when posting content and surfing and frequently engaged in illegal usage by means of sharing and downloading of counterfeit software, TV shows, and movies.”

Chandarman, R., &Van Niekerk, B. (2017) studied students' cybersecurity awareness at a private tertiary educational institution, which examined this issue. “It was found that the students were generally not engaging in safe computing for a number of reasons, including laziness and financial constraints.”

The Symantec (2010) survey, which showed that nearly nine out of ten adults are considering cybercrime and over a quarter actually anticipate being scammed or defrauded online. Bada, M., and Nurse, J. R. in their research on "The social and psychological impact of cyberattacks was stated that, just 50% of the study's adult participants believe they would change their online conduct if they were a victim, despite the ubiquitous threat and prevalence of cybercrime. It was also stated in this study that, a user's motivation to employ security mechanisms depends on their perceptions of their susceptibility to external security risks, their potential severity, and the cost and effectiveness of preventative or mitigation measures.”So, students with unsafe skills and behaviour may feel that, cybercrime is not real crime and will occur only to celebrities or big business tycoons only and not to the students.

One of the most common criticisms of cybersecurity education programmes is that they place too much focus on theory and book learning, which inhibits students from developing the necessary practical skills. This is highlighted in the cybersecurity workforce gap (2019) article. The tasks graduates will encounter once they start working cannot be prepared for by theory alone. Students must receive practical instruction and hands-on experience in order to equip themselves with the concrete skills employers want. (https://www.csis.org/analysis/cybersecurity-workforce-gap)

So, this implies that it is important for universities and academicians to address these issues and help students understand the importance of cybersecurity, as well as provide

them with the knowledge and tools to practice good cybersecurity hygiene. Academics must think about how they help present and future college students deal with the personal hazards associated with utilizing internet of things.

Table 41: Frequency and percentage distribution of the respondents according to their actual cybersecurity skills and behaviour (n=242)

Sr. No.	Factors	Questions	Correct	Partially correct	Incorrect
			%	%	%
1.	Password Security	Strong passwords can be challenging to recall. What can you do to ensure that you remember them? (can select > 1 option)	**79.9**	**20.1**	0
2.	Network Security	You were in dire need of an internet and suddenly find public Wi-Fi available without a password so, you'll;	**53.7**	0	46.3
3.	Website Security	To stay safe online I ensure following actions before/during browsing; (can select > 1 option)	23.3	**14.9**	**61.8**
4.	System Security	From the following given security tools and applications for computer/ laptops/ mobile etc which are you using in your digital devices? (can select > 1 option)	28.5	**8.3**	**63.2**
5.		The mouse pointer on your computer screen starts to move and click on things by itself. How will you proceed?	27.3	0	**72.7**
6.		I update my anti-virus software and other applications in my devices; (can select > 1 option)	16.1	0	**83.9**
7.		What should you do if a message stating that a group of viruses has to be eliminated has shown on your computer?	34.7	0	**65.3**

8.	Operational Security	You receive a call in which a person is asking you about buying electric vehicle as company is celebrating 75th year of independence offering huge discount and your ordered it and paid the required amount. After that you didn't receive any call or message regarding your order. What do you do in this situation?	36.0	0	**64.0**
9.		Which of these are good methods to prevent yourself from identity theft? (can select > 1 option)	**71.7**	**24.3**	4
10.	Operational Security	You are visiting a cybercafé to take print out of your project work documents, from your e-mail. While the print-out is processing, you are accessing your social media profile and checks other e-mails. As soon as the printouts are ready, you rush to collect it. You close the browser window without logging out of the account and leave the cybercafé. After two hours you receive a notification that the password of your social media account has been reset. Now you are trying hard but unable to access your social media account. What can be the reason that you are unable to access your social media account?	**67.8**	0	32.2

(n=242)

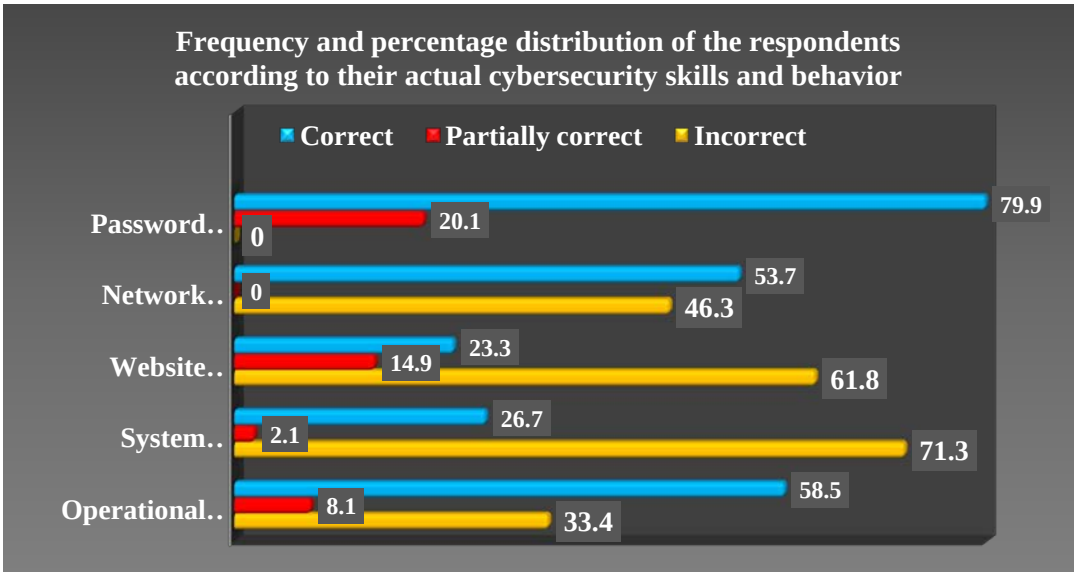


Figure 16 - Frequency and percentage distribution of the respondents according to their actual cybersecurity skills and behavior

Above table 41and figure 16 reveals the frequency and percentage distribution of the respondents according to their actual cybersecurity skills and behavior on its different dimensions.

According to the aforementioned cyber security dimensions, the dimension relating to password security had the highest percentage of accurate actual cyber skills and behaviour among respondents (79.9%), followed by the dimensions relating to operational security (58.5%), and network security (53.7%).

The use of the internet and digital technology in education poses a risk to users. It is important for individuals to prioritize cybersecurity education and adopt best practices to protect themselves and their sensitive data.

- It reveals that the majority of the respondents, i.e., 79.9%, had correct actual skills and behavior regarding password security, while only 20.1% of the respondents had partially correct actual skills and behavior for the same, for a question like, “Strong passwords can be challenging to recall. What can you do to ensure that you remember them?"
- Regarding network security little more than half of the respondents had correct actual skills and behavior, whereas little less than half of them had incorrect

actual skills and behavior, for the question like, “You were in dire need of an internet and suddenly find public Wi-Fi available without a password so, you’ll;”

- Majority of the respondents (61%) had incorrect actual skills and behavior regarding website security and 23% of the respondents had correct actual skills and behavior, whereas 14.9% had partially correct actual skills and behavior for the question like, “To stay safe online I ensure following actions before/during browsing;”
- On the other hand, majority of the respondents i.e. 71.3% of the respondents had incorrect actual skills and behavior, whereas 26.7% &very few i.e. 2.1% of the respondents had correct and partially correct actual skills and behavior regarding system security, respectively, for the questions like, “From the following given security tools and applications for computer/ laptops/ mobile etc which are you using in your digital devices?”, “The mouse pointer on your computer screen starts to move and click on things by itself. How will you proceed?”, “I update my anti-virus software and other applications in my devices” and “What should you do if a message stating that a group of viruses has to be eliminated has shown on your computer?.”
- It also reveals that more than half of the respondents had correct actual skills and behavior regarding operational security while one third of them were having incorrect actual skills and behavior, whereas, 8.1% of the respondents had partially correct actual skills and behavior.

So, above arguments recommends that, today, the digital age, as represented by ideas like network society, cyber area, and cyberspace, has made life easier than it has ever been before for humans. However, it also brings new responsibilities and its challenges. In this regard, digital information and culture that trying to replace information and culture on traditional necessities requires redefining and becoming functional on the basis of security which enables the communities to live with themselves and each other.

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

Table 42: Mann-Whitney U test showing differences in actual skills and behavior of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variables (n=242)

Sr. No.	Variables	Category	N	Mean rank	Mann-Whitney U	p-Value	Remarks
1.	Age	Young	156	128.6	5603.5	0.033	Significant
		Old	86	108.7			
2.	Gender	Male	116	116.1	6686.5	0.251	Not Significant
		Female	126	126.4			
3.	Type of university	Government	106	132.2	6073.0	0.035	Significant
		Private	136	113.2			
4.	Digital competency	Beginner	171	102.4	2798.0	0.000	Significant
		Intermediate	71	167.6			
5.	Internet Usage Pattern	Moderate users	147	117.7	6419.0	0.287	Not Significant
		Heavy users	95	127.4			

*p value significant at < 0.05

The above table 42 indicates that there were significant differences in the actual cybersecurity skills and behavior of the respondents in relation to the variables viz, age, type of university and digital competency. It means that the respondents who were young or old, study in government or private university, whether they were at beginner or intermediate level of proficiency of internet related tasks differ significantly regarding CSA in accordance with their actual skills and behaviour.

Therefore, the null hypotheses stating that there will be no significant differences in the actual cybersecurity skills and behavior of the selected university students of the Vadodara city with respect to the variables age, type of university and digital competency were rejected.

The study's findings regarding age variation showed that young students mean rank was higher than those of older students, indicating that older students in the study follow

unsafe cybersecurity skills and behavior. So, it can be interpreted that, older students of the study were at higher cyber risk as compared to younger students.

The most likely explanation is that, some schools in Gujarat state already offer cybersecurity chapters under the computer or ICT courses. So, it can be assumed that the younger students may have exhibited stronger real-world cybersecurity skills and behaviour than their older peers as a result.

Another possible reason for having unsafe cybersecurity skills and behavior is that when Gen millennial has born, technology has spread its wings; however, Gen Z is still in the acceptance and livingly mode. Older students may be less willing or struggling or to adopt new cybersecurity practices or to keep pace with technologies, which can leave them vulnerable to newer threats.

However, it’s a contradictory finding with a study by Debb, S. M., et.al. (2020)“Generation Y individuals sample engage in safer information security practises than their Generation Z counterparts. Looking to their greater exposure to digital technology, it is reasonable to assume that the older group's self-reported safer behaviours are accompanied by more in-depth knowledge of information security.”

The study's findings regarding type of university variation showed that government university students mean rank was higher than private university students, indicating that private university students in the study used to follow unsafe cybersecurity skills and behavior. It indicates that, compared to government university students, private university students were more at high risk.

This may be due to the fact that a university's institutional culture can also affect students' actual cybersecurity knowledge and behaviour. Universities that place a high priority on cybersecurity may encourage a culture of less cautious online practises because students felt at ease without having to worry about cyber threats. As a result, those carefree habits may continue even outside the university's boundaries, making students the most vulnerable even using IoTs. While universities that do not prioritize cybersecurity may create an environment where students are less likely to take cybersecurity seriously.

The possible reason could be that, student's conduct and cybersecurity skills influenced by personal characteristics motivation, experience, and beliefs.

The study's findings regarding digital competency variation showed that intermediate level students mean rank was higher than beginner, indicating that students whose level of digital competency was basic in the study had unsafe cybersecurity skills and behavior. It indicates that, compared to intermediate; the beginner level digital competency students had unsafe cybersecurity skills and behavior.

This is obvious as students with high level of digital competency may be more aware of cybersecurity risks than those with lower digital competency, they may still lack awareness of all the potential cyber threats. For example, they may not be aware of the latest phishing scams or malware attacks. Another reason could be students' cybersecurity skills and behavior may be influenced by their social networks. They may be more likely to take risks or ignore security best practices if their peers are doing the same. Addressing these factors through education, awareness campaigns, and peer influence can help promote safe cybersecurity utilize behavior among university students.

The above table 42 clearly indicates that there were no significant differences in the actual cybersecurity skills and behavior of the respondents in relation to their gender and internet usage pattern. So, it can be inferred that irrespective of categories of male or female and moderate or heavy users their actual cybersecurity skills and behavior were not significantly different.

Hence, the null hypothesis stating that there will be no significant differences in the actual cybersecurity skills and behavior of the selected university students of the Vadodara city with respect to the variable viz. gender and internet usage pattern were accepted.

Hargittai, E., & Shafer, S. (2006) also stated similar findings in their study and reported that men and women do not differ greatly in their online abilities.

The first generation that was truly digital was Generation Z, which began to be born in 1997.Microsoft claims that because they were raised in a world without privacy, these digital natives feel powerless to regulate their own lives. (https://www.vonage.com/resources/articles/generational-gap-cybersecurity-privacy/)

Above scenario concludes that, a fundamental component of cybersecurity is the human dimension. Human mistake in the context of security refers to unintentional actions—or inaction—by users and individuals that result in, spread, or enable a security breach. So,

in the present study, where sample belong to in the age group of 18-25 years, shows that, this Gen Z may not be much bother about privacy which ultimately may lead them towards higher cyber risks. Although there are virtually endless possibilities for human error, university can consider mainly skill-based errors and decision-based errors, to be reduced by organising periodically security awareness training programmes on regular basis for the students.

