JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FACULTY AND STUDENTS OF ASSAM DON BOSCO UNIVERSITY, GUWAHATI ON CYBERCRIME AND EDUCATION

[1]Henry V.L Nghilhlova Zote, [2]Dr. Tania S. Roy

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

Abstract: *This study examined the level of cybercrime awareness among the faculty members and students at Assam Don Bosco University. Descriptive cum normative survey was adopted to obtain data from 20 faculty members and 80 students from both schools of Social Sciences and Sciences. Results display that half of the faculty members out of 20 respondents were found to have a below-average level of cybercrime knowledge and out of 80 students 53 fall under average and below-average level of cybercrime awareness. Moreover, students claimed to have basic cybercrime knowledge but are not well informed of how to protect themselves from cyber threats and universities do not have an active cybercrime and safety awareness program to improve students' knowledge on how to protect themselves from any threats. the significance of increasing awareness by providing effective solutions for reducing the risk of becoming entangled in cybercrime is vital and the need to consider cyber-ethics and cyber-values in the curriculum, and frequent awareness sessions on cybercrime preventive strategies are needed at academic institutions to make students and faculties aware of the latest cyber threats and changes. Students and faculties can be aware by organizing workshops, seminars, conferences, etc. The present paper is therefore an effort to understand the role of education and its awareness regarding the preventive measures taken against cybercrime. The researcher has tried to bring into light the significance and relevant perspectives regarding the approach towards cybercrimes in the present era.*

Index Terms **– Cyber-crime, Digital crime, Awareness, Adolescent, Curriculum, Higher Education.**

I. INTRODUCTION

The Internet is a global computer network that enables governments, businesses, organizations, and individuals to conduct global economic, social, and informational activities. Social researchers have defined and used multiple metaphors to describe the information age, including Post-industrial society, Information society, Network society, Cyber-society. According to O'Dea (2021), China will have more smartphone users than any other country in the world in 2021, with nearly 912 million, and India will have the second most smartphone users, with both countries expected to continue to lead the smartphone user ranking. Bhati & Bansal (2019) pointed out the fact that internet usage has shifted heavily to applications and websites, and social media has grown from a simple chat room for a group of people to millions of users active all over the world, with a variety of social media applications and the majority of active users being youths. Likewise, several studies have shown that computers are no longer the only way to access 'Cyberspace'. Furthermore, Mesko (2018) examines the causes of cybercrime and its consequences for the physical environment (particularly on cyberspace users). This new branch of criminology is based on the following fundamental assumptions, which Jaishankar (2007) refers to as 'Space Transition Theory,' which are detailed below:

(i) Individuals who suppress their proclivity for criminal activity in their physical setting are more likely to engage in deviant behaviour in virtual worlds.

(ii) Individuals can commit criminal offences in cyberspace due to the flexibility of their identity, anonymity, and a lack of deterrent factors.

(iii) Criminality has spread from the physical to the virtual worlds. Due to the characteristics of cyberspace, perpetrators can easily flee/hide.

(iv) Individuals who commit crimes in their physical setting recurrently form groups in cyberspace. "Acquaintances" frequently form cybercrime groups.

(v) Individuals from closed societies are more prone to crime in cyberspace.

(vi) Conflicts between norms and values in the physical setting and norms and values in cyberspace frequently lead to cybercrime.

The number of hackers and organized cybercrime groups has steadily increased, and these cybercriminals have been adopting new methods to carry out cybercrime, with the primary motivation for hacking being financial gain obtained by stealing information and retaining it all for compensation. Cybercriminals can also monetize secret data to competitors on the dark web, making cyberspace unsafe and posing significant risks to businesses and their customers (Alharbi & Tassaddiq, 2021). Furthermore, the global increase in cybersecurity incidents is primarily due to most people failing to strictly adhere to the exact security rules and instructions provided at the workplace. People are the weakest link in an organization's cybersecurity, making it vulnerable to both external and internal actors. As a result, cybersecurity should be initiated across the board, not just in the IT department (Whitman & Mattord, 2012; Green, 2016).

Cybercrime/ Digital Crime: Holt & Bossler (2020) spotlighted concepts related to cybercrime as shown in table 1.1

Table 1.1: *Concepts related to Cybercrime*

List	Why it was Introduced	Limitations	Sources
Computer Crime	Researchers, academics, and policymakers acknowledged that new computer-related behaviours resulted in criminal acts.	Crimes that were previously limited to computers can now be committed without the use of a computer by utilising other technological devices as technology advances and the number of devices connected to the Internet grows.	Hollinger & Lanzakaduce (1988) Richardson (2008)
Digital Crime	Researchers and practitioners, particularly forensics experts, recognised that crimes could be committed using digital technologies whether a computer is used.	The phrase may limit the types of offences that can be included to those that require a level of computer sophistication that is not required for the majority of computer offences.	Gogolin (2010) Kanellis (2006) Taylor et al, (2014)
Electronic Crime	Researchers' language was used to capture communication strategies (e.g., email) that were like computer uses.	As society has evolved, the term "electronic" has fallen out of favour, with many young people now avoiding electronic mail.	Etter (2001) Grabosky (2006)
Internet Crime	Other phrases inferred a level of expertise to commit the offences, even though many offences were simply committed 'via' or 'on' the Internet.	The phrase could be interpreted to exclude crimes committed without the use of the Internet but motivated by cyber technology.	Jewkes & Yar (2010) Taylor & Quayle (2003) Wall (2013)
Network Crime	The authors (particularly the engineers) wished to emphasise the fact that crime occurs via the network that connects various technological devices.	Many cybercrimes occur that have little to do with computer networks and more to do with computer users' behaviour.	Wang (2012)
Techno Crime	The authors were emphasising the connection between technology and crime, particularly in the workplace.	The term implies that the crime occurs as a result of technology, despite the fact that the majority of cyber offences are motivated by human factors.	Friedrichs (2009) Lema-Langois (2008) Steinmetz & Nobles (2017)
Virtual Crime	Courts have considered whether crime can be committed in the virtual world, including game settings.	While some crimes may be committed in the virtual world, they are the exception.	Brenner (2001b) Lastowka & Hunter (2004)

The Australian Crime Commission (now the Australian Criminal Intelligence Commission) lists a variety of traditional crimes as well as their cybercrime counterparts ('Cyber and technology-enabled crime,' 2013, p. 2). Cited by Martellozzo & Jane (2017) these are some indications:

(i) Theft (the cybercrime equivalents being online fraud, and mass-marketed fraud including auction fraud, advance fee fraud, and phishing).

