IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY ON CYBERSECURITY AWARENESS AMONG FACULTY AND STUDENTS AT ASSAM DON BOSCO UNIVERSITY, GUWAHATI

[1]Henry V.L Nghilhlova Zote, [2]Dr. Tania Sur Roy, [3]Oshyajem Longkumer

[1]Research Scholar, [2]Assistant Professor (Senior) and Head of the Department, [3]Research Scholar
[1]Department of Education,
[1]Assam Don Bosco University, Guwahati, Assam, India

Abstract: Internet connectivity is frequently regarded as one of the most crucial amenities provided by modern educational institutions. Online services have become essential elements of the quickly changing learning and teaching environment of the 21st century to fulfil the demands of modern educational needs. This study examined at the students and faculties level of cybersecurity awareness in Assam Don Bosco University, Guwahati. In the current study, a descriptive cum normative survey was used to collect data from 80 students and 20 faculty members from the social sciences and the sciences streams. A 5-point Likert scale on cybersecurity was specifically created to serve the study's objectives in determining cybersecurity knowledge. The 't' test was also employed to analyze the variation in group means. Results showed that among Assam Don Bosco University students and faculty, "gender" and "stream" are not indicators of cybersecurity awareness.

***Index Terms* – Information Security, Cyber-values, Cyber-ethics, Curriculum, Higher Education**

I. INTRODUCTION

Today's organizations, which rely so heavily on technology, particularly the internet, to do business, can be both attacked physically and virtually as the cyber landscape is complex and constantly changing. Every time a security flaw is patched, a new one appears, and the fact that technology is involved provides attackers a tremendous edge over defenders. In addition to being able to attack anyone, anywhere, from their comfort zone, they frequently use automated techniques to pinpoint their victims and their vulnerabilities. Theft of the information does not necessitate its removal from its original place; therefore, the owner of the information may never discover that it was stolen.

Online criminal activity can include phishing, hacking websites, and compromising personal email and social media accounts. These have already caused significant disruption for individuals, groups, offices, organizations, agencies, businesses, governments, and nations. However, preventive measures can be taken to counteract each of these threats, thereby reducing the risk posed by the threats to online security. However, this will only be feasible if there is adequate knowledge and awareness about the dangers, their consequences, and the solutions to the problems. Recent studies reveals that the risk of an online security breach is becoming a major concern for everyone, but it is especially dangerous for young people, who spend most of their waking hours online. Furthermore, many young people are unaware of the security risks and threats associated with using the internet and electronic devices. Simply being aware of the risk and threat will not solve any problems associated with risk and security breaches if it is not put into practice, and users must be educated about the security threat and risk to create a safe online environment (Nidup, 2021). Ulevn & Wangen (2021) stated that higher education needs research on information security assets, threats, vulnerabilities, and risk.

II. ROLE OF CYBERSECURITY

According to Steingberg (2022) and Calder (2020), cybersecurity professionals frequently emphasize that the purpose of information security and cybersecurity is to protect the confidentiality, integrity, and availability (CIA) of data, also known as the CIA Triad.

- **Confidentiality:** Only those who require access to information systems and assets should be able to gain entry.
- **Integrity:** Information assets and systems must be safeguarded against unauthorized alteration, destruction, or loss.
- **Availability:** Information assets and systems must be accessible to authorized users on an as-needed basis.

Steinberg (2020) also emphasizes the possibility that cybersecurity threats can be viewed in terms that more accurately represent the human condition.

- **Privacy risks:** Dangers stemming from the potential lack of proper control over or misuse of personal or other confidential data include.

- **Financial risks:** There is the potential for monetary losses due to cyberattacks. Both direct and indirect financial losses are possible, such as the theft of funds from a bank account by a hacker who hacked into the account, or the loss of clients who no longer trust a small firm following a security breach.
- **Professional hazard:** Breach-related career dangers. Cybersecurity specialists are at risk of career damage if a breach occurs under their watch and is deemed negligent, but other professionals can also be harmed. Board members can be sued, sacked, etc. Professional damage can also occur if hackers expose private communications or data that shows someone in an unfavourable light, such as evidence that a person was penalised for inappropriate behaviour or sent an offensive email.
- **Business risks:** Like the professional dangers that an individual has, a business also faces hazards. After a security breach at Sony Pictures, the company's pay policies were shown in a bad light by internal documents that were made public.
- **Personal risks:** Numerous individuals save confidential details on their digital equipment, including explicit images and records of involvement in activities that may not be judged acceptable by members of their specific social circles. Leaks of such information can occasionally cause substantial harm to personal relationships. Stolen personal information can also make it easier for someone to steal your identity, which can cause several problems for you.
- **Physical danger dangers:** Cyberattacks on wastewater treatment plants, industries, and hospitals in recent years have made it abundantly evident that the failure to safeguard cybersecurity can put human lives at risk. For instance, in the year 2020, a German woman died while being moved between clinics after the hospital where she was a patient was infected with ransomware. And in 2021, a lawsuit was filed alleging that a new-born died because of medical errors made during her birth at an Alabama hospital during system disruptions induced by a ransomware assault.

III. Significance of cyber security in India

Singar & Akhilesh (2020) remarked that cybersecurity is not simply about protecting information or system resources. It's also about protecting humans in cyber environments who are vulnerable to ICT vulnerabilities. As ICT has become more pervasive, so too has the role of humans in cybersecurity evolved. In ICT security, humans pose a threat, although in information security, they are a crucial component of the system. Cybersecurity must safeguard individuals and societies. Humans are a menace and a weakness, but they are also the most precious asset in cyberspace. According to a recent survey, the number of cybercrime cases in the country has increased by 300%. This demonstrates that the digital domain is extremely susceptible to multiple invasions, such as the theft of sensitive national data, attacks on open networks that temporarily interrupt services, electronic scams via hacking, the theft of economically valuable computerized data, and cyberespionage. As India works hard to make its economy cashless, the risk of data breaches increases (Kulkarni & Akhilesh, 2020).

In addition, they focus on India's cybersecurity difficulties and challenges as outlined below.

- The 95% of hardware and software technologies as well as cyber security tools in India are imported, and India lacks the expertise to scan them for hidden Trojans, malware, rootkits, and weaknesses, leaving them vulnerable to cyberattacks. The sole sources of knowledge regarding these shortcomings and vulnerabilities are publicly accessible sources and vendor communication.
- Currently, there are no top-level experts for high-end jobs in cyber security, which emphasizes the need to build skills in these very sophisticated areas for building high-tech products indigenously or obtaining the knowledge and experience to critically examine them before implementation in the critical industry and infrastructure sector.
- There is a need for professional hands-on cyber security specialists in the five primary functional areas of cyber security, as there are currently only 62,000 trained cybersecurity professionals and the demand will increase to 1 million by 2025's end (NASSCOM's Cyber security Task Force).
- In India, there are no formal courses at the graduate level on cyber security, and there are no training ideas such as virtual laboratories and cyber ranges.
- A smartphone can be utilized as a remote-controllable master-spying device without the owner's awareness. The majority of the one billion mobile phone users do not know this. Consequently, this lack of awareness must be addressed (Kulkarni & Akhilesh, 2020).