Table 43: Kruskal Wallis test showing differences in actual skills and behavior of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variables (n=242)

Variable	N	Mean	Std. Deviation	p-value	Remarks
Year of study	242	11.03	3.442	0.279	Not significant

*p value significant at < 0.05

The above table 43 clearly indicates that there were no significant differences in the actual cybersecurity skills and behavior of the respondents regarding cybersecurity skills in relation to the variable year of study.

It means that the mean scores of the respondents who were study from first year to fifth year from undergraduate level or first to second year of postgraduate level did not differ significantly. Slusky, L., & Partow-Navid, P. (2012) in their study on students' information security practices and awareness reported that the main issue with security awareness is not a dearth of security knowledge, but rather how the students utilize such knowledge in practical settings. It also stated that, the compliance with information security awareness is lower than the understanding of it. As a result, this can be applied to students of any year of study, and as a result, there is no discernible difference between the indicated categories of year of study regarding CSA for this variable. Thus, the variable year of study did not make any difference in the actual cybersecurity skills and behvaior of the respondents. Therefore, null hypotheses stating that there will be no significant differences in the actual cybersecurity skills and behvaior of the selected university student of Vadodara city of the Gujarat state with respect to the variable year of study were accepted.

This recommends that, educational institutions have a responsibility to protect their students of this cyber threats, as many of them would have been studying away from home for the first time. However, at the same time students also equally needs to be accountable for their own cyber security course of action, just like anybody else that uses the internet. They must need to think before they act particularly when they are using IoT.

4.5.4 Section F: Student's Cybersecurity Attitude

4.5.4.1 Attitude of the selected university students of the Vadodara city regarding cybersecurity

Table 44: Frequency and percentage distribution of the selected university students of the Vadodara city according to their attitude regarding cybersecurity (n=242)

Sr. No.	Student's Cybersecurity Attitude	f	%
1	Negative	165	68.2
2	Positive	77	31.8

(n=242)

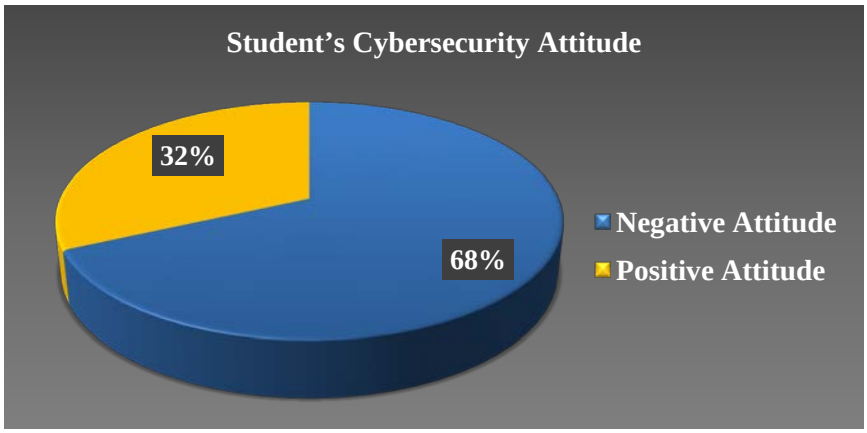


Figure 17 - Percentage distribution of the selected university students of the Vadodara city according to their attitude regarding cybersecurity

Table 44 & figure 17 reveals the frequency and percentage distribution of the respondents according to their attitude regarding cybersecurity. It shows that majority of the respondents i.e. 68.2% had negative attitude, whereas little less than one third one the respondents i.e., 31.8% had positive attitude. So, it can be inferred that, negative attitudes

of the respondents towards cybersecurity, means higher levels of cyber risks, they were carrying.

User attitudes towards behaviour can include positive or negative personal evaluation of performing (or not performing) a behaviour.

(https://proceedings.informingscience.org/InSITE2017/InSITE17p065-076Pham3440.pdf).

Pham, H., Brennan, and Richardson (2017) stated in their study that, attitude towards a behaviour may be the strongest predictor of behavioural intent." According to TPB theory, attitude is the level of perception that an individual has the action of interest as favorable /positive or unfavorable/ negative attitude is indicated by all this. It requires taking into account how the behavior will affect the results.

So, from the above findings it can be assumed that even though majority of the respondents may believe that they were already well-versed about cybersecurity acts and were not needed to be cautious while surfing internet, in a way they were having unrealistically high opinion of one's own judgment, ability, towards cybersecurity.

The fact that the majority of the students in the current study had insufficient cyber security awareness could be the cause of their potentially negative attitudes towards CSA. As a result, individuals may be feeling helpless to protect themselves from cybercrime or they may be underestimating the risk, resulting in them by having negative attitudes about the CSA.

So, it implies that, the respondent needs to have an internet user's digital identity has a physical presence and leaves a trail of evidence of data and information that they share with various internet services throughout when they use IoTs. Therefore, study recommends need internet users develop a cybersecurity culture from an early age. Users may prevent the possibility of cyberattacks and the loss of personal information, which could result in material, psychological, and financial damages, by incorporating a set of cyber hygiene practices into their everyday routines.

Table 45: Frequency and percentage distribution of the selected university students of the Vadodara city according to their attitude of cybersecurity

(n=242)

Sr. No.	Factors	Statements	Great Extent		Some Extent		Less Extent	
			n	%	n	%	n	%
1.	Network Security	use Wi-Fi password to prevent unauthorized people from using my home network.	123	**50.8**	100	41.3	19	7.9
2.		never get an email with a dangerous attachment from my university student email address.	57	23.6	127	**52.5**	58	24.0
3.	Website Security	register for seminar/ conferences only on those educational websites that clearly state their privacy rules.	109	45.0	117	**48.3**	16	6.6
4.		worried about unintentionally coming across porn on the website utilised.	79	32.6	99	**40.9**	64	26.4
5.	System Security	disable security options in my digital device to work faster.	64	26.4	105	**43.4**	73	30.2
6.		prefer to secure files and emails using encryption software.	99	40.9	116	**47.9**	27	11.2
7.		set the computer screen to lock automatically, when don't use it frequently or for a long time.	100	41.3	105	**43.4**	37	15.3
8.	SNS Security	create an account by using different ID if I want to know about a person whom I don't know	49	20.2	120	**49.6**	73	30.2
9.		give my correct details of name, age, gender, location while playing online games with strangers.	56	23.1	99	**40.9**	87	36.0

Sr. No.	Factors	Statements	Great Extent		Some Extent		Less Extent	
			n	%	n	%	n	%
10.	SNS Security	use obscene language on social networking sites	51	21.1	120	**49.6**	71	29.3
11.		keep my social networking site account or profile private.	118	**48.8**	99	40.9	25	10.3
12.	Operational Security	keep my cybersecurity knowledge updated to guard against threats or attacks online.	96	39.7	118	**48.8**	28	11.6
13.		rarely backup my files from my department's PC.	41	16.9	143	**59.1**	57	23.6
14.		put all electronic files in a folder with my name on it, and place it on the desktop in the department computer lab so I can easily get to it the following day for work.	51	21.1	123	**50.8**	68	28.1

It is clear from the above table that the half of the respondents had a more positive attitude towards cyber acts, such as using a Wi-Fi password to prevent strangers from accessing their home network and keeping their social networking account or profile private, as they were more aware of them. The respondents' responses were found mixed, with a higher percentage indicating that they were somewhat aware of it.

However, to avoid engaging in cybercrime, one should never open an email from a student email account from a university (52.5%), only register for seminars and conferences on websites that explicitly outline their privacy policies (49.3%), and so on. fearful of accidently discovering porn on the used website (40.9%); To make my digital gadget run more quickly (43.4%), disabled the security features; prefer to use encryption software to secure my files and emails (47.9%) ; also enabled my computer's screen to automatically lock when I'm not using it for a while (43.4%), use vulgarity on social media; maintain my cybersecurity knowledge current to protect myself from threats or assaults online (49.6%); infrequently backup my files from the department PC (59.1%); put all electronic files in a folder with my name on it (50.8%), and placed it on the desktop in the department computer lab so can easily access it the next day for work.

Therefore, it can be concluded that these may be the areas where students of the present study need to be given the proper viewpoint orientation.

This recommends students need to be of being aware of cybersecurity in everyday situations. Further one need to talk about cybersecurity awareness and to have proactive mindset as wellbeing conscious of the dangers posed by online activities including emailing, web browsing, and social networking.

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

Table 46:'t' test showing differences in attitude of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variables

(n=242)

Sr. No.	Variables	Category	N	Mean	S.D.	T-Value	p-Value	Remarks
1.	Age	Young	156	30.7	4.7	0.71	0.479	Not Significant
		Old	86	30.3	4.2			
2.	Gender	Male	116	29.6	4.1	3.19	0.002	Significant
		Female	126	31.5	4.7			
3.	Type of university	Government	106	32.2	5.0	5.25	0.000	Significant
		Private	136	29.3	3.6			
4.	Digital competency	Beginner	171	29.9	4.1	3.77	0.000	Significant
		Intermediate	71	32.2	4.9			
5.	Internet Usage Pattern	Moderate users	147	30.1	4.3	1.94	0.054	Not Significant
		Heavy users	95	31.3	4.7			

*p value significant at < 0.05

The above table 46 indicates that there were significant differences in the attitude regarding cybersecurity of the respondents in relation to the variables viz, gender, type of university and digital competency. It shows that the mean scores of the respondents who were male or female, study in government or private university and the level of digital proficiency as beginner or intermediate differ significantly.

Therefore, the null hypotheses stating that there will be no significant differences in the overall cybersecuity attitude of the selected university students of the Vadodara city with respect to the variables gender, type of university and digital competency were rejected.

Regarding variable gender, the study's findings showed that females' mean scores were higher than those of their male counterparts, indicating that the study's female participants had favorable attitude towards cybersecurity than their counterparts. This indicates that compared to men, women had a more positive attitude regarding cybersecurity.

Cain et al. (2018) tested different levels of "cyber hygiene" and found that self-identified professionals had less secure behaviour than self-identified non-experts.”This can also be used to explain why male students have a negative attitude towards technology. As more male students use technology, this may cause them to see cyberthreats as less serious than they actually are. A study on students' attitudes towards information technology and the digital divide done by Aswathi, P., and Mohamed Haneefa, K. (2019), revealed the opposite results.

“However, There are gender variations in computer and Internet use, with men expressing higher levels of self-efficacy, more positive attitudes, and lower levels of anxiety than women”(Chou, 2001; Losh, 2004; and Broos, 2005.)”

Regarding variable type of university, the study's findings showed that mean scores of government university was higher than private university, indicating that the students from government university had positive attitude towards cybersecurity. This indicates that compared to private university, government university students had a positive attitude regarding cybersecurity.

Government universities may be well-known, well-established, and more focused on technology-related fields or research, which may explain why staff members at these institutions place more emphasis on cybersecurity while engaging with students. As a result, students might view cybersecurity more favorably and be more open to learning about the dangers of internet security. Further, the attitude of university students towards cybersecurity will depend on a range of factors, including individual beliefs and experiences, as well as the cybersecurity-related initiatives and resources available to them at their university.

“Demirdag (2016) asserts that a lack of IT expertise can also lead to a lack of confidence in one's ability to utilise it, which can have a negative impact on one's attitude towards it. This information was provided in the study article Attitude towards Information Technology and Digital Divide: A Study among Students at Universities in Kerala, India by Aswathi, P., and Mohamed Haneefa, K. (2019). Therefore, compared to students at public colleges, students at private universities were less knowledgeable about cyber security.”

Regarding variable digital competency, the study's findings showed that intermediate level students mean scores were higher than beginner, indicating that the study's intermediate level of digital competent students had positive attitude towards cybersecurity. This indicates that compared to intermediate, beginner level of digital competent students had a negative attitude regarding cybersecurity.

Students with lower levels of digital competency may not have a better understanding of cybersecurity best practices, such as using strong passwords, avoiding public Wi-Fi, and regular updation of software. This lack of awareness and knowledge may lead to a more negative attitude towards cybersecurity and a greater possibility of becoming a victim online.

“According to Aswathi, P., and Mohamed Haneefa, K.'s (2019) in their research article from 2019 titled Attitude towards Information Technology and Digital Divide: A Study among Students in Universities in Kerala, India, respond that students who are less at ease with and more anxious about using IT will find it less enjoyable to use it.”This may create negative attitude to those were digitally less proficient in comparison to intermediate category of the digitally proficient students.

The above table 46 clearly indicates that there were no significant differences in the attitude regarding cybersecurity of the respondents in relation to their age and internet usage pattern. So, it can be inferred that irrespective of categories of young or old and moderate or heavy users their attitude regarding cybersecurity was not significantly different.