(ii) Burglary and malicious harm (including online hacking, denial of service attacks, and viruses); child sex offenses (online grooming, child pornography websites).

(iii) Money laundering (through online payment systems and e-cash). Stealing (identity theft, bank website phishing, and movie, music, and software piracy).

(iv) (Stalking, bullying, and domestic violence have all evolved into distinct online versions, as have various forms of technology-facilitated and technology-amplified abuse, harassment, and coercion.

II. REVIEW OF THE RELATED LITERATURE

According to Verma & Kushwaha (2021), the significance of increasing awareness by providing effective solutions for reducing the risk of becoming entangled in cybercrime is the need to consider cyber-ethics and cyber-values in the curriculum, and frequent awareness sessions and cybercrime preventive strategies are needed at academic institutions and in societies to make learners and young folk aware of the latest cyber threats and changes. The Internet provides people with an almost limitless number of social events. People can interact with others in the virtual world through social media applications. However, the Internet and these technologies were not designed with security in mind, and the evolution of the Internet has also created significant threats for users. B. Bullying, for example, has long been a cause of concern for adolescents, children, parents, and educational leaders; nevertheless, the rise of cyberbullying has propelled these issues to the top of the list of priorities for policymakers. Another example is child pornography, Millions of child pornography images are now available on the Internet, and even if law enforcement shuts down a pornography website, the images have already been shared with millions of people and will remain online indefinitely (Kremling & Parker, 2017). Research shows that etiquette norms are just as important on the internet as they are in the real world, and bad netiquette (online or internet etiquette) can follow you for a long time. Likewise, Ariola, et al. (2018) recommended introducing a cybercrime education intervention to all courses or departments in academic systems, and that it is the educational institutions' responsibility to improve education about cybercrime, cyber-ethics, and computer security for learners to understand the positive and negative effects of using the internet.

Choudhary's (2020) study on 'Cybercrime awareness among higher education students from Haryana with respect to various demographic variables' discovered that cybercrime is affected by stream, and professional students are found to be more aware than their counterparts. The study also found that male and female cybercrime awareness is the same, implying that we can reduce these crimes through some guidelines and proper preventive measures, and educational institutions and the government have a critical role to play in adhering to some guidelines related to cybercrime and cyber security through seminars, workshops, and awareness programs at any level.

Punia & Phor (2019) stated that cybercrime awareness and internet addiction among students is a source of concern not only for parents and teachers, but also for the government, and that the youth of the country are the most powerful generation, so it is our responsibility to guide them toward a better life. Youth who are addicted to the internet spend most of their time engaging in illegal cyber-space activities. Organizations and individuals can strive to reduce or prevent cybercrime. Previous Study on ‘Awareness of Cybercrime among teachers’ trainees in Addalaichenai Government teacher’s college’ by Jazeel (2018) found most teacher trainees have a low level of awareness about cybercrime, indicating the need for workshops and seminars to be included in the curriculum to educate students about cybercrime and cyber security. Awareness about cybercrime and cyber security is important because it educates students in various aspects of life.

Senthilkumar & Easwaramoorthy (2017) conducted a survey in major cities of Tamil Nadu on internet safety among college students and discovered that college students have an above-average awareness of cyber-related threat issues that can help them protect themselves from cyber-attacks and pointed out that cyber awareness will nurture the students to protect themselves from hackers and cyber-attacks and that more awareness needs to be implemented. Similarly, Zayid & Farah (2017) did a study on cyber risk with 132 students enrolled in Saudi Arabia's Southern district of Alnamas and discovered that 15% of the participants had experienced a cybercrime, 80.7% were interested in obtaining training to enhance their knowledge, and 69.6% of cybercrimes occurred through digital networking, with 57% of them being sexual in nature.

According to the technological deterministic viewpoint, the internet is a transformative force with far-reaching consequences for children and youth, as technology creates new patterns of expression, communication, and motivation. This viewpoint has been labelled "The Net – Generation," "The Millennium Generation," and "Digital Natives." (Tapscott, 1998; Prensky, 2001). Many city centres, public places, schools, universities, cafes, shopping malls, and entertainment venues offer Wi-Fi or hotspot services to laptop or notebook users. There are, however, several cell phones include Internet access. Internet-based activities are no longer novel in today's information society, with pre-schoolers, parents, businessmen, organisations, and employees, as well as homemakers, using the internet (Umanailo & Fachruddin et al., 2019; Anderson et al.,2013).