IV. Review of the related literature

According to Townsend (2021), In the year 2020, cybercriminals focused their attention on Michigan State University, The University of California, and Columbia College Chicago for the following three reasons such as:

- **Financial possibilities:** As with most of the hacking, financial opportunities have always been the major motivation; in 2018, 79% of assaults on educational institutions were financially oriented. Cybercriminals have numerous chances, ranging from stealing money to holding academic data or websites hostage for a ransom. Even if not all organizations have a lot of resources, it is still worthwhile to hack them if you can do it quickly.
- **An abundance of personally identifiable information:** Information can be found in great abundance in educational institutes of Higher education learning. They have significant student populations with recent credit histories, in addition to alumni and employee information. Universities and schools frequently retain a vast array of useful data, including loan and bank account information, social security numbers, passport data, and even medical data.
- **Valuable, confidential research:** Chinese hackers targeted twenty-seven universities, including the Massachusetts Institute of Technology and the University of Washington, according to the Wall Street Journal. The hackers sought material pertaining to maritime studies conducted by the United States military. In 2019, cyberespionage attacks on educational institutions have increased.

Institutions/Universities are targets for cyberattacks because they have a lot of computing power and allow public access. Visitors and researchers can share large amounts of data in addition to academics, staff, and students. Higher education requires openness and transparency, but intellectual property must be protected. Preventing knowledge loss in higher education requires understanding IT security threats. Universities are least cyber-secure, say experts. University security wasn't taught. Many universities train students and employees on IT security so they can use security lessons effectively. Attacks target 18-24-year-olds. Clicking on an email link can cause a cyberattack (Singar & Akhilesh, 2020). Lee (2020) stated universities are a tempting target for cyber attackers looking to steal intellectual property and cyber thieves looking to make quick cash. In higher education, thousands of people use personal, often unsecured, or unpatched devices like laptops and smartphones to access and store university data. This makes universities a tempting target. Many will be students with inadequate security knowledge and training, making them an easy target for social engineers. Some university employees will have access to sensitive research. Contact details and research interests of university staff members are easy to find on the university website, giving hackers everything, they need to build a personalized phishing attack.

Gabra et al. (2020) researched cyber security awareness in Nigerian universities and found that higher education institutions lacked cybersecurity courses, prompting university administration to act. 325 out of 367 students said there were no security officers on campus, and they lacked basic cybersecurity knowledge. Human error is the weakest link in network security, according to Shah & Agarwal (2020). Government and private internet service providers may run campaigns on gadget security. Programs should promote awareness and related skills. Cyber security awareness (CSA) is often ignored by educational institutions, and university students should be warned about online dangers. Therefore, students must develop a safety culture. Establish this culture early. Students should also know how to avoid cyber-attacks (Aljohani & Elfadil, 2020).

Monrad (2019) spotlighted that Lancaster University students fell victim to a phishing attack that sent fraudulent bills to applicants. 4,400 University of York students' information was breached. Data theft from universities could be used to commit fraud or steal intellectual property. With so many options, cyber-attacks against educational institutions of higher learning are increasing worldwide. It is critical for university leaders and administrators to evaluate whether their cyber security governance is adequate. Organizations that do not adequately protect themselves risk losing or exposing personal student and staff data as well as commercial, institutional, and research data that is valuable to domestic and international cyber criminals. Universities must maintain an open atmosphere because they are, by definition, welcoming places for people of all backgrounds. The need for transparency and safety must be carefully balanced. Universities frequently lack confidence in their cyber-security measures.

According to Kashiwazaki (2018), unauthorized accesses caused by phishing, weak passwords, brute force attacks, and so on, malware infections, and denial of service are among the cybersecurity issues affecting Japanese research and educational institutions. Security breach and malware attacks can both result in the disclosure of personal or confidential information. Among the entries were 36,623 unique email addresses, as well as tens of thousands of students, faculty, and staff names; thousands of usernames; hashed and plain-text passwords; addresses; phone numbers; and database schema information. Birth dates, citizenship, race, marital status, and gender were all deemed sensitive information. Senthilkumar & Eastwaramoorthy (2017) noted that cyber awareness helps students avoid cybercriminals. Therefore, students need more cyber awareness. Due to the valuable information on educational networks and the fact that threat actors could use network infrastructure to attack other targets, educational institutions will likely face cyber threats for the foreseeable future. According to FireEye (2016), university networks are hard to secure due to their size, number of users, and need for internal and external users to share information. Stolen educational data includes student records, grades, and test scores, business documents, employee evaluations, and financial documents. Research news, invoices, meeting minutes, program and initiative information, and a newsletter.

V. Significance of the Study

One of the most critical components of a top-notch higher education is frequently regarded as having access to the internet. The significance of online services in the context of the current learning and teaching environment cannot be emphasized. The higher education sector has been actively utilizing technology and information systems in both its on-campus and online instructional environments. This is being done to satisfy the needs of today's varied student population. Cyber-threats can undermine an organization's security. Threats to higher education abound. Because hackers may misuse student data, educational institutions must have strong security. Educational databases often contain student names, contact info, and email addresses. Academic progress, including projects and grades, enrolment, exams, and information on administration.

More than 90% of Indian firms consider cybersecurity awareness and education their main security concern, and 75% think it would be difficult to find cybersecurity personnel. This is despite escalating ransomware incidents, a lack of cybersecurity awareness in Indian boardrooms, and CEOs' unfounded beliefs that their institutions won't ever be attacked. 61% of Indian companies surveyed believe their board understands cybersecurity, 93% believe raising employee and leadership awareness and educating them about security will be their biggest challenge in the next 24 months, and 75% believe finding qualified cybersecurity professionals will be difficult (Jain 2020). Similarly, Nanda (2021) stresses that there have recently been more cybersecurity incidents. According to cybersecurity firm Barracuda Networks, more than 1,000 spear-phishing attacks targeted Indian educational institutions between July and September 2020. Because of a lack of awareness, limited funds, and scarce resources, higher education institutions and colleges are obvious targets for cyberattacks, which unfortunately makes attacks more potent. Meanwhile, in the aftermath of the COVID-19-imposed lockdown, India saw an increase in cyberattacks as well as a rapid adoption of digital services across the country. There were 1.16 million recorded cyberattacks in 2020, roughly three times as many as in 2019. According to the Indian Computer Emergency Response Team, 394,499, 1,158,208, and 607,220 cybersecurity events were recorded in 2019, 2020, and 2021, respectively (CERT). Every day in 2020, 3,137 cybersecurity-related concerns were reported.

Nanda (2021) outlined that as online learning becomes more common, India's top higher education regulator, the University Grants Commission (UGC), has urged colleges and universities to strengthen their cybersecurity and establish a cybersecurity ecosystem. The education sector deals with a lot of data on students, faculty, and other education-related parties, making it a prime target for cyber-frauds. It uses online payments heavily, making it a fraud target. Santosh (2020) asserts that stakeholders are key to the effective and efficient use of cyberspace in education. Each institution's principal or head should be aware of new technological trends to protect students and staff from cyber-dangers. Using technology ethically is a social responsibility.