Hence, the null hypothesis stating that there will no significant differences in attitude regarding cybersecurity of the selected university students of the Vadodara city with respect to the variables viz. age and internet usage pattern were accepted.

If a well-educated internet user is surrounded by less-educated users, who have lower security awareness (Bostan & Akman, 2015), the well-educated person may gradually lessen safe practices. These studies imply that social influences from the workplace, family, and friends can influence people's attitudes and behaviors about cybersecurity.

So, it is recommended that, students of these universities must think that there is a significant threat that is likely to occur and that the threat can be much reduced by having better human control. They all need to be convinced that they can engage in the safe cyber practice by acquiring positive attitude and adequate knowledge and that doing so would only need minimal effort.

Table 47: One way ANOVA test showing differences in attitude of the selected university students of the Vadodara city regarding cybersecurity in relation to the selected variable of year of study. (n=242)

Sr. No.	Year of study	Sum of Squares	df	Mean Square	F	Sig.	Remarks
1.	Between Groups	48	4	12	0.6	0.669	Not Significant
2.	Within Groups	4844	237	20			

Table 46 above makes it abundantly evident that there were no significant differences in the respondents' overall attitude regarding cybersecurity in relation to their year of study. Therefore, it can be inferred that respondents' cybersecurity attitude did not differ considerably depending on whether they were in the first, second, third, fourth, or fifth year of their UG or PG studies in university. The null hypothesis, which states that there will not be significantly different in the overall cybersecurity attitude of the selected university students from Vadodara city with respect to the variable year of study, was therefore accepted. The probable reason could be that, students of UG or PG irrespective of their year of study might be feeling powerless or helpless against cyber threat and hence, when everyone accept this situation, there was no significant difference in the respondents' overall attitude regarding cybersecurity in relation to their year of study

The most likely explanation is because, as previously indicated, people may accept a situation even if it is unpleasant simply because they do not comprehend it or have

sufficient knowledge of it. In light of this, one could contend that people may accept cyberattacks due to a feeling of "learned helplessness."Users may just accept the prospect of being victims due to a sense of learned helplessness (for more on the phrase, see: Seligman, 1975; Hirtz, 1998) and a lack of understanding regarding online attacks and how to deal with an incident. Additionally, the feeling of acquired helplessness may also have a negative impact on the adoption of protective security behaviours. As a result, regardless of whether they were in UG or PG, students may experience a sense of acquired helplessness, which has no discernible effect regardless of the student's variable year of study.

4.7 Differences in the co-relation between TPB constructs viz, knowledge, self-perception, actual cybersecurity skills and behaviour and attitude

In the current study, the Pearson correlation was used to evaluate the co-relation between TPB constructs. The strength of the linear link between two or more variables is gauged by the Pearson correlation. The independent and dependent variables can be tested using this technique to see how closely they are related to one another.

Hence, for each of the TPB constructs viz, knowledge, self-perception of skills, actual cybersecurity skills and behaviour, and attitude, based on data from all the questions on the various cybersecurity dimensions viz. password security, network security, website security, system security, social networking site security, and operational security.

Table 48: Co-relations between TPB constructs viz, knowledge, self-perception, actual cybersecurity skills and behaviour and attitude for cybersecurity

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)					

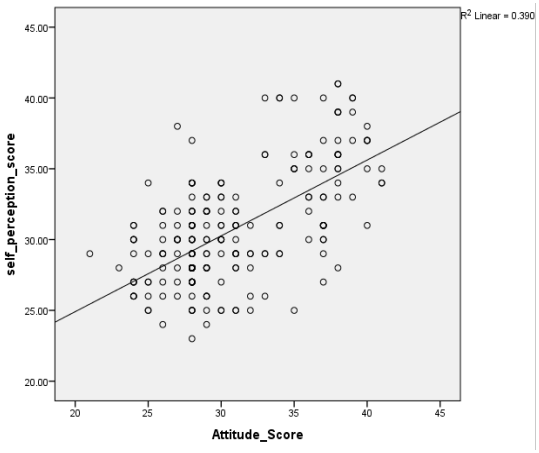


Figure 18: Co-relations between self-perception, and attitude for cybersecurity

Table 48& figure 18shows that all four TPB constructs—knowledge, self-perception of skills, actual skills, and behaviour and attitude—have positive connections with one another. The greatest positive correlation is seen between self-perception of skills and attitude, with the other associations having relatively moderate values. This shows how knowledge, one's perception of one's own talents, those actual skills, behavior, and attitude are all positively correlated. In other words, when students learn and develop their cybersecurity knowledge and abilities, they are more likely to have a positive attitude towards the subject, which in turn strengthens their knowledge and actions.

“According to Chandarman and Van Niekerk's (2017), knowledge, one's opinion of their own talents, and their actual skills and behaviours are all positively correlated. The strongest positive correlation is between one's perceived skills and their actual skills and behavior, with the other correlations having relatively low values. This demonstrates the positive, though modest, correlations between knowledge, one's impression of one's own talents, and one's actual skills and behaviour.”

Overall, our results indicate that a thorough strategy for enhancing cybersecurity among university students should take into account using all four TPB constructs and concentrate on expanding the knowledge, skills, attitude, and conduct in an integrated manner. These findings imply that the TPB can serve as a valuable framework for analysing and encouraging university students' cybersecurity awareness including action.

4.8 Students readiness regarding cybersecurity awareness training program

Table 49: Frequency and percentage distribution of the selected university students of the Vadodara city according to their readiness regarding cybersecurity awareness training program

(n=242)

Sr. No.	Students readiness regarding cybersecurity awareness training program	f	%
1	Yes	86	35.5
2	No	156	64.5

(n=242)

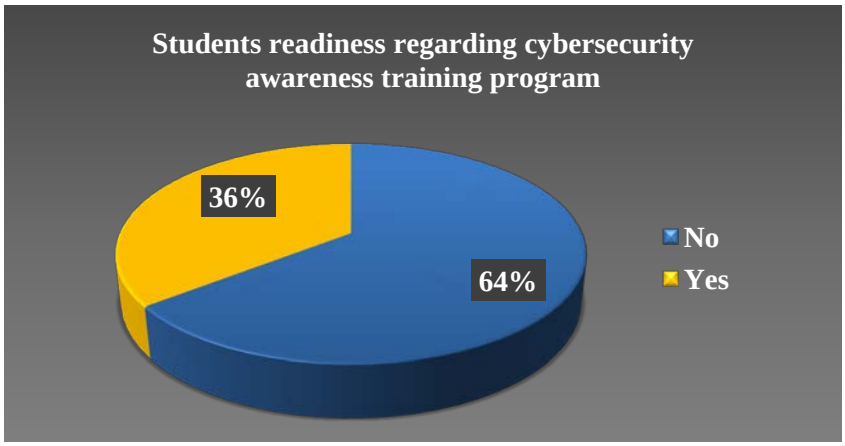


Figure 19 - Percentage distribution of the selected university students of the Vadodara city according to their readiness regarding cybersecurity awareness training program

Table 48& figure 19 reveals the frequency and percentage distribution of the respondents according to their readiness regarding cybersecurity awareness training program. It shows that one third of the respondents i.e. 35.5% were ready for the training, whereas majority of the respondents i.e. 64.5% were had refused to undergo cybersecurity awareness training program. The probable reason could be that, there may not be enough mentors or role models in the field of cybersecurity for students particularly Gen Z to look up to and learn from. Kim (2014) found that many college students in the US did not participate in information security awareness training, even though they appeared to understand the need for and importance of the training. The study also revealed that the students' security education came in bits and pieces from many sources and that in order for them to establish secure behaviors that would last. This shows for they needed to take part in more concentrated information security and awareness training.

CHAPTER 5
SUMMARY

CHAPTER 5

SUMMARY

5.1 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.

According to Internet and Mobile Association of India (IAMAI) and consultancy company Kantar, by 2025, India's internet user base will be close to 1 billion. Social commerce platforms were used to make more than 500 million digital transactions, representing more than half of the country's online shoppers. By 2025, there will be 50% of all students using online learning in some capacity. (Pramshu, 2022, May 17).

5.1.1 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. Data must be accurate, and any changes must be obvious.
- Accessibility is crucial since data is only useful if it is **available**.

5.1.2 University vulnerability to cyber threats/attack at global level and in India

Despite the fact that 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.

5.1.3 Significance of cyber security awareness

When the COVID-19 pandemic began, students wishing to advance their education without attending classes or training facilities have 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 importance of cybersecurity awareness amongst the university staff, students in higher education institutions.

5.1.4 Statement of Problem

To seek the answers to the research questions, it was decided to conduct a research study on the **"Cybersecurity awareness among the university students of the Vadodara, 2022-23"**

5.1.5 Objectives of the study

1. To prepare the profile of the selected university students of the Vadodara.
2. To assess the overall cybersecurity awareness among the selected university students of the Vadodara.
3. To assess the overall cybersecurity awareness among the selected university students of the Vadodara with reference to the following variables:
    a) Age
    b) Gender
    c) Type of university
    d) Year of Study
    e) Internet usage pattern
    f) Digital competency

g) Issues encountered during cyber surfing

4. To study the differences in the overall cybersecurity awareness of the selected university students of the Vadodara with reference to the selected variables.
5. To assess the cybersecurity awareness using Theory of Planned Behaviour (TPB) constructs viz, knowledge, self-perceptions, actual skills and behaviour and attitude among the selected university students of Vadodara.
6. 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 with reference to the selected variables.
7. To study the co-relations within the TPB constructs viz, knowledge, self-perceptions, actual skills and behaviour and attitude in the context of cybersecurity awareness.
8. To identify the readiness regarding cybersecurity awareness training program of the selected university students of Vadodara.

5.1.6 Null Hypotheses of the study

1. There will be no significant differences in the overall cybersecurity awareness of the selected university students of the Vadodara in relation to the selected variables.
2. There will be no significant differences in the TPB constructs viz, knowledge, self-perceptions, actual skills and behaviour and attitude among the selected university students of Vadodara with reference to the selected variables.
3. There will be no co-relation within the TPB constructs viz, knowledge, self-perceptions, actual skills and behaviour, and attitude in cybersecurity awareness.

5.1.7 Assumptions of the study

- Selected university students of the Vadodara will possess cyber security knowledge.
- Security awareness of selected university students, Vadodara will vary in their cyber security awareness level according to the selected variables.
- Practices regarding cyber security used by the selected university students of the Vadodara will vary.

5.1.8 Delimitations of the study

- The study will be delimited to the selected university of the Vadodara only.
- The study will be delimited to the cyber security awareness only.

5.2 Methodology

This study aims to investigate the "**Cybersecurity awareness among the university students of Vadodara, 2022-2023."**

Icek Ajzen developed the Theory of Planned Behavior (TPB) in an attempt to predict human behavior (Ajzen, 1991). It is a psychological theory that connects beliefs and behaviors. 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 operational definition of the cybersecurity awareness in the present study, the most fitted Theory of Planned Behavior (TPB) framework used by Chandarman R. & Van Niekerk, B. (2017), in their study entitled "Students' Cybersecurity Awareness at a Private Tertiary Educational Institution" has been adapted in the present study.

5.2.1 Population of the study

The population of this study include students from selected government and private universities accredited by the University Grants Commission (UGC) of Vadodara for 2021-2022.

5.2.2 Sample of the study

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

5.2.3 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 pattern, a scale for digital competency, a knowledge test, a self-perception scale, actual skill and behavior as well as an attitude scale for the purpose of gathering 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 of the people regarding cyber security awareness.

5.2.4 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:

(I) Demographic details and (II) The subscales of the Theory of planned behavior (TPB) model.

(III) Demographic information included age, gender, year of study, internet usage pattern, and digital competency. The tool of digital competency was adapted using the modified version "Digital Competence Assessment Framework (DIGCOMP) framework" by Evangelinos G & Holley D (2015) used for the current study. (http://eprints.bournemouth.ac.uk/23477/)

(IV) The sub-scales of constructs viz a knowledge test, self-perception scale, actual skill and behavior as well as attitude scale items were prepared to keep in mind the CIA (Confidentiality, Integrity, and Availability) Triad model. This focused on six cyber security dimensions viz password security, network security, website security, system security, social networking site security, and operational security as a framework for the questions and statements. Moreover, the question regarding the readiness of participants to take cybersecurity awareness training was also included. A detailed description of each of the seven sections is given below.

Table 50: 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	Parameters	Total No. of items	Tools	Response system
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
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 behaviour	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
Section G	Student's readiness regarding cybersecurity awareness training.	4	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.

5.2.5 Validation 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. Minor

modifications were made to the tool based on suggestions and feedback received from experts.

5.2.6 Reliability of the research tool

To assure internal and external consistency, the tool's reliability was assessed.

- The test-retest method has been used to assure external consistency.
- The Cronbach's Alpha coefficient test was used to measure internal consistency.

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.

5.2.7 Pre-testing of the Research Tool

In order to evaluate the questionnaire's clarity, a pre-test of the tool was conducted with ten university students to evaluate the language's clarity and determine how long it would take to complete the form. The tool was made simple and understandable by removing ambiguous items which were found. The average time to fill up the questionnaire was 10-15 minutes.