III. SIGNIFICANCE OF THE STUDY

Cybercrime knows no borders and evolves as quickly as new technologies, and a lack of awareness about cyber hygiene is a significant barrier to combating the crime (Keelery, 2021). Every year, an increasing number of cybercrimes are reported across the nation. The crimes, on the other hand, ranged from minor online deception to lottery scams and sexual harassment. In 2020, over 50,000 cybercrime incidents were reported in India, with Karnataka and Uttar Pradesh accounting for the lion's share. Keelery (2021) also mentions over 10,000 cases of cyber stalking and bullying in India, which are covered by IPC sections 420, 465, 468, and 471 (Indian Penal Code). Karnataka had the highest number of registered online identity theft offences, with over 3000 cases reported to authorities. Over 5000 cases of online identity theft were reported in India in 2020, and the crime was covered by Section 66C of the Indian Penal Code (Indian Penal Code). In 2020, there were over four thousand cases of online banking fraud reported across India, representing a significant increase in the number of reported cases. Another worrying trend is that in India, over 3.2 thousand cases of cyber-crime involving sexual harassment or exploitation were reported in 2020. Even though from 2018 to 2020, the country's crime rate increased. As a result, more research into students’ cyber awareness is required, to avoid becoming a victim of cybercrime, everyone must be aware of their own security and safety countermeasures, including instructors and educational stakeholders. As Verma & Kushwaha (2021) stated, there is a need to establish cyber security courses that include cyber hygiene, cyber etiquette, software security, networking fundamentals, basic system administration, and cybercrime detection in text-based communications. Academic institutions must prepare students for their professional fields of study, but student awareness of digital technologies and cyber security issues is dwindling. To avoid becoming a victim of cybercrime, it is necessary to teach cyber security topics. Although we cannot eliminate cyber-threats from cyberspace, we may be able to keep these threats under control.

IV. 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 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 cybercrime among the faculty members of Assam Don Bosco University
2. To find out the awareness level of cybercrime among the students at Assam Don Bosco University
3. To investigate the difference between mean scores of cybercrime level in:
   (i) Male and Female faculties
   (ii) Science and Social Science faculties
4. To investigate the difference between mean scores of cybercrime 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 cybercrime among the educational stakeholders of Assam Don Bosco University

V. HYPOTHESES

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

VI. 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.
3. The study is restricted to Tapesia campus alone.
4. The investigator selected only 100 sample.

VII. METHODOLOGY

Due to emerging nature of cybercrimes 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 1.2: *Represents the sample of students*

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

Table 1.3: *Represents the sample of faculty members*

Sl.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 dis-agreed 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 49 items in the survey and the questionnaire comprised of four (4) 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 (1.4) which were used to measure cybercrime victimization among the students.
3. Section 3: The survey questionnaire included on a close ended design on 5-point Likert scale as shown in table (1.4) which were used to measure the level of cybercrime awareness level for both faculty members and students.
4. Section 4: The survey questionnaire included on a close ended design on 5-point Likert scale as shown in table (1.4) which were used to measure the roles of education and this section targets the students.

Table 1.4: *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 1.5: *Dimension – wise distribution of the statements*

Sl.no	Dimensions	Nature of Items	Item no.	Total Items.	Total
1	Online Victimization	Positive	1,3,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19	17	19
		Negative	2,4	2	
2	Cybercrime Awareness	Positive	20,21,22,23,24,25,26,28,29,31,32,33,34,35,36,37	16	18
		Negative	27,30	2	
3	Education related	Positive	38,39,40,41,42,46,47,48,49	9	12
		Negative	43,44,45	3	
	Total Items				49

Positive Items =42. Negative Items =7.

First draft of the scale: This draft contained 75 items prepared on three dimensions of cybercrime awareness i.e., online victimization, cybercrime awareness and role of education. For filling up the scale instructions were given with it, while the respondents were required to put check mark for each statement to which they agreed. This form of scale was ready for pre-try out. After pre-try out of the scale on the subjects the response was discussed with the experts and critically analyses of the items were done and 26 items were eliminated from the scale.

Final draft of the scale: A total of 49 items were selected and was filled by 30 students from Assam Don Bosco University. After collecting the responses of the scale items analysis of the cybercrime awareness scale was done. Finally, a total of 49 items were selected for the scale along with 3 dimensions.

Standardization of the scale: The final form of the Cybercrime awareness scale with 49 statements was administered on a sample of 30 students, males and females taken up from Assam Don Bosco University, Tapesia Campus, Assam, India.

Reliability: The Cronbach's alpha method was used to find out the reliability of the scale. A statistical analysis computer programme SPSS 23 (Statistical package for Social Sciences) was used to calculate the Cronbach's Alpha. The reliability of the scale was found to be 0.8.

Validity: The Content validity of the scale was determined based on the opinions of the experts of different fields i.e., Education, Psychologist, Sociologist, Counsellor, and Advocates. This scale was given to 10 highly qualified experts to find out the content validity of the scale. Majority of the experts were satisfied regarding the items of the scale, providing sample coverage regarding the cybercrime awareness scale among the students and faculty members of Assam Don Bosco University.

Table 1.6: *Norms of interpretation for CCAS (Cybercrime Awareness Scale)*

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

VIII. RESULTS AND FINDINGS

Objective 1: To find out the awareness level of cybercrime among the faculty members of Assam Don Bosco University

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

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

Gender	Level of Cyber Crime Awareness				Total
	Above Average	Average	Below Average	High	
Male	1 (5 %)	2 (10 %)	5 (25 %)	2 (10 %)	10 (50 %)
Female	2 (10 %)	1 (5 %)	5 (25 %)	2 (10 %)	10 (50 %)
Total	3 (15 %)	3 (15 %)	10 (50 %)	4 (20 %)	20 (100 %)

As per table 2.1 a total of 4 (20%) of 20 (100%) respondents were found to have a high level of awareness in terms of cybercrime, with 2 (10%) being male and 2 (10%) being female. A total of 3 (15%) of 20 (100%) respondents were found to have an above-average level of awareness of cybercrime, with 1 (5%) male and 2 (10%) female respondents. A total of 3 (15%) respondents out of 20 (100%) respondents were found to have average levels of cybercrime awareness, with 2 (10%) male respondents and 1 (5%) female respondent. A total of 10 (50%) out of 20 (100%) respondents were found to have below-average levels of awareness in terms of cybercrime, with 5 (25%) males and 5 (25%) females as depicts in fig 2.1.