Townsend (2021) outlined five factors that make schools and universities an attractive target for cybercriminals:

- **Institutions are not secure and reliable:** According to the Security Scorecards 2018, the education sector scored last overall for cybersecurity. Particularly for institutions with tight resources, investing in security has a cost.
- **Accessible Network and Software**: Institutional networks occupy a sizable amount of space and give staff and students access to a wide range of software and data. Institutions have largely focused on facilitating easy access for students and offering all the services necessary to keep their institution competitive with other academic institutions, but this also provides opportunities for cybercriminals.
- **Targets include students:** While businesses can invest in cyber-education and train their employees, schools constantly welcome new students, making it unfeasible to provide significant cyber-education. Young people frequently lack experience and are more vulnerable to conventional hacking approaches.
- **Bringing your own devices (BYOD):** Everyone uses their personal laptops, desktop computers, cell phones, and tablets to connect. Each gadget offers a chance.
- **Large, welcoming campuses:** When it comes to man-in-the-middle attacks, tailgating, or social engineering techniques, there is no richer environment than a college or university campus. Strangers can easily enter, sneak past security, and plant USBs, snoop on traffic, or penetrate labs and research spaces.

VI. OBJECTIVES OF THE STUDY

The purpose of the study is to increase knowledge and understanding among the faculty and students about online safety and strengthen a culture of security and its potential ramifications for probable cyberattacks, as well as to recommend changes about cybercrime and cybersecurity knowledge and understanding among educational stakeholders. The study also has the following objectives, which are as follows:

1. To find out the awareness level of cybersecurity among the faculty members of Assam Don Bosco University
2. To find out the awareness level of cybersecurity among the students at Assam Don Bosco University
3. To investigate the difference between mean scores of cybersecurity level in:
   (i) Male and Female faculties
   (ii) Science and Social Science faculties
4. To investigate the difference between mean scores of cybersecurity level in:
   (i) Male and Female students
   (ii) U.G and P.G students
   (iii) Science and Social Science students
5. To suggest recommendation for creating awareness about cybersecurity among the educational stakeholders of Assam Don Bosco University

VII. HYPOTHESES OF THE STUDY

1. There will be no significant difference between the mean scores of cybersecurity level of male and female faculties of Assam Don Bosco University
2. There will be no significant difference between the mean scores of cybersecurity level of science and social science faculties of Assam Don Bosco University
3. There will be no significant difference between the mean scores of cybersecurity level of male and female students at Assam Don Bosco University
4. There will be no significant difference between the mean scores of cybersecurity level of U.G and P.G students at Assam Don Bosco University
5. There will be no significant difference between the mean scores of cybersecurity level of science and social science students at Assam Don Bosco University

VIII. DELIMITATIONS OF THE STUDY

The present study has been delimited to:

1. Undergraduate and Post Graduate students of Social Sciences and Sciences stream.
2. Faculties of Social Sciences and Sciences stream.

IX. METHODOLOGY

Due to emerging nature of cybersecurity in higher education the descriptive-causal-normative survey approach is used to gather the information, which is desired from the respondents, who are rated on a Likert scale that has a range of five points. The respondents, their caregivers, the faculty members, and the administration of the university all gave their informed permission for the study, with the understanding that the respondents' personal information would indeed be treated with confidentiality and would only be used for this research study. This was done to eliminate any ethical concerns that could have arisen from the research.

Population of the study: The population of the study includes all faculty members and students at Assam Don Bosco University, Tapesia Campus, Guwahati-Assam, India.

Sample of the study: As shown in tables 1.2 and 1.3, a sample of 80 students (40 male and 40 female); 20 faculties (10 male and 10 female) from Assam Don Bosco University's Schools of Humanities & Social Science and Sciences were chosen for this study by adopting random sampling technique.

Table 1.1: *Represents the sample of students.*

Sr.no	Stream	Male	Female	Total
1	Social Science	20	20	40
2	Science	20	20	40
	Total	40	40	80

Table 1.2: *Represents the sample of faculty members.*

Sr.no	Stream	Male	Female	Total
1	Social Science	5	5	10
2	Science	5	5	10
	Total	10	10	20

Tools used: This survey was based on an online platform, namely Google forms. To ensure data confidentiality, and the results were stored in a local database for further analysis. During pre-processing, participants were asked if they agreed or disagreed with participating in the survey. If they agreed, they could access the questionnaire by logging in to Google forms using their Google accounts. They were allowed to submit their answers only one time. Following this phase, all responses were stored locally to process the data and further analyze the results using SPSS 23 (Statistical Package for Social Sciences).

Development of Scale: The research depended on the structured questionnaire as the main instruments for data collection. There are 38 items in the survey and the questionnaire comprised of three (3) sections such as: -

1. **Section 1:** Personal information which contained the gender, age group, department of the research sample.
2. **Section 2:** The survey questionnaire included on a close ended design on 5-point Likert scale as shown in table (1.3) which were used to measure the level of cybersecurity awareness level for both faculty members and students.
3. **Section 3:** The survey questionnaire included on a close ended design on 5-point Likert scale as shown in table (1.3) which were used to measure the roles of education and this section targets the students.

Table 1.3: *Scoring System*

Statement	Always/ Strongly Agree	Often/ Agree	Sometimes/ Undecided	Rarely/ Disagree	Never/ Strongly Disagree
Positive	5	4	3	2	1
Negative	1	2	3	4	5

Table 1.4: *Dimension – wise distribution of the statements*

Sr.no	Dimensions	Nature of Items	Item no.	Total Items.	Total
1	**Education related**	Positive	1,2,3,4,5,9,10,11,12	9	12
		Negative	6,7,8	3	
2	**Cybersecurity Awareness**	Positive	13,14,15,16,19,20,21,23,24,25,26,27,28,29	14	18
		Negative	17,18,22,30	4	
Total Items				38	

Positive Items =23. Negative Items =7.

Table 1.5: Norms of interpretation for CSA (Cyber Security Awareness)

Sr. no	Range of raw Score	Range of z-Score	Grade	Level of Cyber Security Awareness
1	180 and more	+2.01 & above	A	Extremely High
2	168-179	+1.26 to +2.00	B	High
3	157-167	+0.51 to +1.25	C	Above Average
4	140-156	-0.50 to +0.50	D	Average/ Moderate
5	129-139	-1.25 to -0.51	E	Below Average
6	117-128	-2.00 to -1.26	F	Low
7	116 and less	-2.01 & below	G	Extremely Low

First draft of the scale: This draft included 44 items that were created on two different aspects of cybersecurity awareness, namely, the level of cybersecurity awareness and the role that education plays in the process. Instructions for filling out the scale were included with it, and respondents were instructed to place a check mark next to each statement with which they agreed. This variation of the scale was prepared for preliminary testing. After conducting preliminary testing of the scale on the subjects and discussing the results with the experts, doing critical assessments of the items, and then removing 6 of the items from the scale, the scale was refined.

Final draft of the scale: A total of 38 items were selected to be filled out by 30 different students attending Assam Don Bosco University. Following the completion of the survey's items and their associated replies, an analysis of the cybersecurity scale was carried out. A total of 38 components and two dimensions were chosen to comprise the scale.

Standardization of the scale: At Assam Don Bosco University's Tapesia Campus in Assam, India, a sample of 30 students, including males and females, were asked to complete the final version of the Cybercrime awareness scale, which contained a total of 38 statements.

Reliability: For determining the reliability of the scale, the Cronbach's alpha approach was applied. To determining Cronbach's Alpha, a statistical analysis computer application known as SPSS 23 (Statistical Package for Social Sciences) was utilized. A value of 0.8 was determined to represent the reliability of the scale.

Validity: The content validity of the scale was determined based on the opinions of professionals from a variety of fields, including education, psychology, sociology, professionals in the information technology field, and advocates. For determining the content validity of this scale, it was administered to ten individuals who held very high levels of relevant expertise. Most of the experts were content with the aspects of the scale, which provided a sample coverage of the cybersecurity awareness scale among the students and faculty members of Assam Don Bosco University.