5.2.8 Ethical Approval of the Study by IECHR Committee

The study was presented to IECHR Committee for ethical approval on 24th November 2022. It was approved by the ethical committee with ethical approval number IECHR/FCSc/M.Sc./2022/18.

5.2.9 Data Collection

To study cyber security awareness among the university students of Vadodara, 2022-23, the data was collected from 242 university students aged between 18-28 years of Vadodara by the researcher from November to December, 2022. The data was collected 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. Out of total 252 distributed questionnaires, total 10 incomplete/ invalid questionnaires were excluded and considered 242 valid questionnaires for formal data analysis. 139 samples were collected through online mode, whereas 103 were collected offline mode. In total, 116 male students and

126 female students submitted valid responses. Questionnaires which found incomplete, ambiguous were dismissed.

5.2.9.1 Difficulties faced while collecting the data

b. Respondents required constant repeated reminders.

5.2.9.2 Tabulation of Data

c. Data were coded in accordance with the conclusions on the response scores, as discussed below.

d. The researcher created Excel spreadsheet for the same purpose.

5.2.10 Scoring and Categorization of the Data

5.2.10.1 Scoring and Categorization of Variables

Table 51: Categorization of variables of the study

Sr. No.	Variables	Basis		Categories
1.	Age	18-23		Young
		24-29		Old
2.	Gender	Male		Male
		Female		Female
		Other		Other
3.	Type of University	Government (as per UGC list)		Government
		Private (as per UGC list)		Private
4.	Year of study	Undergraduate	First year	First year
			Second year	Second year
			Third year	Third year
			Fourth year	Fourth year
			Fifth year	Fifth year
		Post-graduate	First year	First year
			Second year	Second year
5.	Internet usage pattern	Below mean		Moderate users
		Mean and Above mean		Heavy users
6.	Digital competency	Lower level of competency		Beginner
		Medium level of competency		Intermediate
7.	Issues encountered during Cyber surfing	Dropped as a Variable after data collection		

5.2.10.2 Scoring and categorization of Internet usage pattern

Table 52: Scoring of data for Internet usage pattern

Type of statements	Minimum score	Maximum score
Multiple choice questions	9	50
Total	**9**	**50**

Table 53: Categorization of scores in internet usage pattern

Variable	Range	Basis	Categories
Internet usage pattern	9-29	Below mean	Moderate use
	30-50	Mean and Above mean	Heavy use

5.2.10.3 Scoring and categorization of digital competency

Table 54: Scoring of data for Digital Competency

Total no. of items	Minimum score	Maximum score
15	15	45

Table 55: Categorization of scores in digital competency

Variable	Range	Basis	Categories
Digital Competency	15-30	Mean and Below mean	Beginner
	31-45	Above Mean	Intermediate

5.2.10.4 Scoring and categorization of student's overall cybersecurity awareness

Table 56: Categorization of scores in student's overall cybersecurity awareness

Variable	Range	Basis	Categories
Student's overall cybersecurity awareness	61-85	Mean and Below mean	Low awareness
	86-110	Above Mean	High awareness

5.2.10.5 Scoring and categorization of student's cybersecurity knowledge

Table 57: The possible scores of the knowledge test

Type of statements	Minimum score	Maximum score
Multiple choice questions	0	20
Total	**0**	**20**

Table 58: Categorization of scores in student's cybersecurity knowledge

Variable	Range	Basis	Categories
Cybersecurity Knowledge	0-10	Mean and Below Mean	Less Knowledgeable
	11-20	Above Mean	Knowledgeable

5.2.10.6 Scoring and categorization of student's self-perception of cybersecurity skills

Table 59: Scoring pattern according to the nature of statement regarding student's self-perception of cybersecurity skills

Statements	Great Extent	Some Extent	Less Extent
Positive statements	3	2	1
Negative statements	1	2	3

Table 60: Scoring of data for student's self-perception of cybersecurity skills

Total no. of items	Minimum score	Maximum score
14	14	42

Table 61: Categorization of scores in student's self-perception of cybersecurity skills

Variable	Range	Basis	Categories
Self-perception of cybersecurity skills	14-28	Below mean	Unfavourable
	29-42	Mean and Above Mean	Favourable

5.2.10.7 Scoring and categorization of student's actual cybersecurity skills and behavior

Table 62: The possible scores of student's actual cybersecurity skills and behavior

Type of statements	Minimum score	Maximum score
Multiple choice questions	0	24
Total	**0**	**24**

Table 63: Categorization of scores in student's actual cybersecurity skills and behavior

Variable	Range	Basis	Categories
Actual cybersecurity skills and behaviour	0-11	Mean and Below mean	Unsafe
	12-24	Above Mean	Safe

5.2.10.8 Scoring and categorization of student's cybersecurity attitude

Table 64: Scoring pattern according to the nature of statement regarding student's cybersecurity attitude

Statements	Great Extent	Some Extent	Less Extent
Positive statements	3	2	1
Negative statements	1	2	3

Table 65: Scoring of data for student's cybersecurity attitude

Total no. of items	Minimum score	Maximum score
14	14	42

Table 66: Categorization of scores in student's cybersecurity attitude

Variable	Range	Basis	Categories
Student's cybersecurity attitude	14-28	Below mean	Negative Attitude
	29-42	Mean and Above Mean	Positive Attitude

5.2.10.9 Correlation base

Table 67: Categorization of scores in correlation

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

Pearson correlation coefficient formula:

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

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

5.2.11 Plan for Statistical Analysis of the Data

Table 68: Different statistical measure used for the analysis of the data

Sr. No.	Purpose	Statistical measures
1	Demographic profile of the students	Percentages
2.	Internet usage pattern of the students	Percentages
3.	Digital competency of the students	Percentages
4.	Overall cybersecurity awareness of the students	Percentages
5.	Variable wise overall cybersecurity awareness of the students	Percentages
6.	Differences in the overall cybersecurity awareness of the students with respect to variables	t-test and ANOVA
7.	Overall knowledge, Self-perceptions, actual skills and behaviour, attitude (as per TPB framework) for Cybersecurity awareness of the students	Percentages

Sr. No.	Purpose	Statistical measures
8.	Differences in the knowledge, self-perceptions, actual skills and behaviour and attitude (as per TPB framework) regarding cybersecurity awareness of the students	Mann-Whitney U, Kruskal Wallis Test, t-test and ANOVA
9	Differences in the co-relation within TPB constructs viz, knowledge, self-perception, actual cybersecurity skills and behaviour and attitude	Correlation
10	Readiness of students regarding cybersecurity awareness training program	Percentages

5.3 Major Findings

Demographic profile of the respondents

- 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 from Private University, and rest were from Government University.
- 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). Remaining 30% of the respondents were postgraduate students in their first and second years of study.
- Majority of the respondents, i.e., 60.7% were moderate internet users.
- High majority (70.7%) of the respondents were found with primary level of digital competency skills i.e. Beginner followed by 29.3% of them with advance digital competency skills i.e. Intermediate.
- High majority of the respondents, i.e., 83% were not fallen victim to online crimes, whereas 17% of respondents had fallen victim to the online crime.
- 17% of the respondents responded that they have faced issues during cyber surfing. Amongst which 35% and 30% reported issues related to phishing emails and malware respectively.

I. Overall cybersecurity awareness of the selected university students of Vadodara

- Majority, 62.8% of the respondents, had low cybersecurity awareness, followed by less than forty percent (37.2%) having a higher level of cybersecurity awareness.

Differences in overall Cyber Security Awareness (CSA) of the selected university students of the Vadodara in relation to the selected variables

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

II. <u>Theory of planned behaviour core constructs</u>

A. CSA and overall knowledge of the respondents

i. More than half (53.7%) of the respondents were having less knowledge on cyber security, followed by less than half (46.3%) of them having knowledge of cybersecurity.

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

ii. There was **significant** difference found in the respondents' knowledge regarding cybersecurity in relation to the variable, viz, digital competency.

iii. 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

i. Majority of the respondents i.e. 67.4% had unfavorable perceptions, whereas one-third of the respondents i.e., 32.6% had favorable perceptions.

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

ii. There were **significant** differences found in the self-perception regarding cybersecurity skills of the respondents in relation to the variables viz, gender, type of university and internet usage pattern.

iii. There were **no significant** differences found in the self-perception of cybersecurity skills of the respondents in relation to variable viz. their age, digital competency and year of study.

C. CSA and overall Actual skills and behavior of the respondents

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

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

ii. There were **significant** differences found in the actual cybersecurity skills and behavior of the respondents in relation to the variables viz, age, type of university and digital competency.

iii. There were **no significant** differences found in the actual cybersecurity skills and behavior of the respondents in relation to their gender, internet usage pattern and year of study.

D. CSA and overall Attitude of the respondents

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

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

ii. 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.

iii. 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.

III. Differences in the co-relationships between TPB constructs viz, knowledge, self-perception, actual cybersecurity skills and behaviour 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 with the strongest positive correlation, however, rest of the three construct's showed moderate association with one another.

Student's readiness regarding cybersecurity awareness training program

- Only one third of the respondents i.e. 35.5% were ready for the cybersecurity training, whereas majority of the respondents i.e. 64.5% were not willing to undergo cybersecurity awareness training program.

5.4 Conclusion

The present study was conducted with the main focus on the "Cybersecurity awareness among the university students of the Vadodara, 2022-23".

The study revealed that majority of the respondents had low awareness regarding cybersecurity.

While daily technology breakthroughs make our society more linked than ever and simplify our daily lives, they also increase the risks to our personal 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 softwares 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 organisations under pressure when its targeted the most. Higher education organisations 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, despite the fact that 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 implicates that a complete solution is required since the root reasons of university students' poor cybersecurity knowledge, negative self-perception, unsafe/dangerous cybersecurity skills and behaviour, and negative attitude may be complicated.

The constructs of the TPB framework exhibit positive results in the current investigation. The association between knowledge, one's own impression of one's own 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, behaviour, 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 usage of social media, blogs, online courses, and other resources, in order to increase awareness and encourage safe conduct. University students can be protected from cyber dangers and assist to create 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.

5.5 Future Recommendations for Research

1. This study can be taken up on larger scale by including parents and teachers along with students to measure CSA.
2. Needs and expectations of the school/ university students for CSA can be studied.
3. A comparative study assessing cybersecurity awareness of the government school going children Vs private school children can be conducted in Gujarat and other states of India

4. A research study on designing and developing cybersecurity training intervention 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.

CITED LITERATURE

Adamu, A. G., 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, 12(1), 572.

Ahaskar, A. (2021, February 8). Cyber threats disguised as online learning platforms grew by 60% in H2 2020 | Mint. Mint. https://www.livemint.com/technology/tech-news/cyber-threats-disguised-as-online-learning-platforms-grew-by-60-in-h2-2020-11612784120540.html

Alanazi, M., Freeman, M., &Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. Computers in Human Behavior, 136, 107376.

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

Almarabeh, T., Majdalawi, Y. K., & 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), 577-587.

Alqahtani, M. A. (2022). Cybersecurity awareness based on software and e-mail security with statistical analysis. Computational Intelligence and Neuroscience, 2022

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Anand, N., Jain, P., Prabhu, S., Thomas, C., Bhat, A., Prathyusha, P. V., Bhat, S., Young, K. S., & 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), 458–467. https://doi.org/10.4103/ijpsym.ijpsym_135_18

Anand, Nitin, et al. “Internet Use Patterns, Internet Addiction, and Psychological Distress Among Engineering University Students: A Study from India.” Indian Journal of Psychological Medicine, vol. 40, no. 5, Sept. 2018, pp. 458–67. DOI.org (Crossref), https://doi.org/10.4103/IJPSYM.IJPSYM_135_18.

Anwar, M., He, W., Ash, I. K., 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.2016.12.040

Aswathi, P., & Mohamed Haneefa, K. (2019). Attitude towards Information Technology and digital divide: A study among students in Universities in Kerala, India

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Academic Press

Barnicoat, C. A. (2014). Perceptions of cyberbully victimization among college students: An examination using routine activities theory (Doctoral dissertation, Middle Tennessee State University

Benson, V., & McAlaney, J. (Eds.). (2019). Emerging cyber threats and cognitive vulnerabilities. Academic Press

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.

Bogdanovskaya, I., Koroleva, N., & Uglova, A. (2020). Digital competence and information security in adolescents. In Ceur Workshop Proceedings (pp. 63-72)

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and* Communication, 20, 133-155.

Chasanah, B. R., & Candiwan, C. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia. SISFORMA, 7(2), 49-57.

Daengsi, T., Pornpongtechavanich, P., & 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), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

Debb, S. M., Schaffer, D. R., & 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), 42-55

Dwarakanath, S., Ravi, K., & Vijayakumar, R. (2022). A Study on the Emotions of an Employee After a Cyber Security Attack in Their Organization.

Eduljee, N. B., & Kumar, S. S. (2015). Patterns of Internet use with Indian students from aided and unaided Colleges. Asian Journal of Multidisciplinary Studies, 3(7), 32-43.

Evangelinos, G., & 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).