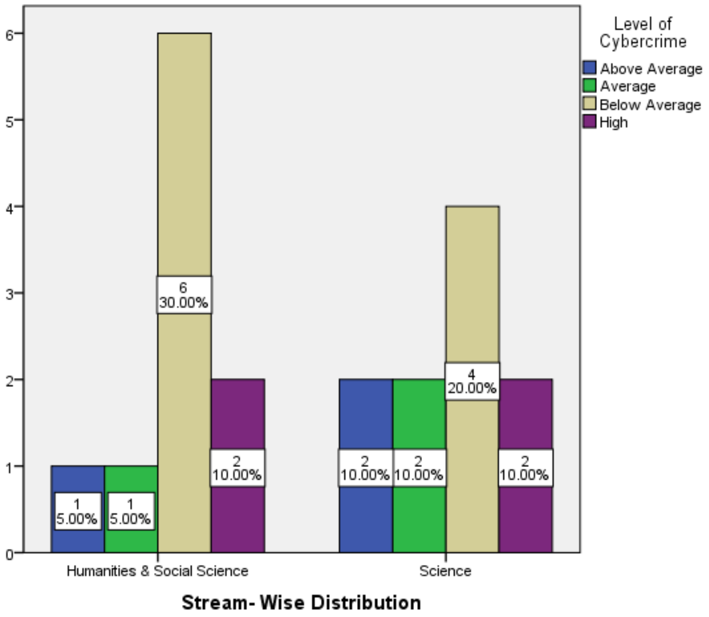

Figure 2.1: *Depicts the level of awareness of cybercrime among faculty members based on gender*

Table 2.2: *Depicts the level of cybercrime awareness among faculty members by stream*

Stream	Level of Cyber Crime Awareness				Total
	Above Average	Average	Below Average	High	
Social Science	1 (5 %)	1 (5 %)	6 (30 %)	2 (10 %)	10 (50 %)
Science	2 (10 %)	2 (10 %)	4 (20 %)	2 (10 %)	10 (50 %)
Total	3 (15 %)	3 (15 %)	10 (50 %)	4 (20 %)	20 (100 %)

As per table 2.2 a total of 4 (20%) respondents out of 20 (100%) were found to have a high level of awareness of cybercrime, with 2 (10%) respondents from social science and 2 (10%) respondents from science. A total of 3 (15%) of 20 (100%) respondents were found to have above-average awareness of cybercrime, with 1 (5%) responding from Social Science and 2 (10%) responding from science. A total of 3 (15%) respondents were found to have an average level of awareness regarding cybercrime, with 1 (5%) from the social science and 2 (10%) from science. A total of 10 (50%) respondents out of 20 (100%) were found to be below average in terms of cybercrime awareness, with 6 (30%) participants from humanities and 4 (20%) participants from sciences as depicts in fig 2.2.

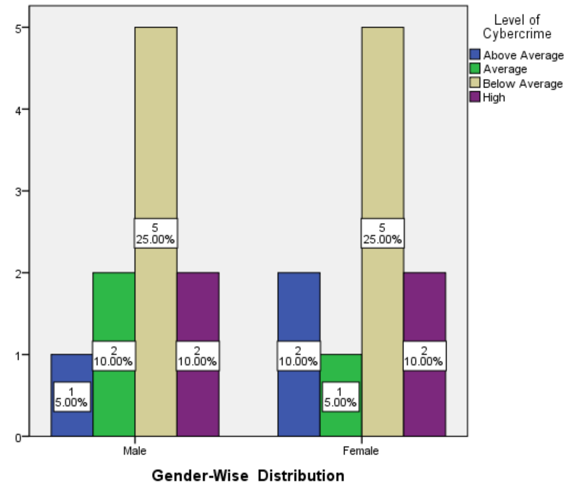

Figure 2.2: *Depicts the level of cybercrime awareness among faculty members by stream*

Objective 2: To find out the awareness level of cybercrime among the students at Assam Don Bosco University

For achieving objective 2, the researchers formulated a cybercrime awareness scale to assess 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 awareness of cybercrime among students based on gender*

Gender	Level of Cyber Crime Awareness					Total
	Above Average	Average	Below Average	High	Low	
Male	7 (8 %)	13 (16.3 %)	14 (6.3 %)	5 (6.3 %)	1 (1.3 %)	40 (50 %)
Female	6 (7 %)	12 (15 %)	13 (16 %)	9 (11 %)	0 (0 %)	40 (50 %)
Total	13 (16 %)	25 (31 %)	27 (33 %)	14 (17 %)	1 (1.3 %)	80 (100 %)

As per table 3.1 a total of 14 (17%) of 80 (100%) respondents demonstrated a high level of cybercrime awareness, with 9 (11%) female respondents and 5 (6.3%) male respondents. A total of 13 (16%) out of 80 (100%) respondents were found to have above-average awareness of cybercrime, with 7 (8%) males and 6 (16%) females. A total of 25 (31%) respondents were found to have an average level of cybercrime awareness, with 13 (16.3%) males and 12 (15%) females. A total of 27 (33% of respondents) were found to have a lower-than-average level of awareness of cybercrime, with 14 (17%) males and 13 (16.3%) females. A total of 1 (1.3%) respondent with low cybercrime awareness was identified, with 1 male respondent out of 80 (100%) as depicts in fig 3.1.