X. RESULTS AND DISCUSSION

Objective 1: to find out the awareness levels of cybersecurity awareness among the faculty members of Assam Don Bosco University

For achieving objective 1, the researcher formulated a cybersecurity awareness scale to access the level of awareness among Assam Don Bosco University faculty members, and the researchers used the following tables and figures:

Table 2.1: *Depicts the level of cybersecurity awareness for faculty members in terms of gender.*

Gender	Level of Cybersecurity Awareness					Total
	Above Average	Average	Below Average	High	Low	
Male	3 (15.0%)	2 (10.0%)	4 (20.0%)	0 (0.00%)	1 (5.0%)	10 (50.0%)
Female	4 (20.0%)	3 (15.0%)	0 (0.00%)	1 (5.0%)	2 (10.0%)	10 (50.0%)
Total	7 (35.0%)	5 (25.0%)	4 (20.0%)	1 (5.0%)	3 (15.0%)	20 (100%)

As per table 2.1 out of 20 (100%) respondents who were surveyed, 1 (5.0%) were deemed to have high degree of cybersecurity awareness, and 1 (5.0%) of those respondents were female. A total of 7 (35.0%) of 20 (100%) respondents were determined to have above-average levels of cybersecurity awareness, with 3 (15.0%) male and 4 (20.0%) female respondents. A maximum of 5 (25.0%) out of 20 (100%) respondents were determined to have average levels of cybersecurity knowledge, with 2 (10.0%) male and 3 (15.0%) female respondents. A total of 4 (20.0%) out of 20 (100%) respondents, had below average levels of awareness in terms of cybersecurity, with 4 (20.0%) of the respondents being male. A total of 3 (15.0%) out of 20 (100%) respondents had low levels of cybersecurity awareness, with 1 (5.0%) male and 2 (10.0%) female respondents as depicts in figure 2.1.

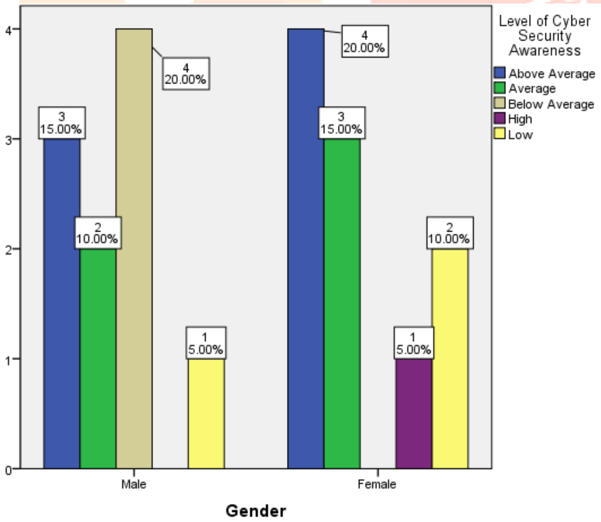

Figure 2.1: *Depicts the level of cybersecurity awareness among faculty members based on gender.*

Table 2.2: *Depicts the level of cybersecurity awareness for faculty members by stream.*

Stream	Level of Cybersecurity Awareness					Total
	Above Average	Average	Below Average	High	Low	
Social Science	5 (25.0%)	2 (10.0%)	2 (10.0%)	0 (0.0%)	1 (5.0%)	10 (50.0%)
Science	2 (10.0%)	3 (15.0%)	2 (10.0%)	1 (5.0%)	2 (10.0%)	10 (50.0%)
Total	7 (35.0%)	5 (25.0%)	4 (20.0%)	1 (5.0%)	3 (15.0%)	20 (100%)

According to table 2.2, a maximum of 1 (5.0%) out of 20 (100%) respondents were determined to have high levels of cybersecurity, with the respondent 1 (5.0%) from science having the highest levels. Out of 20 respondents, 7 (35.0%) had been found to have above-average cybersecurity knowledge, with 5 (25.0%) coming from the social sciences and 2 (10.0%) from the sciences. Out of 20 (100%) respondents, a total of 5 (25.0%) were found to have an average level of awareness regarding cybersecurity, with 2 (10.0%) coming from the Social Scientific field and 3 (15.0%) coming from the science field. Out of 20 (100%) respondents, 4 (20.0%) had below average level of cybersecurity awareness, with 2 (10.0%) came from Social Science and another 2 (10.0%) came from the Science field. The maximum number of respondents with a low degree of cybersecurity awareness was 3 (15.0%), out of a total of 20 (100%). Of these, 1 (5.0%) were from the social sciences, and 2 (10%) were from the science disciplines as depicts in figure 2.2.

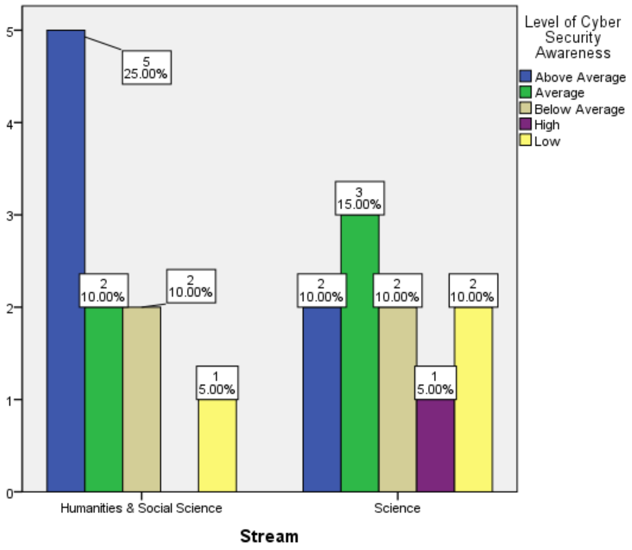

Figure 2.2: *Depicts the level of cybersecurity awareness among faculty members by streams.*

Objective 2: to find out the awareness levels of cybersecurity awareness among the students at Assam Don Bosco University
For achieving objective 2, the researcher formulated a cybersecurity awareness scale to access the level of awareness among Assam Don Bosco University students, and the researcher used the following tables and figures:

Table 3.1: *Depicts the level of cybersecurity awareness for students in terms of gender.*

Gender	**Level of Cybersecurity Awareness**							**Total**
	Above Average	**Average**	**Below Average**	**Extremely High**	**Extremely Low**	**High**	**Low**	
Male	11 (13.8%)	11 (13.8%)	11 (13.8%)	1 (1.3%)	1 (1.3%)	4 (5.0%)	1 (1.3%)	40 (50.0%)
Female	8 (10.0%)	23 (28.7%)	4 (5.0%)	0 (0.00%)	1 (1.3%)	2 (2.5%)	2 (2.5%)	40 (50.0%)
Total	19 (23.8%)	34 (42.5%)	15 (18.8%)	1 (1.3%)	2 (2.5%)	6 (7.5%)	3 (3.8%)	80 (100%)

As per table 3.1 out of 80 (100%) respondents, a total of 1 (1.3%) of the respondents displayed an exceptionally high level of cybersecurity awareness with the respondent being a male participant. A total of 6 (7.5%) of 80 (100%) respondents indicated a high level of cybersecurity awareness, with 4 (5.0%) male and 2 (2.5%) female respondents. A total of 19 (23.8%) out of 80 (100%) respondents had above average level of cybersecurity awareness, with 11 (13.8%) male and 8 (10.0%) female respondents. Out of 80 (100%) respondents, a total of 34 (42.5%) were assessed to have an average levels of cybersecurity awareness, with 11 (13.8%) male and 23 (28.7%) female respondents. A total of 15 (18.8%) out of 80 (100%) respondents were determined to have below average level of cybersecurity awareness, with 11 (13.8%) male and 4 (5.0%) female respondents. A total of 3 (3.8%) respondents out of 80 (100%) had a poor degree of cybersecurity knowledge, including 1 (1.3%) male and 2 (2.5%) female respondents. Out of 80 (100%) respondents, 1 (1.3%) exhibited extremely low cybersecurity awareness, with the respondent 1 (1.3%) being male as depicts in figure 3.1.