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The 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. https://doi.org/10.1088/1742-6596/1339/1/012098

Funke, J. (2017). How much knowledge is necessary for action? In P. Meusburger, B. Werlen, & L. Suarsana (Eds.), Knowledge and Action (pp. 99–111). Springer International Publishing. https://doi.org/10.1007/978-3-319-44588-5_6

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, *2012*(3), 12-15.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. Int. J. Emerg. Technol, 11(5), 41-49.

Garba, A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. Science Proceedings Series, 2(1), 82-86

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. PloS one, 12(2), e0171620.

Hargittai, E., & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social science quarterly*, *87*(2), 432-448.

Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia. Journal of Social Sciences, 11(4), 395.

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies*, *28*(1), 439-470.

Hossain, M. A., & Rahman, M. H. (2017). Comparative study of internet usage among university students: A study of the University of Dhaka, Bangladesh. European Scientific Journal December.
https://www.vonage.com/resources/articles/generational-gap-cybersecurity-privacy/

Igba, I. D., Igba, E. C., Nwambam, A. S., Nnamani, S. C., Egbe, E. U., &Ogodo, J. V. (2018). Cybercrime among university undergraduates: implications on their academic achievement. International Journal of Applied Engineering Research, 13(2), 1144-1154.

Joseph, J., Varghese, A., Vijay, V. R., Dhandapani, M., Grover, S., Sharma, S., Khakha, D., Mann, S., &Varkey, B. P. (2021). Prevalence of internet addiction among college students in the Indian setting: A systematic review and meta-analysis. *General Psychiatry*, *34*(4), e100496. https://doi.org/10.1136/gpsych-2021-100496

Khawrin, M. K. (2022). An Assessment of Cyberbullying Behavior among Gujarat University Students in Relation to Gender, Age, and Internet Surfing. IAHRW International Journal of Social Sciences Review, 10(4), 390-395.

L. Slusky and P. Partow-Navid, "Students information security practices and awareness," International Journal of Information Security, vol. 8, no. 4, pp. 3–26, 2012, doi: 10.1080/15536548.2012.10845664.

Moallem, A. (2019). Cyber security 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.

Moletsane, T., &Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. In 2020 conference on information communications technology and society (ICTAS) (pp. 1-6). IEEE.

Nagaur, A. (2020). Internet Addiction and Mental Health among University students during CVOID-19 lockdown. MuktShabd J, 9, 684-692.

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.

Nyikes, Z., &Baimakova, K. V. (2016). An Examination of the Relationship between Security Awareness and Digital Competence.

Ozdamli, F., &Uzunboylu, 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

Pham, H., Brennan, L., & Richardson, J. (2017, June). Review of behavioural theories in security compliance and research challenge. In Informing Science and Information Technology Education Conference, Vietnam (pp. 65-76). Santa Rosa, CA: Informing Science Institute

Reddy, G. N., & Reddy, G. J. U. (2014). A study of cyber security challenges and its emerging trends on latest technologies. arXiv. https://doi.org/10.48550/arXiv.1402.1842

Safarpour, F., Kurd, N., &Ghazanfari, Z. (2021). A Study on Internet Usage Pattern among Students at the Medical University of Ilam and Influential Factors. Biomedical Journal of Scientific & Technical Research, 33(2), 25761-25765.

Sanzgiri, V., & Sanzgiri, V. (2022). 12.67 lakh cyber attacks reported in India by November 2022: IT Ministry in Parliament. MediaNama.https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/

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

Senthilkumar, K., & Easwaramoorthy, 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.

Skinner, W., & Fream, 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

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

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

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.

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

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.

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

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.

WEBLIOGRAPHY

"Most Students Say Cyber Security Is a Growing Threat | Computer Weekly." ComputerWeekly.Com, https://www.computerweekly.com/news/4500278781/Most-students-say-cyber-security-is-a-growing-threat. Accessed 7 Apr. 2023

Ahaskar, A. (2021, February 8). *Cyber threats disguised as online learning platforms grew by 60% in H2 2020*. Mint. https://www.livemint.com/technology/tech-news/cyber-threats-disguised-as-online-learning-platforms-grew-by-60-in-h2-2020-11612784120540.html

BL New Delhi Bureau. (2022, March 15). Indian Gen Z spends average 8 hours a day online: report. https://www.thehindubusinessline.com/news/variety/indian-gen-z-spends-average-8-hours-a-day-online-report/article65227021.ece

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.). http://eprints.bournemouth.ac.uk/23477/

Bureau, B. N. D. (2022, March 15). *Indian Gen Z spends average 8 hours a day online: Report*. https://www.thehindubusinessline.com/news/variety/indian-gen-z-spends-average-8-hours-a-day-online-report/article65227021.ece

Campbell, S. (2017). Cybersecurity in Higher Education: Problems and Solutions. ToptalToptal Insights Blog. https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

CIA Triad in Cyber Security: Definition, Examples, Importance. (n.d.). https://www.knowledgehut.com/blog/security/cia-in-cyber-security

Cyber crime in india: An overview. (n.d.). Retrieved April 9, 2023, from https://legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html

Cyber security awareness and why it is important | Australian Institute of ICT. (n.d.). Retrieved April 9, 2023, from https://aiict.edu.au/blog/what-is-cyber-security-awareness-and-why-is-it-important/

Cyber space and the various challenges attached to the regulation of information and communication technology. - Lawpanch. (2022, March 2). https://lawpanch.com/cyber-space-and-the-various-challenges-attached-to-the-regulation-of-information-and-communication-technology-%ef%bf%bc/

Cybersecurity awareness is about both "knowing" and "doing." (2014, October 1). *Security Intelligence*. https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/

Cybersecurity in higher education: Problems and solutions | toptal®. (n.d.). ToptalToptal Insights Blog. Retrieved April 9, 2023, from https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

Delhi university, amu, iit-bhu websites hacked; "pakistan zindabad", pro-kashmir messages seen. (n.d.). India Today. Retrieved April 9, 2023, from https://www.indiatoday.in/india/story/delhi-university-amu-website-pakistan-zindabad-kashmir-kashmiri-youths-indian-army-973492-2017-04-25

Desk, I. T. W. (2017, April 25). Delhi University, AMU, IIT-BHU websites hacked; 'Pakistan Zindabad', pro-Kashmir messages seen. India Today. https://www.indiatoday.in/india/story/delhi-university-amu-website-pakistan-zindabad-kashmir-kashmiri-youths-indian-army-973492-2017-04-25

Desk, T. (2022, June 13). 18 out of every 100 Indians victim of data breaches: SurfShark. The Indian Express. https://indianexpress.com/article/technology/tech-news-technology/18-out-of-every-100-indians-affected-by-data-breaches-surfshark-7967560/

Dunning-kruger effect | definition, examples, & facts | britannica. (2023, March 27). https://www.britannica.com/science/Dunning-Kruger-effect

Economic Diplomacy Division. https://indbiz.gov.in/india-to-have-nearly-1-billion-internet-users-by-2025-report/

Education report cybersecurity. (n.d.). Security Scorecard. Retrieved April 25, 2023, from https://resources.securityscorecard.com/all/education-report-cybersecurity

Facts and figures 2021. (n.d.). Retrieved April 6, 2023, from https://www.itu.int/itu-d/reports/statistics/2021/11/15/youth-internet-use

Indian education sector biggest target of cyber threats, remote learning among key triggers: Report. (2022, May 1). *The Times of India*. 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

Lara. (2018, February 24). *Answer to "What's the difference between "knowledge of sth" and "perception of sth "?"* English Language & Usage Stack Exchange. https://english.stackexchange.com/a/432673

Matters, S. M. (n.d.). Patterns of internet usage among youth in india. Social Media Matters. Retrieved April 6, 2023, from https://www.socialmediamatters.in/internet-usage-among-youth-in-india

Measuring digital development: Facts and Figures 2022. (n.d.). ITU Hub. Retrieved April 9, 2023, from https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/

Murnane, K. (n.d.). How men and women differ in their approach to online privacy and security. Forbes. Retrieved April 6, 2023, from https://www.forbes.com/sites/kevinmurnane/2016/04/11/how-men-and-women-differ-in-their-approach-to-online-privacy-and-security/

Pramshu. (2022, May 17). India to have nearly 1 billion Internet users by 2025: Report - IndBiz | Economic Diplomacy Division. IndBiz | Economic Diplomacy Division. https://indbiz.gov.in/india-to-have-nearly-1-billion-internet-users-by-2025-report/

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

Redmonster.In. (2022). Cyber Space and the various Challenges attached to the regulation of Information and Communication Technology. - LawPanch. LawPanch - Let's Spread Law. https://lawpanch.com/cyber-space-

and-the-various-challenges-attached-to-the-regulation-of-information-and-communication-technology-%EF%BF%BC/

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

Security Culture Report. (n.d.). Knowbe4. https://www.knowbe4.com/hubfs/Security-Culture-Report.pdf

Statistics. (n.d.). ITU. Retrieved April 9, 2023, from https://www.itu.int:443/en/ITU-D/Statistics/Pages/stat/default.aspx

Statistics. (n.d.). ITU. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

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

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

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

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

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

Wilde, N. (2022). The benefits of cyber security awareness training within universities. Open Access

Government. https://www.openaccessgovernment.org/the-benefits-of-cyber-security-awareness-training-within-universities/139452

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

BIBLIOGRAPHY

Amreliwala J. (2020). A study on the satisfaction level of the mothers/guardians regarding services rendered in the child malnutrition treatment centre (CMTCS) of Vadodara district 2019-20.

Bhate, K. (2020). Information and communication technology in higher education. University.

Damor P. (2021). Knowledge and practices of selected citizens of Ahmadabad city of Gujarat state to combat covid-19, 2020-2021.

Devnani S. (2018). Knowledge and Perceptions of Selected Citizens of Vadodara City regarding Organ Donation.Leena, C. (2018). Use of internet for performance of household responsibilities by married women of Vadodara city. University.

Thakor S. (2022). A study on barriers in use of smartphone among the senior citizens residing in Vadodara city.

Trivedi B. (2020). A study on web series and its influence on selected youth of Vadodara city.

Appendix-1

Tool Validation Letter

DEPARTMENT OF EXTENSION AND COMMUNICATION
FACULTY OF FAMILY AND COMMUNITY SCIENCES
THE MAHARAJA SAYAJIRAO UNIVERSITY OF BARODA,
VADODARA

To, Date:

Subject: Covering letter for Tool Validation

Respected Sir/ Madam,

I, **Ms. Manasi Nimbekar**, Master student of the Department of Extension and Communication, Faculty of Family and Community Sciences, The Maharaja Sayajirao University of Baroda, Vadodara, is working on a research study entitled, **"Cybersecurity Awareness among the university students of Vadodara, 2022-23"**.

In this regard, I have prepared questionnaire to assess "Awareness" level of selected university students of Vadodara. The attached questionnaire contains questions regarding Cybersecurity Awareness. You are selected as one of the experts to validate the tool as you have had the valuable experiences of working in this field. I request you to validate the tool of my research in terms of its content validity, response system to make my study valuable.

I wish to convey my thanks in anticipation for contributing your valuable suggestions and your valuable time to help me to make an authentic tool.

Thanking You

Sr. M.Sc. EC student

Ms. Manasi Nimbekar
Batch 2021-23

Guide

Dr. Varsha Parikh,
Associate Professor
Faculty of Family and Community Sciences
The Maharaja Sayajirao University of Baroda,
Vadodara.

Appendix-2

Consent Letter

Consent letter

Department of Extension and Communication
Faculty of Family and Community Sciences
The Maharaja Sayajirao University of Baroda, Vadodara

STATEMENT OF INFORMED CONSENT FROM RESPONDENT

Dear Respondent,

My name is Ms. Manasi Nimbekar and I am a Senior Master student of Department of Extension and Communication, Faculty of Family and Community Sciences, The Maharaja Sayajirao University of Baroda, Vadodara. As a part of my study of partial fulfilment of dissertation, I am carrying out a research on, **"CYBERSECURITY AWARENESS AMONG THE UNIVERSITY STUDENTS OF VADODARA, 2022-23."** The aim of the study is to assess the overall cyber security awareness among the selected university students of the Vadodara.

The Department of Extension and Communication supports the practice of protection of human participants in research. The following will provide you with information about the research that will help you in deciding whether or not you wish to participate. Participation in this study is voluntary and it is entirely up to you to answer or not answer any question or the questionnaire.

In this questionnaire the respondents will be asked to provide information related to own profile viz age, gender, year of study, stream, programme, name of university, internet access, and usage pattern as well as items related to awareness.

You have been selected by chance as respondent for this tool. There is no risk/harm as well as benefit in responding this questionnaire. But your response and valuable feedback will help us in understanding how much people are aware about cyber security and what practices they follow to stay safe and stop the spread of cyber attacks for self and society. This study is purely linked only for educational purpose.

I respect your privacy and in no circumstances, your identity will be revealed directly or indirectly at any stage of the research and the information you provide will be kept strictly confidential. I request and really hope that you take part in responding this tool of questionnaire, it will take only 12-15 minutes of your valuable time.