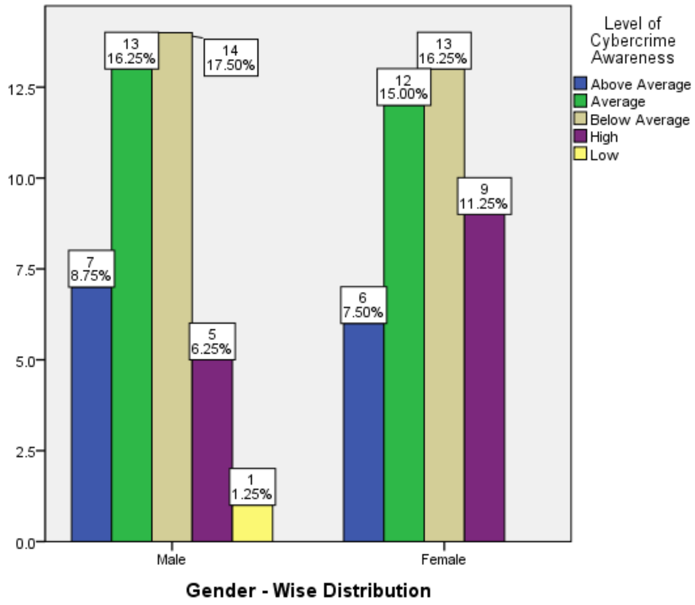

Figure 3.1: *Depicts the level of awareness of cybercrime among students based on gender*

Table 3.2: *Depicts students' level of awareness of cybercrime in terms of qualifications*

Qualification	Level of Cyber Crime Awareness					Total
	Above Average	Average	Below Average	High	Low	
U. G	8 (10 %)	14 (17 %)	12 (15 %)	6 (7.5 %)	0 (0 %)	40 (50 %)
P. G	5 (6.3 %)	11 (13.8 %)	15 (18.8 %)	8 (10 %)	1 (1.3 %)	40 (50 %)
Total	13 (16 %)	25 (31 %)	27 (33 %)	14 (17 %)	1 (1.3 %)	80 (100 %)

As per table 3.2 a total of 14 (17%) of 80 (100%) respondents were found to have a high level of cybercrime awareness, with 8 (10%) from P.G and 6 (7.5%) from U.G. A total of 13 (16%) of 80 (100%) respondents were found to have above-average cybercrime awareness, with 8 (10%) from U.G and 5 (6.3%) from P.G. A total of 25 respondents, representing 31% of 80 (100%), were found to have an average level of awareness in terms of cybercrime, with 14 (17%) from U.G. and 11 (13.8%) from P.G. In terms of cybercrime awareness, a total of 27 (33%) of the 80 (100%) respondents were found to be below average, with 15 (18%) from P.G and 12 (15%) from U.G. 1 respondent, representing 1.3% of 80 (100%), was found to have a low level of cybercrime awareness, with 1 respondent from P. G.

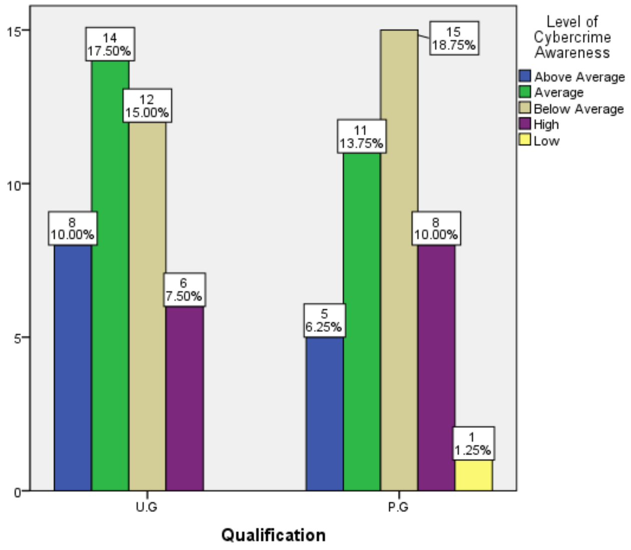

Figure 3.2: *Depicts students' level of cybercrime awareness in terms of qualifications*

Table 3.3: *Depicts the level of awareness of cybercrime among students by stream*

Stream	Level of Cyber Crime Awareness					Total
	Above Average	Average	Below Average	High	Low	
Social Science	8 (10 %)	14 (17 %)	12 (15 %)	6 (7.5 %)	0 (0 %)	40 (50 %)
Science	5 (6.3 %)	11 (13.8 %)	15 (18.8 %)	8 (10 %)	1 (1.3 %)	40 (50 %)
Total	13 (16 %)	25 (31 %)	27 (33 %)	14 (17 %)	1 (1.3 %)	80 (100 %)

As per table 3.3 total of 14 (17%) of 80 (100%) respondents were found to have high cybercrime awareness, with 8 (10%) from science and 6 (7.5%) from social science. A total of 13 (16%) of 80 (100%) respondents were found to be above average in terms of cybercrime awareness, with 8 (10%) from social science and 5 (6.3%) from science stream. A total of 25 (31%) out of 80 (100%) respondents were found to have an average level of cybercrime awareness, with 14 (17%) from social science and 11 (13.8%) from science. In terms of cybercrime awareness, 27 (33%) of 80 (100%) respondents were found to be below average, with 15 (18%) from science and 12 (15%) from social science. 1 respondent (1.3%) out of 80 (100%) was found to have a low level of awareness of cybercrime, with 1 (1.3%) belonging to the science stream as depicts in fig 3.3.

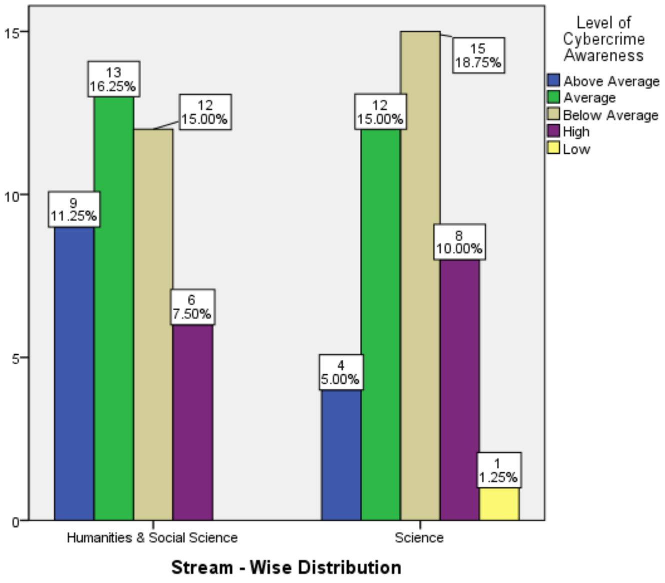

Figure 3.3: *Depicts the level of awareness of cybercrime among students by stream*