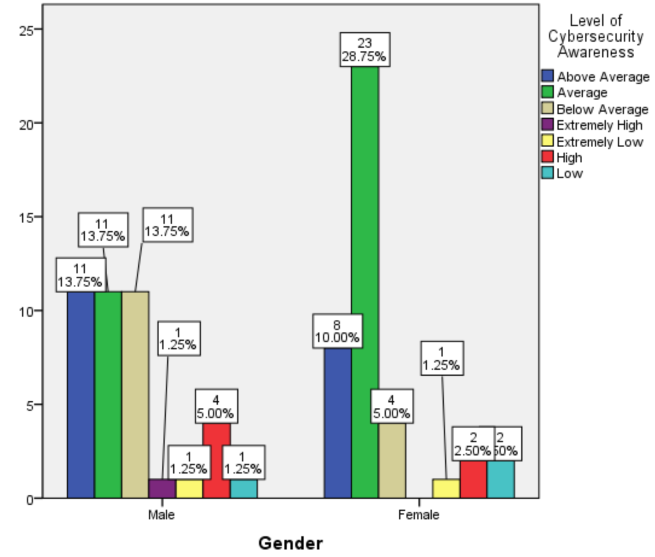

Figure 3.1: *Depicts the level of cybersecurity awareness for students in terms of gender.*

Table 3.2: *Depicts the level of cybersecurity awareness for students by stream.*

Stream	**Level of Cybersecurity Awareness**							**Total**
	Above Average	**Average**	**Below Average**	**Extremely High**	**Extremely Low**	**High**	**Low**	
Social science	8 (10.0%)	17 (21.3%)	8 (10.0%)	0 (0.00%)	2 (2.5%)	4 (5.0%)	1 (1.3%)	40 (50.0%)
Science	11 (13.8%)	17 (21.3%)	7 (8.8%)	1 (1.3%)	0 (0.00%)	2 (2.5%)	2 (3.8%)	40 (50.0%)
Total	19 (23.8%)	34 (42.5%)	15 (18.8%)	1 (1.3%)	2 (2.5%)	6 (7.5%)	3 (3.8%)	80 (100%)

As per table 3.2 out of 80 (100%), 1 (1.3%) of the respondent displayed exceptionally high level of cybersecurity awareness, with the respondent 1 (1.3%) being from the sciences stream. A total of 6 (7.5%) of the 80 (100%) respondents indicated high level of cybersecurity awareness, with 4 (5.0%) from social science and 2 (2.5%) from the sciences. Out of 80 (100%) respondents, 19 (23.8%) exhibited above average cybersecurity awareness, with 8 (10.0%) coming from social sciences and 11 (13.8%) coming from the sciences. A total of 34 (42.5%) out of 80 (100%) respondents, were assessed to have an average level of cybersecurity awareness, with 17(21.3%) from social sciences and another 17 (21.3%) are from science stream. Out of 80 (100%) respondents, a total of 15 (18.8%) had a below average level of cybersecurity awareness, with 8 (10.0%) were from social science and 7 (8.8%) were from sciences stream. A total of 3 (3.8%) out of 80 (100%) respondents, lack a strong understanding of cybersecurity awareness with 1 (1.3%) from social science and 2 (3.8%) were from science stream. Out of 80 (100%) respondents, a total of 2 (2.5%) exhibited extremely low cybersecurity awareness, with 2 (2.5%) from social sciences as depicts in figure 3.2.

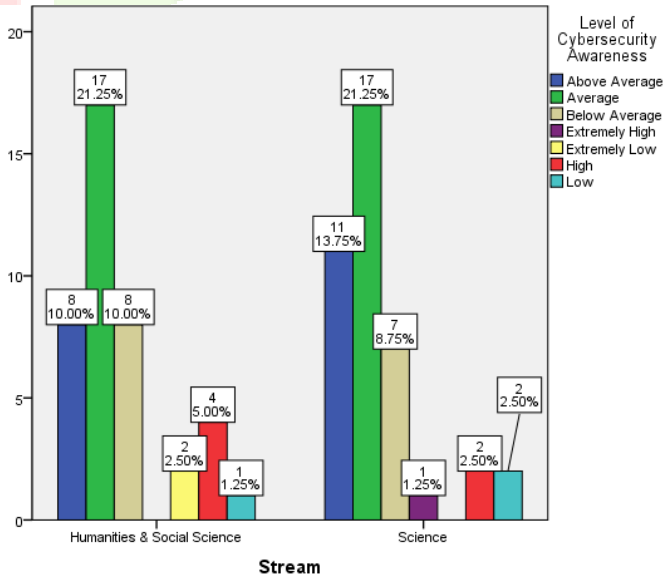

Figure 3.2: *Depicts the level of cybersecurity awareness for students by stream.*

Table 3.3: *Depicts the level of cybersecurity awareness for students in terms of qualification.*

Qualification	Level of Cybersecurity Awareness							Total
	Above Average	Average	Below Average	Extremely High	Extremely Low	High	Low	
U. G	13 (16.3%)	12 (15.0%)	8 (10.0%)	0 (0.00%)	2 (2.5%)	2 (2.5%)	3 (3.8%)	40 (50.0%)
P. G	6 (7.5%)	22 (27.5%)	7 (8.8%)	1 (1.3%)	0 (0.00%)	4 (5.0%)	0 (0.00%)	40 (50.0%)
Total	19 (23.8%)	34 (42.5%)	15 (18.8%)	1 (1.3%)	2 (2.5%)	6 (7.5%)	3 (3.8%)	80 (100%)

Table 3.3 depicts that out of 80 (100%) only 1 (1.3%) who is from U.G, has an extraordinarily high level of cybersecurity knowledge. 6 (7.5%) of the 80 (100%) respondents had a high degree of cybersecurity knowledge, including 2 (2.5%) from the U.G. and 4 (5.0%) from the P.G. A total of 19 (23.8%) out of 80 (100%) respondents, with 13 (16.3%) from the U.G. and 6 (7.5%) from the P.G., having higher than average cybersecurity knowledge. Out of 80 (100%) respondents, 34 (45.5%) had an average level of cybersecurity knowledge, with 12 (15.0%) coming from the U.G. and 22 (27.5%) from the P.G. 8 (10%) respondents from the U.G. and 7 (8.8%) from the P.G. are among the 15 respondents (18.8%) with below-average cybersecurity awareness. 3 (3.8%) out of 80 (100%) participants had low cybersecurity awareness, including 3 (3.8%) from the U.G. Of the 80 respondents (100%) who responded, 2 (2.5%) were determined to have a shockingly low degree of cybersecurity awareness as depicts in figure 3.3.