If you have any further questions concerning this study, please feel free to contact us through phone or email: **Manasi Nimbekar** at [7433821224/manasinimbekar@gmail.com].

Your participation is important and is highly appreciated.

Thanking you.

Ms. Manasi Nimbekar **Dr. Varsha Parikh**

Research Scholar **Research Guide**

Signature of Participants _____

Appendix-3
Research Tool

Section-A

Demographic Profile

Directions – Please carefully read the following information, and where applicable, mark it with a checkmark or write it in the space provided.

1. Email ID: _____
2. Mobile Number: _____
3. Age (In years): _____
4. Gender: coding
   - ☐ Male **1**
   - ☐ Female **2**
   - ☐ Other (please specify): _____ **3**
   - ☐ Prefer not to say **4**
5. Name of the University: _____
6. Type of University: coding
   - ☐ Government **1**
   - ☐ Private **2**
   - ☐ Any other (Specify) **3**
7. Stream/ specialization: _____
8. Programme: coding
   - ☐ Undergraduate **1**
   - ☐ Post-Graduate Degree/ Diploma **2**
   - ☐ Ph.D. & above **3**
   - ☐ Any other (please specify): _____ **4**
9. Year of study: coding
   - ☐ 1st year **1**
   - ☐ 2nd year **2**
   - ☐ 3rd year **3**
   - ☐ 4th year **4**
   - ☐ 5th year **5**
   - ☐ Any other (please specify): _____ **6**

Section-B

Note: This section comprised information related to respondent's Internet Usage Pattern, Digital Competency & Issues encountered by respondent during cyber surfing.

A) Internet Usage Pattern

Directions – Please read following items related to your internet usage pattern carefully read the following information, and where applicable, mark it with a checkmark or write it in the space provided.

1. Since how many years you are using internet?_____ (In years) **(1)**

2. Which of the following devices do you use daily to connect to the internet?
(can select > 1 option)

☐ Desktop	**1**	**(1)**
☐ Laptop	**2**	**(1)**
☐ Smart Phone	**3**	**(1)**
☐ Any other (please specify): _____	**4**	**(1)**

3. From which of the following places you are using internet? (can select >1 option)

☐ At home	**1**	**(1)**
☐ At college	**2**	**(1)**
☐ At Library	**3**	**(1)**
☐ At my friend's home	**4**	**(1)**
☐ At café	**5**	**(1)**
☐ Any other (please specify): _____	**6**	**(1)**

4. How do you access internet? (can select > 1 option)

☐ Broadband (wired/ unwired at home)	**1**	**(1)**
☐ Mobile Network	**2**	**(1)**
☐ Public Wi-Fi	**3**	**(1)**
☐ Private Wi-Fi	**4**	**(1)**
☐ University Wi-Fi	**5**	**(1)**
☐ I do not know	**6**	**(1)**
☐ Any other (please specify): _____	**7**	**(1)**

5. Frequency of using internet

i) How frequently do you use the internet?

☐ Everyday	**1**	**(1)**
☐ Once or twice a day	**2**	**(1)**
☐ Once a week	**3**	**(1)**
☐ Don't know	**4**	**(1)**
☐ Any other (please specify): _____	**5**	**(1)**

ii) How much hours do you typically spend online/use internet each day?

☐ 4 hours or more	**1**	**(1)**
☐ 3-4 hours	**2**	**(1)**
☐ 2-3 hours	**3**	**(1)**
☐ 1-2 hours	**4**	**(1)**
☐ 1 hour or less	**5**	**(1)**

6. For which of the following reasons do you use the internet?

(can select > 1 option)

☐ Entertainment (e.g.to watch movies, gaming, etc)	**1**	**(1)**
☐ Education (e.g. study, research, assignment/ project, etc)	**2**	**(1)**
☐ E-commerce (e.g. online shopping)	**3**	**(1)**
☐ E-payment (e.g. online banking)	**4**	**(1)**
☐ To communicate (e.g. chatting, video/ voice calling, sharing information and files, etc)	**5**	**(1)**
☐ Any other (please specify): _____	**6**	**(1)**

7. Which of the following information do you collect/ access/ store as part of your easy access? (can select > 1 option)

☐ Aadhaar card number	1	(1)
☐ My PRN/ college unique ID	2	(1)
☐ Bank account information	3	(1)
☐ Debit card information	4	(1)
☐ Credit card information	5	(1)
☐ PAN card	6	(1)
☐ Voter ID	7	(1)
☐ Driving License	8	(1)
☐ None of the above	9	(1)
☐ Any other (please specify): _____	10	(1)

8. Which of the following Social Networking Sites do you use? (can select > 1 option)

☐ Facebook	**1**	**(1)**
☐ WhatsApp	**2**	**(1)**
☐ Instagram	**3**	**(1)**
☐ YouTube	**4**	**(1)**
☐ Snapchat	**5**	**(1)**
☐ Any other social network site (please specify): _____	**6**	**(1)**

Minimum Score- 9

Maximum Score – 50

Range of the Section is 9 – 50

B) Digital Competency

Directions – Please read carefully following items related to your digital device competency and select your appropriate digital competency level by tick marking in ANYONE column in the space provided.

Here, GE represents **Great Extent**; **SE** represents **Some Extent; LE** represents **Less Extent**

i) What level of proficiency do you have in handling the following Internet tasks?

Sr. No.	Statements	GE	SE	LE
	I can-			
1	use a variety of search engines to access information.	3	2	1
2	use variety of filter process to evaluate the accuracy and liability of information.	3	2	1
3	download data from the internet in a variety of forms.	3	2	1
4	use a variety of online communication platforms, including e-mail, chat, SMS, instant messaging, blogs, and social networks.	3	2	1
5	use collaboration tools to create/ manage materials (e.g. Google docs, online spreadsheets).	3	2	1
6	actively engage in online forums/ use a variety of online services (such as e-banking, online shopping, and public services).	3	2	1
7	use the internet to pass on information to others (e.g., through social networking sites or online communities).	3	2	1
8	create complex digital content in various formats such as text, tables, images, audio files.	3	2	1
9	use many tools for advanced formatting features (such as mail merge, combining documents of various formats, using advanced algorithms and macros), using the internet.	3	2	1
10	use licenses/ copyrights information when creating online content.	3	2	1
11	check whether security software installed on the device(s) which access the internet(e.g. antivirus, firewall).	3	2	1
12	use the cloud's data storage services.	3	2	1
13	activate or configured/ change security settings in my digital devices.	3	2	1
14	find or deal with solutions to the more common issues that come up using digital technologies.	3	2	1
15	find support from computer professional when a technical issue in digital device arise.	3	2	1

Minimum score – 15

Maximum score – 45

Range of the Section is 15 - 45

B) Issues encountered during cyber surfing

Directions – Please read carefully following items and state the issues encountered by you during cyber surfing and where applicable, mark it with a checkmark or write it in the space provided.

i) Have you ever fallen victim to online crime? (E.g., losing data or an email account; having your computer infected with malware or spyware; having your photos or digital devices stolen)

- ☐ Yes **(1)**
- ☐ No **(0)**

ii) If yes, which of the following cyber related issues you have ever faced?

- ☐ I got a phishing emails (requesting money, personal info or bank details) **1** **(1)**
- ☐ Identity fraud (somebody stealing your personal information and impersonating you, for example, by tweeting under your name) **2** **(1)**
- ☐ Malware (e.g. virus) infected equipment **3** **(1)**
- ☐ Being prevented from using online services (such as banking services) as a result of cyberattacks **4** **(1)**
- ☐ Unintentionally coming across content that encourages hate or religious extremism **5** **(1)**
- ☐ Online blackmail (a request for money made in order to cease or prevent extortion or to avoid scandal) **6** **(1)**
- ☐ Any other (please specify): _____ **7** **(1)**

(iii) Being a victim whom did you report about the cybercrime?

- ☐ Police department **1**
- ☐ Cybercrime protection cell of your city **2**
- ☐ Family/ friends **3**
- ☐ e-portal of government **4**
- ☐ No one **5**
- ☐ Any other (please specify): _____ **6**

(iv) If no one, reason for not reporting.

_____

2) Do you feel possibility of being victim in future?

- ☐ Yes **1**
- ☐ No **0**

a) If yes, whom would you report that?

_____

b) If no, what is the reason?

_____

Minimum score – 0

Maximum score – 8

Range of the Section is 0 - 8

Section-C
Student's Cybersecurity Knowledge

Directions – Following questions are regarding cybersecurity knowledge in relation to personal computer/ laptop/ mobile/ I-pad/ tablet used by you. Please select the most appropriate answer according to you.

1. What is software piracy?
   - ☐ Stealing the technology and devices of others (0)
   - ☐ **Unlawful and Unofficial copying or downloading software** **(1)**
   - ☐ Watch a film without paying for it (0)
   - ☐ Purchase legally movie-related software (0)

2. Which of the following does not contribute to email security being maintained?
   - ☐ **Opening unknown links/websites** **(1)**
   - ☐ Connect your email with all digital devices (0)
   - ☐ Use two-factor authentication for password verification and login (0)
   - ☐ Creating strong password with lower, uppercase, number & special character (0)

3. Which of the following act is not done by Trojans?
   - ☐ Deleting Data (0)
   - ☐ **Protecting Data** **(1)**
   - ☐ Modifying Data (0)
   - ☐ Copying Data (0)

4. _____ is sending spam or unsolicited emails to any target victim's inbox.
   - ☐ Phishing (0)
   - ☐ **Spamming** **(1)**
   - ☐ Hooking (0)
   - ☐ DoS (0)

5. In _____ phishing, specific keywords are targeted and a fake webpage is built while waiting for the searcher to arrive at the fake webpage.
   - ☐ Voice (0)
   - ☐ SMS (0)
   - ☐ **Search engine** **(1)**
   - ☐ Email (0)

6. When you visit a website, _____ are small files that are downloaded to your computer.
   - ☐ **Cookies** **(1)**
   - ☐ Caches (0)
   - ☐ Bots (0)
   - ☐ Crawlers (0)

7. The built-in security app called the _____ by Microsoft is intended to filter network data from your Windows system and prohibit hazardous communications or the apps that are starting them.
   - ☐ Windows Security Essentials (0)
   - ☐ Windows applications (0)
   - ☐ **Windows Firewall** **(1)**
   - ☐ Windows Security commands (0)

8. Turn on _____ just when you need to use it; otherwise, turn it off for security reasons.
   - ☐ **Blue tooth** **(1)**
   - ☐ App updates (0)
   - ☐ Flashlight (0)
   - ☐ Rotation (0)

9. Which of the following actions won't spread the virus?
   - ☐ Infected website (0)
   - ☐ Emails (0)
   - ☐ **Official Antivirus CDs** **(1)**
   - ☐ USBs (0)

10. _____ is an online fraud run by cybercriminals, in which sensitive data is obtained from the user via digital methods.
    - ☐ **Phishing attack** **(1)**
    - ☐ DoS attack (0)
    - ☐ Website attack (0)
    - ☐ MiTM attack (0)

11. A number of social media platforms and services offer _____ to properly verify accounts.

☐	Retina scanning	(0)
☐	Fingerprint scanning	(0)
☐	CAPTCHA	(0)
☐	**2-step verification**	**(1)**

12. There are three standard measures used to safeguard information accessibility:

☐	Redundancy, backups and access controls	(0)
☐	**Encryption, file permissions and access controls**	**(1)**
☐	Access controls, logging and digital signatures	(0)
☐	Hashes, logging and backups	(0)

13. Which of the following passwords are more secure? (can select > 1 option)

☐	**Wtf!9C**	**1**	**(1)**
☐	**M#P52s@ap$V**	**2**	**(1)**
☐	12345	3	(0)
☐	aarti99	4	(0)

14. Which of the following is a proper precaution for social networking account security? (can select > 1 option)

☐	**Strong passwords**	**1**	**(1)**
☐	**Link your account with a phone number**	**2**	**(1)**
☐	**Never write your password anywhere**	**3**	**(1)**
☐	Maintain a soft copy of all your passwords in your PC	**4**	(0)

15. From given URLs which are secure? (can select > 1 option)

A. https://www.xyz.com
B. http://www.xyz.com
C. https://www.registry.gov.in
D. https://www.quora.com
E. http://www.quora.com

☐	**A, C**	**1**	**(1)**
☐	B, D	2	(0)
☐	**C, D**	**3**	**(1)**
☐	**A, D**	**4**	**(1)**

Minimum score – 0

Maximum score – 20

Range of the Section is 0-20

Section-D

Student's Self-Perception of cybersecurity Skills

Direction: Please read following statements carefully and tick mark in the most appropriate Column by expressing your own self-perception regarding cyber skills in relation to personal life i.e. cybersecurity acts in relation to own/ family digital devices, for academic life i.e. cybersecurity acts for academic purposes and social life i.e. cybersecurity acts in relation to connecting people in society thru social network sites, online games etc.