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

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

The data obtained from the cybercrime awareness scale presents a clear overview of the existing cybercrime awareness among the faculty members and the data obtained from the sample of the teachers (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*

Sl. no	Groups	N	Mean	Standard Deviation	't' value	df	Level of Significance
1	Male	10	44.70	27.36	0.59	18	Not significant at 0.05 level
2	Female	10	51.80	26.33			
3	Social Science	10	43.70	27.25	0.76	18	Not significant at 0.05 level
4	Science	10	52.80	26.11			

Table 4.1 shows that the calculated t-value was 0.59 for both male and female with mean values of 44.70 and 51.80, respectively. The basic assumption when running a two-sample t-test is that the two independent populations have equal variance. To test this assumption, Levene's Test for Equality of Variances was performed, and the p-value was 0.56, indicating that the assumption of equality of the two variances is met. Both tests have p-values greater than 0.05, implying that there is no significant difference in cybercrime awareness between male and female faculty members. As a result, the null hypothesis *"There will be no significant difference between the mean scores of cybercrime level on male and female faculty members of Assam Don Bosco University"* is not rejected, indicating that gender has no effect on cybercrime awareness. Furthermore, the calculated t-value between Humanities & Social Science and Science was 0.76, with mean values of 43.70 and 52.80, respectively, which is not significant at the 0.05 level of significance for df 18. It means that there is no discernible difference between Humanities & Social Science and Science in terms of cybercrime awareness. As a result, the null hypothesis "*There will be no significant difference between the mean scores of cybercrime level on science and social science faculty members of Assam Don Bosco University"* is not rejected, indicating that cybercrime awareness is unaffected by streams.

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

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

The data obtained from the cybercrime awareness scale presents a clear overview of the existing cybercrime awareness among students, and the data obtained from the sample of students (80) 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 shown in table 5.1

Table 5.1: *t – ratio representation of groups*

Sl. no	Groups	N	Mean	Standard Deviation	't' value	df	Level of Significance
1	Male	40	44.57	17.96	0.93	78	Not significant at 0.05 level
2	Female	40	48.67	21.04			
3	Social Science	40	48.80	19.07	0.99	78	Not significant at 0.05 level
4	Science	40	44.45	20.01			
5	U.G.	40	47.47	18.14	0.38	78	Not significant at 0.05 level
6	P.G.	40	45.77	21.06			

Table 5.1 shows that the male and female t-values were 0.93, with mean values of 44.57 and 48.67, respectively, which is not significant at the 0.05 level of significance for a df of 78. It means that there is no discernible difference in the awareness of cybercrime among male and female students. As a result, the null hypothesis *"There will be no significant difference in the mean scores of cybercrime awareness on male and female students at Assam Don Bosco University"* is not rejected, indicating that gender has no effect on cybercrime awareness. Furthermore, with mean scores of 48.80 and 44.45, respectively, the calculated t-value between Social Science and Science students was 0.99, which is not significant at the 0.05 level of significance for df of 78. This means that there are no statistically significant differences in cybercrime awareness between ADBU students majoring in Social Science and Science. As a result, the null hypothesis *"There will be no significant difference in the mean scores of cybercrime awareness on social science and science students at Assam Don Bosco University"* is not rejected, and streams have no effect on cybercrime awareness. Furthermore, for U.G and P.G students with mean values of 47.47 and 45.77, respectively, the calculated t-value was 0.38, which is not significant at the 0.05 level of significance for df of 78. This means that there is no discernible difference in cybercrime awareness between ADBU's U.G and P.G students. As a result, the null hypothesis *"There will be no significant difference in the mean scores of cybercrime level on U.G and P.G students at Assam Don Bosco University"* is not rejected, indicating that U.G and P.G students have no effect on cybercrime awareness.

Objective 5: To suggest recommendation for creating awareness about cybercrime and security 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. Out of 20 (100%) faculty members, 7 (35%) respondents fall under high and average level of cybercrime awareness, with 3 (15%) male and 4 (20%) female faculties.
2. Out of 20 (100%) faculty members, 13 (65%) respondents fall under average and below- average level of cybercrime awareness, with 7 (35%) male and 6 (30%) female faculties.
3. There were no significant disparities in cybercrime awareness level between male and female faculties at Assam Don Bosco University. This study supports the conclusion of Verma & Kushwaha (2021) and Joshi & Kandpal (2020); Geol (2014); Singh (2013).
4. Out of 20 (100%) respondents, 7 (35%) respondents fall under high and above average level of cybercrime awareness, with 3 (15%) from social sciences and 4 (20%) were from sciences.
5. Out of 20 (100%) respondents, 13 (65%) respondents fall under below average and average level of cybercrime awareness, with 7 (35%) from social sciences and 6 (30%) from sciences.
6. There were no significant differences in cybercrime awareness levels between the social sciences and sciences faculties at Assam Don Bosco University. This study supports the conclusion of Singh (2013).

In terms of Students of ADBU

1. Out of 80 (100%) participants, 27 (33%) fall under high and above average level of cybercrime awareness, with 12 (15%) male and 15 (18%) female.
2. Out of 80 (100%) participants, 53 (66%) fall under average, below average and low levels of cybercrime awareness, with 28 (35%) male and 25 (31%) female.
3. There were no significant differences in cybercrime awareness between male and female students at Assam Don Bosco University. This study supports the conclusions of Verma & Kushwaha (2021) and Joshi & Kandpal (2020); Goel (2014); Singh (2013).
4. Out of 80 (100%) participants, 27 (33%) fall under high and above average levels of cybercrime awareness, with 20 (25%) were U.G and 20 (25%) were P.G students.
5. Out of 80 (100%) participants, 28 (%) fall under low and below average level of cybercrime awareness, with 12 (15%) were U.G and 16 (20%) were P.G students.
6. There was no significant difference in cybersecurity awareness between U.G and P.G students at Assam Don Bosco University.
7. Out of 80 (100%) participants, 27 (33%) fall under high and above average level of cybercrime awareness, with 14 (17%) were from social science and 13 (16%) were from sciences.