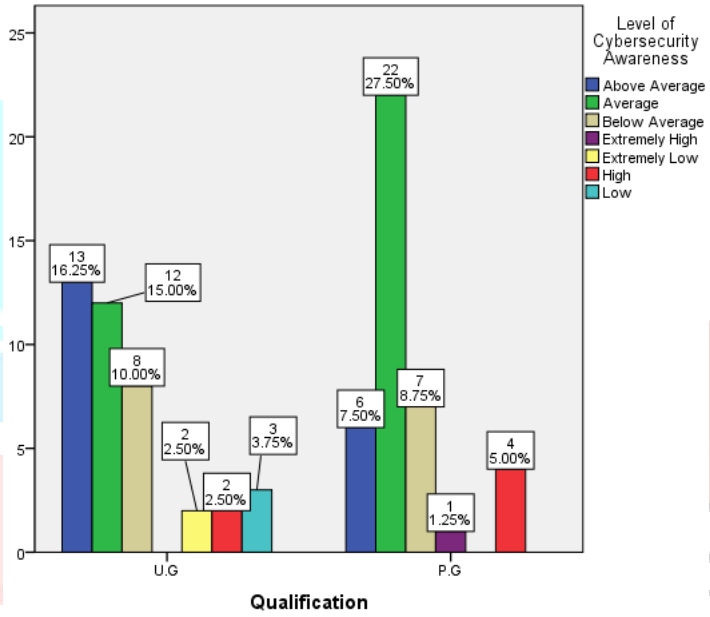

Figure 3.3: *Depicts the level of cybersecurity awareness for students in terms of qualification.*

Objective 3: To investigate the difference between mean scores of cybersecurity in:

1. **Male and Female Faculties**
2. **Science and Social Science Faculties**

The data obtained from the cybersecurity awareness scale presents a clear overview of the existing cybersecurity awareness among the faculty members and the data obtained from the sample of the faculties (20) and to make a comparison of the awareness towards cybercrime between the groups viz; male-female and Humanities & Social Science and Science, Independent ‘t’ test was applied to test the significance of the difference between the means as given in table 4.1.

Table 4.1: *t – ratio representation of groups*

Sr. no	Groups	N	Mean	Standard Deviation	‘t’ value	df	Level of Significance
1	Male	10	88.90	12.60	0.78	18	Not significant at 0.05 level
2	Female	10	93.50	13.55			
3	Social Science	10	93.70	12.16	0.85	18	Not significant at 0.05 level
4	Science	10	88.70	13.88			

The computed t-value was 0.78 for both male and female, with mean values of 88.90 and 93.50, respectively, which is not significant at the 0.05 level of significance for a df of 18, as shown in Table 4.1. Running an independent t-test requires the basic premise that two independents have equal variances. The p-value for the Levene's Test for Equality of Variances, which was run, was 0.84, suggesting that the assumption of equality of the two variances is true. As a result, the null hypothesis, which states that “There will not be a significant difference between the mean cybersecurity awareness scores of male and female faculty members of Assam Don Bosco University” is not disproved, showing that there is no relationship between gender and cybersecurity awareness. Additionally, the t-value between humanities, social sciences, and sciences was computed at 0.85 and had mean values of 93.70 and 88.70, respectively. This result is not significant at the 0.05 level of significance for df 18, as indicated by the results. It implies that there is no appreciable difference in cybersecurity awareness between Humanities & Social Science and Science. Considering this, the null hypothesis, "There will be no significant difference between the mean scores of cybersecurity level on science and social science faculty members of Assam Don Bosco University," is not disproved, demonstrating that stream-independent factors have no impact on cybersecurity awareness.

Objective 4: To investigate the difference between mean scores of cybersecurity in:

1. **Male and Female students**
2. **U.G and P.G students**
3. **Science and Social Science students**

The data obtained from the cybersecurity awareness scale presents a clear overview of the existing cybersecurity awareness among students, and the data obtained from the sample of students (80) and to make a comparison of the awareness towards cybersecurity between the groups viz; male-female and Humanities & Social Science and Science, Independent 't' test was applied to test the significance of the difference between the means, as shown in table 5.1

Table 5.1: *t – ratio representation of groups*

Sr. no	Groups	N	Mean	Standard Deviation	't' value	df	Level of Significance
1	Male	40	86.37	16.26	0.06	78	Not significant at 0.05 level
2	Female	40	84.97	13.58			
3	Social Science	40	83.67	16.57	0.33	78	Not significant at 0.05 level
4	Science	40	87.67	12.92			
5	U.G.	40	83.55	16.49	0.13	78	Not significant at 0.05 level
6	P.G.	40	87.80	12.98			

At the 0.05 level of significance for a degree of freedom (df) of 78, Table 5.1 display that the calculated t-value for both male and female was 0.06, with mean values of 86.37 and 84.97, respectively. This indicates that there is no appreciable variation in the level of cybersecurity knowledge between male and female students. The null hypothesis, "There will be no significant difference in the mean scores of cybersecurity awareness on male and female students at Assam Don Bosco University," is therefore not disproved, proving that gender has no bearing on cybersecurity awareness. Secondly, with mean scores of 83.67 and 87.67, respectively, the estimated t-value between Social Sciences and Sciences was 0.33, which is not significant at the 0.05 level of significance for df of 78. This indicates that there is no statistically significant difference in cybersecurity awareness between ADBU students majoring in social sciences and sciences. The null hypothesis "There will be no significant difference in the mean score of cybersecurity awareness on social sciences and sciences students at Assam Don Bosco University" is therefore not disproved, and stream has no impact on cybersecurity awareness. Lastly, for U.G. and P.G. students, whose mean scores were 83.55 and 87.80, respectively, the computed t-value was 0.13, which is not significant at the 0.05 threshold of significance for df of 78. The null hypothesis, "there will be no significant differences between the mean scores of cybersecurity awareness level on U.G. and P.G. students at Assam Don Bosco University," is not rejected as a result. This means that there is no discernible difference in cybersecurity awareness between ADBU's U.G. and P.G. students.

Objective 5: To suggest recommendation for creating awareness about cybersecurity among the educational stakeholders of Assam Don Bosco University

Major findings

This section highlights the major findings of this study, and 100% of the subjects were educated at Doctorate, postgraduate and undergraduate levels, giving the insights that even for educated people, their awareness background may vary.

In terms of Faculty Members of ADBU:

- 1 (1.5%) female respondent out of 20 (100%) was deemed to have a high level of cybersecurity awareness.
- In terms of cybersecurity awareness, the majority of respondents 12 (60.0%) of 20 (100%) fall between above average and average, with 5 (25.0%) male and 7 (35.0%) female faculties.
- In terms of cybersecurity awareness, 7 (35.0%) of 20 (100%) faculty members fell below average and low, with 5 (25.0%) male and 2 (10.0%) female faculties.
- There were no significant disparities in cybersecurity awareness levels between male and female faculty members at Assam Don Bosco University.
- 1 (1.5%) of 20 (100%) respondents from the sciences stream was determined to have a high level of cybersecurity awareness.
- In terms of cybersecurity awareness, the majority of respondents 12 (60.0%) out of 20 (100%) fall between above average and average, with 7 (35.0%) from the Social Sciences and 5 (25.0%) from the Sciences streams.
- In terms of cybersecurity awareness, 7 (35.0%) out of 20 (100%) fall below average and low, with 3 (15.0%) from the social sciences and 4 (20.0%) from the sciences stream.
- There were no significant differences in cybersecurity awareness levels between the social sciences and sciences faculties at Assam Don Bosco University.