(Scoring pattern for Positive Statement is 3, 2 and 1 and for Negative Statements 1, 2, 3)

Here, GE represents **Great Extent**
SE represents **Some Extent**
LE represents **Less Extent**

+ve or -ve	Sr. No	Statements	GE	SE	LE
1	**1**	**Personal Life**			
P	1.1	A phishing mail is simple to identify.	3	2	1
P	1.2	Users' privacy can be protected through a Virtual Private Network (VPN).	3	2	1
P	1.3	Passwords on all digital devices should be changed on a frequent basis to reduce vulnerability to cyber threats..	3	2	1
N	1.4	Using old passwords is safe while changing passwords.	1	2	3
N	1.5	It's safe to conduct online transactions using public Wi-Fi.	1	2	3
2		**Academic Life**			
P	2.1	It's safe to clear your browser history while using a computer at a cybercafé, college, or another location.	3	2	1
P	2.2	USB plugging at a college computer lab raises the possibility of drives getting viruses.	3	2	1
N	2.3	It's safe to share digital devices with close friends.	1	2	3
P	2.4	While looking on various educational websites, it is imperative that you read the cookie access authorization policies carefully.	3	2	1

+ve or -ve	Sr. No	Statements	GE	SE	LE
3		**Social Life**			
N	3.1	Publicly posting a live location on social media is not detrimental.	1	2	3
N	3.2	You can continue watching movies, web series, or listen to music using authorized programmes after getting a warning message.	1	2	3
N	3.3	One becomes easily popular by sharing private images on social media.	1	2	3
P	3.4	It is dangerous to accept requests/ messages from strangers on social networking sites.	3	2	1
N	3.5	On social media threats/ suspicious activities are informal and do not need to be reported to the cyber cell.	1	2	3

Positive Statements - 7

Negative Statements - 7

Minimum score – 14

Maximum score – 42

Range of the Section is 14 - 42

Section - E

Student's Actual Cybersecurity skills and behavior

Directions – Following questions are regarding your actual cybersecurity skills and behavior in relation to use of digital devices. Please select the most appropriate answer which describes your cyber security behavior/ skills the most in practice.

1. From the following given security tools and applications for computer/ laptops/ mobile, etc. which are you using in your digital devices? (can select > 1 option)
   - **a) Anti-virus** **1** **(1)**
   - **b) Authentication (e.g. Password, PIN)** **2** **(1)**
   - **c) Encryption** **3** **(1)**
   - **d) Software update** **4** **(1)**
   - **e) Backup** **5** **(1)**
   - **f) Firewall** **6** **(1)**
   - g) Any One (please specify): _____ 7 (1)
   - h) None 8 (0)

2. You are visiting a cybercafé to take print out of your project work documents, from your e-mail. While the print-out is processing, you are accessing your social media profile and checks other e-mails. As soon as the printouts are ready, you rush to collect it. You close the browser window without logging out of the account and leave the cybercafé. After two hours you receive a notification that the password of your social media account has been reset. Now you are trying hard but unable to access your social media account. What can be the reason that you are unable to access your social media account?

   a) Your social media account has been hacked as you were accessing it from cyber café (0)
   b) You forgot her social media account password and hence could not access it. (0)
   c) You forgot to logout from your account in cybercafe, made you victim of identity threat. (1)
   d) Nothing to worry. New social media account can be created. (0)

3. Which of these are good methods to prevent yourself from identity theft?
   (can select > 1 option)
   a) Keeping an eye on your money or purse while shopping 1 (1)
   b) Phone calls whereby you disclose your Aadhaar number 2 (0)
   c) Only using trusted websites to enter your credit card information 3 (1)
   d) Choosing strong, difficult-to-guess passwords 4 (1)

4. You were in dire need of an internet and suddenly find public Wi-Fi available without a password so, you'll;
   a) Connect to it and use the internet, (0)
   b) Ask stranger to share mobile hotspot (0)
   c) Wait until you get to the destination then use the internet (1)
   d) Ask around about internet speed, and use it swiftly to finish the work. (0)

5. The mouse pointer on your computer screen starts to move and click on things by itself. How will you proceed?
   a) Call people to witness the miracle (0)
   b) Alternatively, unplug your computer hardware from the network or the internet. (0)
   c) Shut down your computer system. (0)
   d) Run your antivirus or call an expert immediately (1)

6. I update my anti-virus software and other applications in my devices;

(can select > 1 option)

a)	**Monthly**	**1**	**(1)**
b)	When I get reminder	2	(0)
c)	**As soon as system of the devices prompts me**	**3**	**(1)**
d)	Never	4	(0)

7. You receive a call in which a person is asking you about buying electric vehicle as company is celebrating 75th year of independence offering huge discount and your ordered it and paid the required amount. After that you didn't receive any call or message regarding your order. What do you do in this situation?

a)	**It was a phishing call, I should immediately report it to city's cybercrime center**	**(1)**
b)	May be some other reasons of not receiving any call or message	(0)
c)	Don't do anything	(0)
d)	None of the above	(0)

8. Strong passwords can be challenging to recall. What can you do to ensure that you remember them? (can select > 1 option)

a)	Use the mnemonics (acronyms or phrases that are simple for you to remember)	**1**	(1)
b)	Create a password strategy	**2**	(1)
c)	Use encryption-enabled password management software.	**3**	(1)
d)	Use of long, strong and new passwords for each website and account.	**4**	(1)
e)	**All of the above**	**5**	**(4)**

9. To stay safe online I ensure following actions before/during browsing; (can select > 1 option)

a)	**Keep track by reviewing/changing the security settings on my browser/search engine**	**1**	**(1)**
b)	**Limit who can see my posts on social media**	**2**	**(1)**
c)	**Ensure installation and timely updating of anti-virus software on my all devices**	**3**	**(1)**
d)	I pretend to be someone else online	4	(0)

10. What should you do if a message stating that a group of viruses has to be eliminated has shown on your computer?

a) **I choose to disregard the warning and get an antivirus application from a reputable source. (1)**
b) You open a window and immediately download the specified programme to safeguard your device (0)
c) You run an old system scan using the anti-virus software that is already installed. (0)
d) Any of the above (0)

Minimum score – 0

Maximum score – 24

Range of the Section is 0-24

Section - F

Student's Cybersecurity Attitude

Direction: Below mentioned are certain statements. Please carefully read the following information, and where applicable, mark it with a checkmark the most appropriate response of yours in relation to personal life i.e. cybersecurity acts in relation to own/ family digital devices, for academic life i.e. cybersecurity acts for academic purposes and social life i.e. cybersecurity acts in relation to connecting people in society thru social network sites, online games etc. in the given space.

(Scoring pattern for Positive Statement is 3, 2 and 1 and for Negative Statements 1, 2, 3)

Here, GE represents **Great Extent**
SE represents **Some Extent**
LE represents **Less Extent**

+ve / -ve	Sr. No	Statements	GE	SE	LE
1	**1**	**Personal Life**			
		I would -			
P	1.1	use Wi-Fi password to prevent unauthorized people from using my home network.	3	2	1
N	1.2	disable security options in my digital device to work faster.	1	2	3
P	1.3	prefer to secure files and emails using encryption software.	3	2	1
N	1.4	create an account by using different ID if I want to know about a person whom I don't know	1	2	3

+ve / -ve	Sr. No	Statements	GE	SE	LE
1	**1**	**Personal Life**			
		I would -			
P	1.5	keep my cybersecurity knowledge updated to guard against threats or attacks online.	3	2	1
2	**2**	**Academic Life**			
		I would -			
P	2.1	register for seminar/ conferences only on those educational websites that clearly state their privacy rules.	3	2	1
N	2.2	rarely backup my files from my department's PC.	1	2	3
N	2.3	put all electronic files in a folder with my name on it, and place it on the desktop in the department computer lab so I can easily get to it the following day for work.	1	2	3
N	2.4	never get an email with a dangerous attachment from my university student email address.	1	2	3
P	2.5	set the computer screen to lock automatically, when don't use it frequently or for a long time.	3	2	1
3	**3**	**Social Life**			
		I would-			
N	3.1	give my correct details of name, age, gender, location while playing online games with strangers.	1	2	3
N	3.2	use obscene language on social networking sites	1	2	3
P	3.3	keep my social networking site account or profile private.	3	2	1
P	3.4	worried about unintentionally coming across porn on the website utilised.	3	2	1

Positive Statements - 7

Negative Statements - 7

Minimum score – 14

Maximum score – 42

Range of the Section is 14 - 42

Section - G

Student's readiness regarding cybersecurity awareness training

Directions – Please carefully read the following information, and where applicable, mark it with a checkmark or write it in the space provided.

i) Are you interested in taking up cybersecurity training?

☐ Yes		(1)
☐ No		(0)

ii) If yes, what kind of training would you like to select?

☐ 30 hours' course	1	(1)
☐ Certificate course	2	(1)
☐ 2-days workshop	3	(1)
☐ 1-day webinar	4	(1)
☐ From government officials only	5	(1)
☐ From online courses available	6	(1)
☐ Any other (please specify): _____	7	(1)

1. From whom would you like to take training?

☐ Covering in your college curriculum	1	(1)
☐ Undertaking value added course offered by your department	2	(1)
☐ From outside computer classes	3	(1)
☐ Any other (please specify): _____	4	(1)

2. In which of the following topics do you see the need for cyber security training in? (can select > 1 option)

☐ Types, platforms to report and combating cyber crime	1	(1)
☐ Security control	2	(1)
☐ Data privacy security	3	(1)
☐ E-Commerce digital payment and its security	4	(1)
☐ Overview of social media and its security	5	(1)
☐ Cybersecurity of digital devices `	6	(1)
☐ Cyber security practices	7	(1)
☐ Do's & Don'ts	8	(1)
☐ Any other (please specify): _____	9	(1)

Minimum score – 0

Maximum score – 21

Range of the Section is 0 - 21

Appendix-4
Ethical Committee-Approval Certificate

Institutional Ethics
Committee for Human
Research
(IECHR)

FACULTY OF FAMILY AND COMMUNITY SCIENCES,
THE MAHARAJA SAYAJIRAO UNIVERSITY OF BARODA,
VADODARA

Ethical Compliance Certificate 2022-2023

This is to certify that Ms. Manasi Nimbekar's study titled, "Cyber Security Awareness Among the university students of the Vadodara city, 2022-23" has been approved by the institutional Ethics Committee for Human Research (IECHR), Faculty of Family & Community Sciences, The maharaja Sayajirao University of Baroda, Vadodara. The study has been allotted the ethical approval number IECHR/FCSc/M.Sc./2022/18

Prof. Shagufa Kapadia
Chairperson ,
IECHR

Prof. Mini Sheth
Member Secretary
IECHR

Chair Person
IECHR
Faculty of Family & Community Sciences
The Maharaja Sayajirao University of Baroda

Appendix-5
Plagiarism Report

FINAL - Copy.pdf

By: mansi1

As of: Apr 16, 2023 4:35:53 PM
38,701 words - 300 matches - 105 sources

Similarity Index

8%

Mode: Similarity Report

paper text:

CHAPTER 1 INTRODUCTION 1.1 Cyberspace 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** 23

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 cyber world refers to this online environment. 1.1.1 Digital Development Scenario National Information Centre (NIC) created India's cyberspace officially in 1975 to provide government information technology solutions. According to

Internet and Mobile Association of India (IAMAI) **and** consultancy company **Kantar** , by 2025, **India** 20

's internet user base will be close to 1 billion. Social commerce platforms were used to make more than 500 million digital transactions, representing more than half of the country's online shoppers. By 2025, there will be 50% of all students using online learning in some capacity. (Pramshu, 2022, May 17). Nine out of ten active users online spent a daily average of 107 minutes. The study found that in both rural and urban India, the three most popular applications

of the internet were **for social** media, communication, **and entertainment** . (Statistics, (**n** 10

.d.).