8. Out of 80 (100%) participants, 28 (35%) fall under below average and low level of cybercrime awareness, with 12 (15%) were from social sciences and 16 (20%) were from sciences.
9. There were no significant differences in cybersecurity awareness between the Social Sciences and Sciences streams. This study supports the conclusions of Singh (2013).

Regarding Education

1. Out of 80 (100%), 30 (37.5%) are undecided, 18 (22.5%) disagree, and 13 (16.3%) strongly disagree regarding the university organize workshops, seminars, or sessions for students on cybercrime awareness and security.
2. Out of 80 (100%), 31 (38.8%) are unsure, 25 (31.3%) disagree, and 8 (10%) strongly disagree that cyber hygiene and its ethical roles are not included in their university curriculum.
3. Out of 80 (100%), 31 (38.8%) are unsure, 26 (32.5%) disagree, and 7 (8.8%) strongly disagree that the curriculum was designed to provide learners with cyber safety programmes.
4. Out of 80 (100%), 30 (37.5%) are unable to decide, 25 (31.3%) disagree, and 8 (10%) strongly disagree that the current curriculum does not emphasise the significance of cyber laws to learners.
5. Out of 80 (100%), 34 (42.5%) are completely unsure, 24 (30%) agreed, and 11 (13.8%) strongly agreed that the importance of cybersecurity and threats to learners is undervalued in the curriculum.
6. Out of 80 (100%), 18 (22.5%) are unsure, 35 (43.8%) agreed, and 20 (25%) strongly agreed that the curriculum must include cyber safety programmes, awareness, and cybersecurity for instructors and learners.

Online Victimization

1. Out of 80 (100%) respondents, 4 (5%) strongly agreed that they had been victimized online. Out of 80 (100%) respondents, 13 (16.3%) reported having been victims of cyberbullying.
2. Out of 80 (100%) respondents, 3 (3.8%) agreed that they had been victimized somebody on the internet. A total of 2 (2.5%) of 80 (100%) strongly agreed that they had oppressed someone on the internet.
3. A total of 10 (12%) of 80 (100%) respondents agreed that someone had impersonated them online, 1 respondent (1.3 %) of 80 (100%) strongly agreed that someone else had impersonated them on the internet.
4. A total of 8 (10%) of 80 (100%) agreed that they have pretended to be someone else online. Out of 80 (100%), 15 (18.8 %) agreed that someone had decided to share their content or images without their prior consent.
5. Out of 80 (100%), 6 (7.5%) have experienced blackmail or harassment via the internet. A total of 3 (3.8%) of 80 (100%) have been sexually harassed online.
6. A total of 12 (15.0%) out of 80 (100%) have experienced online cyberattacks. 5 (6.3%) out of 80 (100%) fully agreed that someone managed to hack their device, computer, and online account.
7. A total of 12 (15%) of 80 (100%) have strongly agreed that they have been a victim of online fraud. Another 6 (7.5%) of 80 (100%) accepted that they had been a victim of online fraud.

IX. Suggestion and Recommendations

The descriptive findings presented in this paper helped to illustrate the cybercrime awareness of the surveyed Assam Don Bosco University faculty members and students, and it could be concluded based on the findings as follows:

1. A cybercrime awareness education program for faculty and students should be developed, and the curriculum for both social sciences and sciences should include online safety programs, cyber ethics, and computer and network security. Universities should hold comprehensive cybercrime and security training and educational sessions to ensure that all users are aware of the most common internet security risks and vulnerabilities, as well as the most recent cybercrimes and cyber-laws and promote cyber security awareness. According to Singh (2013), education is indeed a powerful tool for promoting cybercrime knowledge and understanding among the younger generation and educational administrators and educators must recognize their role in raising cybercrime awareness among students.
2. To enhance their professional position and effectiveness, institutions should educate and train their faculty and students on widespread cybercrime and cybercrime indicators such as vulnerabilities, cyberattacks, and cases, as well as the dangers of using the internet without adequate safeguards. It may aid in reducing the involvement of both students and faculty in cybercrime who make mistakes due to a lack of awareness about cybercrime. Bansal (2018) also said there's an urgent need to provide cyber security and internet safety education.
3. Universities and schools should direct students toward education that focuses on cyber safety education programs and information technology practices for future safety in the 21st century. One of the primary reasons students are not educated on the effects of cybercrime and security is that educational leaders and employees are not educated either. Many of the same security threats that are associated with computers are also associated with mobile devices, so education for both computer security and mobile device security should be made more widely available. Students must be prepared to face the digital-age workplace challenges. As technology evolves, so must curriculum.
4. More proactive techniques, such as training and guidance, followed by practices and implementation learning, are required. A combination of the two methods is more effective and strongly advised. Because emerging adults are the intended audience for cybercrime awareness and education programs, delivery methods such as multimedia, text, or game-based are all viable options. Security awareness must be taught at various levels to users.

5. A cyber security culture must be developed at the university level to ensure the safety of both students and staffs. According to Aljohani & Elfadil (2020), for students to identify potential threats, a culture must be established. In addition, students need to be well-prepared and educated about the security measures that users can utilize to prevent themselves from becoming victims of cybercrime.