In terms of Students of ADBU:

- It was discovered that the majority of the respondents, 34 (42.5%), have an average level of cybersecurity awareness, with 11 (13.8%) males and 23 (28.7%) females out of 80 (100%).
- A total of 15 (18.8%) out of 80 (100%) falls under below average level of cybersecurity awareness, with 11 (13.8%) male and 4 (5.0%) female.
- A maximum of 19 (23.8%) out of 80 (100%) falls under above average level of cybersecurity awareness, with 11 (13.8%) male and 8 (10.0%) females.
- There were no significant differences in cybersecurity awareness between male and female students at Assam Don Bosco University. This study supports the conclusions of Verma & Kushwaha (2021).
- It was found that out of 80 (100%), a maximum of 49 (61.2%) falls under average and below average, with 25 (31.2%) from the social sciences and 8 (10.0%) from the sciences stream.
- There were no significant differences in cybersecurity awareness between the Social Sciences and Sciences streams.

- A maximum of 44 (55%) of 80 (100%) respondents falls under average and below average with. 20 (25%) from U.G. and 29 (36.2%) from P.G.
- There was no significant difference in cybersecurity awareness between U.G and P.G students at Assam Don Bosco University.

Regard to Education:

- It was discovered that out of 80 (100%) respondents, 32 (40.0%) are unsure about cybersecurity and its roles, and 22 (27.5%) lack adequate knowledge about cybersecurity and its roles.
- It was discovered that majority of the Assam Don Bosco University students are unaware that the university organizes workshops, webinars, or training sessions for students on cybercrime and cybersecurity awareness, as 30 (37.5%) are unaware and 31 (38.7%) disagree that the university holds training programs, workshops regarding cyber safety programs.
- Out of 80 (100%) students who participated, 33 (41.25%) stated that cyber hygiene and cyber etiquettes, as well as their ethical roles, were not currently included in the university curriculum.
- It was observed that 57 (71.2%) of the 80 (100%) express that the current curriculum does not provide learners with cyber safety programs and security.
- It was also discovered that 63 (78.7%) of the 80 (100%) respondents believe their current curriculum does not emphasize the importance of cyber laws among their students.
- A maximum of 69 (86.2%) out of 80 (100%) respondents believe that cyber security and threats are undervalued in the curriculum.
- Maximum of 44 (55%) of 80 (100%) respondents are unfamiliar with university security measures and their roles in protecting university resources.
- A maximum of 55 (68.7%) out of 80 (100%) express that the present curriculum should include cyber safety programs, awareness and cyber security for faculties and learners.
- A maximum of 55 (68.7%) out of 80 (100%) believe that the existing curriculum ought to include cyber safety programs, awareness, and cyber security for both instructors and students.

XI. Suggestion and Recommendations

The descriptive findings provide crucial insights into how cybersecurity is viewed on campus; they point to a grasp of how important cybersecurity is, but also that responsibility for such countermeasures is inadequate.

- Cybersecurity threats are becoming a profitable profession. Institutions and universities should find ways to address security concerns while maintaining a networked environment to stimulate learning and secure academic research, faculty and student personal data, employees, and the institution's reputation. A successful security strategy necessitates the prioritization of various actions:
- Administrative polices and training are crucial:
  - Establish and ensure that all faculties and staff, and students have proper cybersecurity awareness.
  - Developing a strategy to implement if your system or devices is compromised by hackers or cybercriminals.
  - Creating backup of the essential data and practicing data recovery processes.
- Physical security is essential for ensuring a safe campus:
  - Protection of the system always, no matter wherever they are.
  - A sufficient level of control over the students accesses to facilities.
  - Access right to documents and paper records, so that there is no chance of theft.
- Create a safe culture: Protecting against human dangers and errors necessitates user education, which is a core security principle and essential for developing a strong security culture.
  - To fully benefit, the security culture and environment in which it operates must be supportive. Individuals who fear the consequences of falling prey to an attack are less likely to report, putting the entire organization in jeopardy because the blame game does not help anyone.
  - To effectively safeguard against social media attacks, organizations should adopt a social media strategy that prohibits employees from disclosing critical details about your organization on social media channels. Train employees to comprehend the risks mentioned on social media platforms to keep them safe at home and at work.
  - Remote working policies should include requirements for handling mobile devices while off-site, such as not leaving devices unattended, especially in public places, not storing devices in vehicles that are visible, using the safe provided by the hotel for example, and in any case, portable devices should be encrypted.
  - If it is impossible to avoid using a public Wi-Fi network, the next best choice is to connect to a virtual private network (VPN). A VPN allows you to securely connect to another network via the Internet, preventing anyone watching Wi-Fi traffic from obtaining the data you receive or send.
- At the university level, a variety of planned cyber safety programs, cybersecurity coursework, and projects can be covered. Which educates educators and students about the importance of cybersecurity. Since cybersecurity threats can come from any level of the organization, organization must include cybersecurity awareness training to educate about common and latest cybersecurity threats such as social engineering frauds, phishing, ransomware attack, cloud security, and BYOD (bring your own devices) and other rootkits intended to obtain intellectual assets or personal data.
  - Most educational institutions now offer an open Wi-Fi network in addition to BYOD (Bring your own Device) policies and regulations, which leads to students accessing hazardous sites that are often targeted by malware and viruses. Moreover, students store all their personal information's on phone, laptop, tablet connected to an open, hackable Wi- Fi Network.

  - Educational institutions are considered a breeding ground for password-related criminality, owing to the practice of using the same password and username/email for just about everything; millions of stolen and fabricated email details are sold on the dark web. Nidup (2021) emphasized that youths must be taught on security concerns and risk to ensure a safe online environment. If not, youngsters will keep utilizing the Internet and gadgets, exposing themselves to online threats and risks.
- To improve the service quality of higher education in mutually beneficial cooperation, it may be necessary to reevaluate the curriculum materials for both the social sciences and the sciences to incorporate topics such as cyber risk management, cyber leadership programs, and cyber mindfulness practices and according to Zhu et al. (2017), the digital wellbeing movement has also resulted in the development of cyber mindfulness applications that attempt to assist people in becoming mindful.
- In addition, it is essential to incorporate cyber ethics education for both students and faculty to build decent digital attitudes in the 21st century. Educational institutions should also have a cyber safe toll-free helpline for student teachers, parents, and the community at large to facilitate this. According to Berkowicz & Myers (2015), educators cannot prevent students from taking advantage of present and future technology outside the educational institution, but they may educate them on the legal and ethical ramifications of their conduct, as well as help educate parents and community leaders.
- Higher education institutions should also receive training, workshops, and seminars on themes such as cyber welfare, cyber etiquette, and cyber-hygiene. These activities should center on the institutions' subject material, with the purpose of encouraging the development of cognitive and psychological abilities connected to cybersecurity to enhance knowledge, morals, and qualities. Verma & Kushwaha (2021) stress the risk of becoming involved in a cyberattack. Enhancing one's understanding and integrating cyber ethics and cyber values in the curriculum, as well as regular awareness activities and cybercrime prevention initiatives, is critical.