ITU. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/ default.aspx 51

sources:

1 309 words / 1% - Internet from 25-Nov-2020 12:00AM
www.scielo.org.za

2 288 words / 1% - ProQuest
Soni, Uma. "A Study of Environmental Knowledge and Values of Undergraduate Students of The Maharaja Sayajirao University of Baroda, Vadodara", Maharaja Sayajirao University of Baroda (India), 2020

3 266 words / 1% - ProQuest
Mistry, Pooja. "Usage, Opinions and Problems of Web-Based Learning by Undergraduate Students of the Maharaja Sayajirao University of Baroda", Maharaja Sayajirao University of Baroda (India), 2021

4 180 words / < 1% match - ProQuest
Parikh, Varsha. "A study of the perceptions of media professionals and professionals other than media regarding the contemporary role of the newspaper and television in democracy.", Maharaja Sayajirao University of Baroda (India),

5 163 words / < 1% match - ProQuest
Bhate, Krutika. "Information and Communication Technology in Higher Education", Maharaja Sayajirao University of Baroda (India)

6 138 words / < 1% match - Internet from 01-Nov-2022 12:00AM
www.anchor-publishing.com

7 63 words / < 1% match - Internet from 10-Sep-2022 12:00AM
link.springer.com

8 54 words / < 1% match - Internet from 17-Jul-2022 12:00AM
link.springer.com

9 8 words / < 1% match - from 27-Mar-2023 12:00AM
link.springer.com

10 118 words / < 1% match - ProQuest
Chauhan, Leena. "Use of Internet for Performance of Household Responsibilities by Married Women of Vadodara City.", Maharaja Sayajirao University of Baroda (India), 2020

11 76 words / < 1% match - ProQuest
Sidhpura, Megha. "Health Communication Strategies under National Health Mission in Chhotaudepur District of Gujarat State.", Maharaja Sayajirao University of Baroda (India), 2021

12 65 words / < 1% match - ProQuest
Dasgupta, Debolina. "Perceptions of teachers, parents and media professionals regarding media education in schools.", Maharaja Sayajirao University of Baroda (India),

13 65 words / < 1% match - Internet from 22-Jan-2023 12:00AM
www.homescienceassociationofindia.com

14 16 words / < 1% match - Internet from 18-Jul-2022 12:00AM
www.researchgate.net

15 12 words / < 1% match - Internet from 29-Dec-2022 12:00AM
www.researchgate.net

16 10 words / < 1% match - Internet from 02-Mar-2023 12:00AM
www.researchgate.net

17 9 words / < 1% match - Internet from 10-Feb-2023 12:00AM
www.researchgate.net

18 8 words / < 1% match - Internet from 15-Oct-2022 12:00AM
www.researchgate.net

19 6 words / < 1% match - Internet from 24-Feb-2023 12:00AM
www.researchgate.net

20 47 words / < 1% match - Internet from 13-Dec-2022 12:00AM
dspace.hmlibrary.ac.in

21 45 words / < 1% match - Internet
Mercado, J, Mercado, M A V. "Assessing the Level of Effectiveness of Marketing Activities of HEIs in the National Capital Region", 'Knowledge E', 2018

22 40 words / < 1% match - Crossref
"Innovations in Cybersecurity Education", Springer Science and Business Media LLC, 2020

23 39 words / < 1% match - Internet from 10-Jan-2023 12:00AM
lawpanch.com

24 38 words / < 1% match - ProQuest
Bhatia, Ritu. "A study of the perceptions of adolescents regarding the influence of television advertisements on the selected aspects of their lives.", Proquest, 2016.

25 34 words / < 1% match - Internet from 03-Mar-2023 12:00AM
eprints.mdx.ac.uk

26 15 words / < 1% match - Internet from 05-Feb-2022 12:00AM
www.mdpi.com

27 10 words / < 1% match - Internet from 05-Sep-2022 12:00AM
www.mdpi.com

28 9 words / < 1% match - Internet from 13-Nov-2022 12:00AM
www.mdpi.com

29 32 words / < 1% match - Internet from 03-Mar-2021 12:00AM
www.aessweb.com

30 31 words / < 1% match - Crossref
Nooraslinda Abdul Aris, Zafiruddin Baharum, Zuraidah Mohd Sanusi, Ibrahim Kamal Abdul Rahman, Lee Teck Heang. "Assessment of critical success factors for accounting graduates employability", 2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC), 2013

31 22 words / < 1% match - Internet from 04-May-2022 12:00AM
www.coursehero.com

32 9 words / < 1% match - Internet from 23-Feb-2023 12:00AM
WWW.coursehero.com

33 28 words / < 1% match - ProQuest
Bhargava, Veenu. "A study of vocational aspirations of home science college students and their opinions regarding adequacy of their preparation to take up vocations.", Proquest, 2016.

34 26 words / < 1% match - Crossref
Serge Egelman, Eyal Peer. "Scaling the Security Wall", Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15, 2015

35 26 words / < 1% match - Internet from 04-Aug-2022 12:00AM
ccc.msubaroda.ac.in

36 25 words / < 1% match - Internet from 04-Jan-2017 12:00AM
researchbank.rmit.edu.au

37 24 words / < 1% match - Internet from 05-Apr-2021 12:00AM
mobile.wiredspace.wits.ac.za

38 23 words / < 1% match - Internet from 12-Jan-2023 12:00AM
files.eric.ed.gov

39 23 words / < 1% match - Internet from 05-Dec-2019 12:00AM
hiba.edu.sy

40 22 words / < 1% match - Internet from 15-Mar-2023 12:00AM
pubmed.ncbi.nlm.nih.gov

41 20 words / < 1% match - Internet
Garba, Adamu Abdullahi, Siraj, Maheyzah Muhamad, Othman, Siti Hajar. "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria", 'Institute of Advanced Engineering and Science', 2022

42 20 words / < 1% match - Internet
Knowles, Serena. "Improving clinical practice in intensive care: Implementation of an evidence based protocol for bowel management", ACU Research Bank, 2013

43 19 words / < 1% match - Internet from 27-Sep-2022 12:00AM
etd.hu.edu.et

44 18 words / < 1% match - Crossref
Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, Hamdullah Nejat Basim. "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", Journal of Computer Information Systems, 2020

45 18 words / < 1% match - Internet from 15-Feb-2022 12:00AM
library.nhrc.gov.np

46 16 words / < 1% match - Internet from 12-Jan-2023 12:00AM
d85bc6ea86296c327d7f-fc14fae93feb1cf1ff31873061ee8f7d.ssl.cf1.rackcdn.com

47 16 words / < 1% match - Internet from 25-Nov-2022 12:00AM
www.scstatehouse.gov

48 14 words / < 1% match - Internet from 13-Oct-2022 12:00AM
dspace.knust.edu.gh

49 14 words / < 1% match - from 08-Apr-2023 12:00AM
ir.kneu.edu.ua

50 14 words / < 1% match - Internet from 06-Nov-2022 12:00AM
pure.royalholloway.ac.uk

51 13 words / < 1% match - Internet from 23-Dec-2022 12:00AM
scholar.law.colorado.edu

52 12 words / < 1% match - Crossref
Dragana Draganac, Danica Jović, Ana Novak. "Digital Competencies in Selected European Countries among University and High-School Students: Programming is lagging behind", Business Systems Research Journal, 2022

53 12 words / < 1% match - Internet from 18-Dec-2021 12:00AM
sala-35.sciencesconf.org

54 12 words / < 1% match - Internet from 09-Apr-2021 12:00AM
sersc.org

55 12 words / < 1% match - Internet from 21-Aug-2022 12:00AM
www.bsg.ox.ac.uk

56 11 words / < 1% match - Internet from 05-Apr-2022 12:00AM
www.brockbusu.ca

57 11 words / < 1% match - Internet from 13-Apr-2022 12:00AM
zenodo.org

58 10 words / < 1% match - Internet from 16-Jul-2021 12:00AM
docplayer.net

59 10 words / < 1% match - Internet from 21-Sep-2017 12:00AM
pubs.sciepub.com

60 10 words / < 1% match - Internet from 09-Jan-2021 12:00AM
www.toptal.com

61 9 words / < 1% match - Crossref
"Advances in Human Factors and Ergonomics in Healthcare and Medical Devices", Springer Science and Business Media LLC, 2019

62 9 words / < 1% match - ProQuest
Garbovan, Lidis. "Politics of Waiting on Hope: Exploring Embodied Experiences of Tibetans Living in India as Guests and Citizins", Canterbury Christ Church University (United Kingdom)

63 9 words / < 1% match - Crossref
Xianfeng Hu, Shanyong Wang, Rongting Zhou, Lan Gao, Zujun Zhu. "Policy driven or consumer trait driven? Unpacking the EVs purchase intention of consumers from the policy and consumer trait perspective", Energy Policy, 2023

64 9 words / < 1% match - Internet from 20-Jan-2023 12:00AM
core.ac.uk

65 9 words / < 1% match - Internet from 26-Dec-2022 12:00AM
dokumen.pub

66 9 words / < 1% match - Internet from 04-Nov-2021 12:00AM
hillpublisher.com

67 9 words / < 1% match - Internet from 27-Sep-2021 12:00AM
irjms.in

68 9 words / < 1% match - Internet from 20-Oct-2019 12:00AM
nsuworks.nova.edu

69 9 words / < 1% match - from 20-Mar-2023 12:00AM
ojs.unud.ac.id

70 9 words / < 1% match - Internet from 11-Dec-2022 12:00AM
repository.sustech.edu

71 9 words / < 1% match - Internet from 13-Dec-2022 12:00AM
workofriti.files.wordpress.com

72 9 words / < 1% match - Internet from 19-Dec-2020 12:00AM
www.forbes.com

73 9 words / < 1% match - Internet from 01-Mar-2022 12:00AM
www.igi-global.com

74 9 words / < 1% match - Internet from 15-Jan-2019 12:00AM
www.sdiarticle2.org

75 8 words / < 1% match -
"SK298 topic 5 addictions WEB083718", Open University

76 8 words / < 1% match - Crossref
Tamara Almarabeh, Yousef Kh. Majdalawi, Hiba Mohammad. "Internet Usage, Challenges, and Attitudes among University Students: Case Study of the University of Jordan", Journal of Software Engineering and Applications, 2016

77 8 words / < 1% match - Internet from 05-May-2021 12:00AM
academic.oup.com

78 8 words / < 1% match - Internet from 17-Oct-2021 12:00AM
apmaj.uitm.edu.my

79 8 words / < 1% match - from 22-Mar-2023 12:00AM
apps.dtic.mil

80 8 words / < 1% match - Internet from 16-Jan-2023 12:00AM
digitalcommons.usf.edu

81 8 words / < 1% match - Internet from 13-Mar-2023 12:00AM
iieta.org

82 8 words / < 1% match - Internet from 05-Oct-2022 12:00AM
ijrcm.org.in

83 8 words / < 1% match - Internet from 29-Oct-2022 12:00AM
journalppw.com

84 8 words / < 1% match - Internet from 22-Oct-2022 12:00AM
journals.najah.edu

85 8 words / < 1% match - Internet from 27-Sep-2022 12:00AM
scholarworks.sjsu.edu

86 8 words / < 1% match - from 09-Apr-2023 12:00AM
sin.put.poznan.pl

87 8 words / < 1% match - Internet from 13-Jan-2023 12:00AM
telemetr.io

88 8 words / < 1% match - Internet from 09-Jan-2020 12:00AM
ufdc.ufl.edu

89 8 words / < 1% match - from 30-Mar-2023 12:00AM
www.asianinstituteofresearch.org

90 8 words / < 1% match - Internet from 24-Sep-2022 12:00AM
www.ijcseonline.org

91 8 words / < 1% match - Internet
Qin An, Wilson Cheong Hin Hong, XiaoShu Xu, Yunfeng Zhang, Kimberly Kolletar-Zhu. "How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates", International Journal of Information Security

92 8 words / < 1% match - Internet from 13-Jan-2023 12:00AM
www.science.gov

93 7 words / < 1% match - Crossref
Batoul Bakkar, Fatema Mohsen, Humam Armashi, Marah Marrawi, Nizar Aldaher. "A cross-sectional survey of COVID-19: attitude and prevention practice among Syrians", Heliyon, 2022

94 7 words / < 1% match - ProQuest
Mehta, Shivani . "A Study on Silver Workers Residing in Vadodara City.", Maharaja Sayajirao University of Baroda (India), 2019

95 7 words / < 1% match - Crossref
Therdpong Daengsi, Phisit Pornpongtechavanich, Pongpisit Wuttidittachotti. "Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks", Education and Information Technologies, 2021

96 7 words / < 1% match - Internet
Toro-Jarrin, Miguel Angel. "Predictors of Email Response: Determinants of the Intention of not Following Security Recommendations", ODU Digital Commons, 2022

97 6 words / < 1% match - Crossref
"Information Systems", Springer Science and Business Media LLC, 2022

98 6 words / < 1% match - Crossref
Arjun Kishan Pillay, Neeraj Anand Sharma. "Applicable Cyber Security Recommendations to Prevent Cyber Attacks in Universities", 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2022

99 6 words / < 1% match - Crossref
M. Suresh, S. Ravi. "chapter 6 Online Database Use by Science Research Scholars of Alagappa University, Karaikudi", IGI Global, 2020

100 6 words / < 1% match - Crossref
Mohammed Khader, Marcel Karam, Hanna Fares. "Cybersecurity Awareness Framework for Academia", Information, 2021

101 6 words / < 1% match - Crossref
Saadat M. Alhashmi, Mohamed Salem M. Bayou. "An exploratory study of the information security awareness of business school students in UAE", International Journal of Business Information Systems, 2021

102 6 words / < 1% match - ProQuest
Townsend, Howard E., III. "An Examination of the Significance of Security Knowledge and Attitudes on Security Behavior", Capella University, 2022

103 6 words / < 1% match - Internet
P, Aswathi, Haneefa K, Mohamed. "Attitude towards Information Technology and Digital Divide: A Study among Students in Universities in Kerala, India", DigitalCommons@University of Nebraska - Lincoln, 2020

104 6 words / < 1% match - Internet
Lejaka, Tebogo. "A framework for cyber security awareness in small, medium and micro enterprises (SMMEs) in South Africa", 2021

105 4 words / < 1% match - Internet from 25-Sep-2022 12:00AM
www.europeanproceedings.com