X. CONCLUSION

The findings of the study on cybercrime awareness among faculty members and students at Assam Don Bosco University, display that out awareness towards cybercrime is not significantly affected by gender and stream and out of 20 faculty members 10 were found to have below average level of cybercrime awareness with 30% from social science and 20% from sciences faculty members. Similarly, out of 80 (100%) 33% were found to be below average level on cybercrime awareness (15%) from U.G and (18%) from P.G and with (18.8%) from sciences and (15%) from social sciences and half of the respondents agreed that the curriculum must include cyber-safety programs, awareness, and cybersecurity for instructions and learners. Lastly, the current study also reveals that students have been victims of cybercrime such as cyberbullying, cyberstalking, sexual harassment, online fraud, and blackmail. Educational stakeholders and administrators should take precautionary measures, and faculty and students can be made aware by offering training programs, seminars, and conferences, along with many others. As stated by (Choudary. 2020), the government should follow some cybercrime guidelines and hold seminars and workshops to educate learners at all levels.

The concept of traditional education has shifted dramatically and adopted new strategies in recent years. With the rise of the internet and new technologies, being physically present in a classroom is no longer the only way to learn. The entire educational process has undergone a paradigm shift. According to Sarre et al. (2018), there is a great need for more academics to get involved in cybercrime prevention and cybersecurity research. It is also critical to investigate the topic of interdisciplinarity. To understand the impact of cybercrime around the world, we need to look through a variety of lenses, including legal, sociological, and political ones. Individuals can now obtain a high-quality education whenever and wherever they want, if they have Internet access. With the inclusion of e-learning in the educational system, it has become necessary to raise awareness about cybercrime, attacks, and cyber threats, as well as potential solutions to overcome them.

XI. REFERENCES

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput., 5(2), 23. doi: 10.3390/bdcc5020023

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.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., & Levi, M. et al. (2013). Measuring the Cost of Cybercrime. *The Economics of Information Security and Privacy*, 265-300. doi: 10.1007/978-3-642-39498-0_12

Ariola, B., Laure, E. R. F., Perol, M. L., & Talines, P. J. (2018). Cybercrime awareness and perception among students of Saint Michael college of caraga. *SMCC Higher Education Research Journal*, 1(1). https://doi.org/10.18868/cje.01.060119.03

Bansal, P. (2018). Cybercrime Awareness among Prospective Teachers in Relation to Institutional Management and Behavioural Pattern Types. *Online International Interdisciplinary Research Journal*, {Bi-Monthly}, ISSN 2249-9598,

Bhati, V. S., & Bansal, J. (2019). Social media and Indian youth. *International Journal of Computer Sciences and Engineering*, 7(1), 818–821. https://doi.org/10.26438/ijcse/v7i1.818821

Choudhary. (2020). CYBER CRIME AWARENESS AMONG HIGHER EDUCATION STUDENTS FROM HARYANA WITH RESPECT TO VARIOUS DEMOGRAPHICAL VARIABLES. *PalArch's Journal of Archaeology of Egypt / Egyptology*, 17(7), 14454–14461. https://archives.palarch.nl/index.php/jae/article/view/5499

Goel, U. (2014). Awareness among B.Ed teacher training towards Cyber-crime-A Study. *Learning Community-An International Journal of Educational and Social Development*, 5(2and3), 107. https://doi.org/10.5958/2231-458x.2014.00013.x

Green, J. S. (2016). Cyber Security: *An Introduction for Non-Technical Managers*. Routledge.

Holt, T. J., & Bossler, A. M. (Eds.). (2020). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Springer International Publishing.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology*, 1(2), 7-9.

Jazeel. (2018). A Study on Awareness of Cybercrime among Teacher Trainees in Addalaichenai Government Teachers' College. *Journal of Social Welfare and Management*, 10(1), 31–34. https://journals.indexcopernicus.com/publication/2293579/A.M.-Jazeel-A-Study-on

Joshi, & Kandpal. (2020). CYBER CRIME AWEARNESS AMONG ADOLESCENTS. IJCRT - *International Journal of Creative Research Thoughts (IJCRT)*, 8(12), 1736–1743. https://doi.org/10.1729/journal.26002

Keelery, S. (2021, March 10). Topic: Cybercrime in India. Statista. https://www.statista.com/topics/5054/cyber-crime-in-india/#dossierKeyfigures

Kremling, J., & Parker, A. M. S. (2017). *Cyberspace, cybersecurity, and cybercrime*. SAGE Publications.

Martellozzo, E., & Jane, E. A. (2017). *Cybercrime and its victims*. Taylor & Francis.

Meško, G. (2018). On Some Aspects of Cybercrime and Cybervictimization. *European Journal of Crime Criminal Law and Criminal Justice*, 26(3), 189–199. https://doi.org/10.1163/15718174-02603006

O'Dea, S. (2022, February 23). Smartphone users 2026. Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Prensky, M. (2001). Digital natives, digital immigrants' part 1. *On the Horizon*, 9(5), 1–6. https://doi.org/10.1108/10748120110424816

Punia, P., & Phor, M. (2019). Study of Cyber Crime Awareness in Relation to Internet Addiction. *Learning Community-An International Journal of Educational and Social Development*, 10(1), 29-40.

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to cybercrime: current trends. *Police Practice & Research: An International Journal*, 19(6), 515–518. https://doi.org/10.1080/15614263.2018.1507888

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

Singh, J. (2013). To analyze cybercrime awareness of class XII students. *Scholarly Research Journal for Interdisciplinary Studies*, 1(1), 1327-1329.

Tapscott, D. (1998). *Growing Up Digital: The Rise of The Net Generation*. New York: McGraw-Hill.

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Hallatu, T. G. R. (2019). Cybercrime Case as Impact Development of Communication Technology That Troubling Society. *International Journal of Science and Technology. Res*, 8(9), 1224-1228.

Verma, M. K., & Kushwaha, S. S. (2021). Awareness towards cybercrime among secondary school students: the role of gender and school management. *Safer Communities*, 20(3), 150–158. https://doi.org/10.1108/sc-07-2020-0026

Whitman, M. E., & Mattord, H. J. (2012). *Roadmap to information security: For IT and infosec managers*. Cengage Learning.

Zayid, E. I. M., & Farah, N. A. A. (2017). A study on cybercrime awareness test in Saudi Arabia-Alnamas region. *In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 199-202). IEEE.*