XII. Conclusion

In today's highly technologically advanced world, as the movement grows more digitally savvy, so do the crimes. Cyber laws address all legal issues concerning cybercrime. Cybercrime has now become a normal sight, and we can easily become victims of criminal cyber activity in a wide range of ways. As the Indian government enacted the "Information Technology Act, 2000" to prevent acts that infringe internet users' rights. To reduce the crime rate, it is critical to apply successful preventive approaches in all target groups and to make students more aware of current cyber laws and regulations. The formation of a university level cybersecurity curriculum is being stymied by university culture and ideals, as well as our ignorance, and reform is required on all fronts; the failure of a faculty opens the door for others who will take its place (Schneider, 2013), The protection of their students and faculties from cyber threats and its ethical use is a societal obligation that requires the institution's principal or head to be more extremely wary evolving technological developments. According to Chapman (2019), organizations that do not adequately protect themselves risk the loss or exposure of personal student and staff data and commercial, institutional, and research data that is valuable to cyber criminals operating both nationally and internationally. University leaders need to consider whether their cyber protection governance is adequate, and the increasing risk of cyber threat should be well reported. Thapaliya (2019) Although cons and frauds are so convincing and the perpetrators are hard to find, we must always remain vigilant. E-learning is now part of the educational system, it is important to promote knowledge about online crime, attacks, and threats, and potential countermeasures.

References

Aljohani, W., & Elfadil, N. (2020). Measuring Cybersecurity Awareness of Students: A Case Study at Fahad Bin Sultan University. *International Journal of Computer Science and Mobile Computing*, 9(6), 141–155.

Al-Khatib, A., & Teixeira da Silva, J. A. (2017). What rights do authors have? *Science and Engineering Ethics*, 23(3), 947–949. https://doi.org/10.1007/s11948-016-9808-8

Berkowicz, J., & Myers, A. (2015, November 12). Teaching Students Cyber Ethics. *Education Week*. https://www.edweek.org/leadership/opinion-teaching-students-cyber-ethics/2015/11

Calder, A. (2020). *The cyber security handbook–Prepare for, respond to, and recover from cyber-attacks*. IT Governance Publishing Ltd.

Chapman, J. (2019). *How safe is your data? Cyber-security in higher education*. Hepi.ac.uk. https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf

Clemons, M., de Costa e Silva, M., Joy, A. A., Cobey, K. D., Mazzarello, S., Stober, C., & Hutton, B. (2017). Predatory invitations from journals: More than just a nuisance? *The Oncologist*, 22(2), 236–240. https://doi.org/10.1634/theoncologist.2016-0371

Dadkhah, M., Borchardt, G., & Maliszewski, T. (2016). Fraud in academic publishing: Researchers under cyber-attacks. *The American Journal of Medicine*, 130(1), 27–30. https://doi.org/10.1016/j.amjmed.2016.08.030

FireEye. (2016). Cyber Threat to the Education Industry. Fireeye.Com. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-education.pdf

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. https://doi.org/10.31580/sps.v2i1.1320

Jain, S. (2022, April 22). *Cybersecurity awareness, education dismal in Indian boardrooms*. Forbes India. https://www.forbesindia.com/article/news-by-numbers/cybersecurity-awareness-education-dismal-in-indian-boardrooms/75617/1

Jain, S. (2022, April 22). *Cybersecurity awareness, education dismal in Indian boardrooms*. Forbes India. https://www.forbesindia.com/article/news-by-numbers/cybersecurity-awareness-education-dismal-in-indian-boardrooms/75617/1

Kashiwazaki, H. (2018). Personal information leak in a university, and its clean up. *Proceedings of the 2018 ACM SIGUCCS Annual Conference, 43–50.*

Kozak, M., Iefremova, O., & Hartley, J. (2016). Spamming in scholarly publishing: A case study. *Journal of the Association for Information Science and Technology*, 67(8), 2009–2015. https://doi.org/10.1002/asi.23521

Kulkarni, P., & Akhilesh, K. B. (2020). Role of cyber security in public services. *In Smart Technologies* (pp. 67–77). Springer Singapore.

Lee, J. (2020, October 30). *Security Threats Facing Universities*. Info security Magazine. https://www.infosecurity-magazine.com/opinions/security-threats-universities/

Mazzarello, S., Fralick, M., & Clemons, M. (2016). A simple approach for eliminating spam. *Current Oncology (Toronto, Ont.)*, 23(1), 75–76. https://doi.org/10.3747/co.23.2860

McEvatt, P. (2016, July 7). *Aspects to consider in further education security*. Info security Magazine. https://www.infosecurity-magazine.com/opinions/why-education-institutions/

Monrad, J. (2019, August 27). *Universities fall into the cross hairs of cyber attackers*. Info security Magazine. https://www.infosecurity-magazine.com/opinions/universities-attackers/

Nanda, P. K. (2021, August 30). *UGC asks colleges to boost cybersecurity*. Mint. https://www.livemint.com/education/news/ugc-asks-colleges-to-boost-cybersecurity-11630263851159.html

Newman, T., Beetham, H., & Knight, S. (2018). Digital experience insights survey 2018: Findings from students in UK further and higher education. Bristol: Jisc.

Nidup, Y. (2021). Awareness about the online security threat and ways to secure the youths. *Journal of Cyber Security*, 3(3), 133–148. https://doi.org/10.32604/jcs.2021.024136

Pignata, S., Lushington, K., Sloan, J., & Buchanan, F. (2015). Employees' perceptions of email communication, volume and management strategies in an Australian university. *Journal of Higher Education Policy and Management*, 37(2), 159–171. https://doi.org/10.1080/1360080x.2015.1019121

Santhosh, T. (2022, August 03). RE-ENVISAGING CYBER SAFETY PROTOCOL IN SCHOOLS IN KERALA. Retrieved from https://www.academia.edu/45180324/RE_ENVISAGING_CYBER_SAFETY_PROTOCOL_IN_SCHOOLS_IN_KERALA_Research_Poster_36_x_60_C_.

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, 263(4), 042043. https://doi.org/10.1088/1757-899X/263/4/042043

Singar, A. V., & Akhilesh, K. B. (2020). Role of cyber-security in higher education. *In Smart Technologies* (pp. 249–264). Springer Singapore.

Spinello, R. A. (1999). Ethical reflections on the problem of spam. *Ethics and Information Technology*, 1(3), 185–191. https://doi.org/10.1023/a:1010064007816

Steinberg, J. (2022). *Cybersecurity For Dummies*, 2nd Edition. John Wiley & Sons.

Teixeira da Silva, J. A., Al-Khatib, A., & Tsigaris, P. (2020). Spam emails in academia: issues and costs. *Scientometrics*, 122(2), 1171–1188. https://doi.org/10.1007/s11192-019-03315-5

Thapaliya, S. (2021, June 17). *Cognizing scams and frauds in Cyber Space and its preventive measures*. Linkedin.com. https://www.linkedin.com/pulse/cognizing-scams-frauds-cyber-space-its-preventive-suman-thapaliya/

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

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. https://doi.org/10.3390/fi13020039

Wilkinson, T. A., Russell, C. J., Bennett, W. E., Cheng, E. R., & Carroll, A. E. (2019). A cross-sectional study of predatory publishing emails received by career development grant awardees. *BMJ Open*, 9(5), e027928. https://doi.org/10.1136/bmjopen-2018-027928

Zhu, B., Hedman, A., & Li, H. (2017). Designing digital mindfulness: Presence-in and presence-with versus presence-through. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*.