Quantitative Assessment of the Cybersecurity and Cybercrime Awareness among Postgraduate Commerce Students in the Coimbatore District, India

Kaleeshwari S. [a++*] and M. Jegadeeshwaran [a#]

a Department of Commerce, Bharathiar University, Coimbatore, Tamil Nadu, India.

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Original Research Article

_____

Abstract

Aim: Key motive is to research the prevailing level of awareness level of commerce post graduate students on cyber crime and cyber security in their day-to-day life.

Design/ Methodology/Approach: In the current research paper, data has been collected based on census method using high ended questionnaire from 178 M. Com students from University in Coimbatore district of Tamil Nādu in India. The accumulated information is further analyzed in testing their level of awareness using descriptive statistics and Anova to check the difference with respect to their demographics. The Researchers want to know how college students feel about being aware of cybercrime and cyber security so they are looking into that.

_____

[++]*PhD Research Scholar;*
[#]*Associate Professor;*
Corresponding author: Email: madhukaleeshwari@gmail.com;

Findings: The study has identified the factors for the level of awareness on cybercrime with 5 variables and cybersecurity with 6 variables. These variables have different perspective with respect to the demographic factors of the commerce post graduate students. Especially the Course of study and the year of study creates difference in the awareness level.

Research Limitations: The study is a valuable understanding for the students in commerce stream at their post graduate level in knowing their level of understanding and awareness of cybercrimes and cyber security. This study has only focused on the commerce post graduate students of university and it is restricted to the Coimbatore district of Tamil Nādu alone. The results cannot be generalized commonly for the students in post-graduation.

Originality: The study is original contribution to understand the awareness of commerce post graduate students in Tamil Nadu. It can be definitely used for further references in terms of level of awareness of students from different range or the study can be further expanded by the researchers and policy makers in developing the safety and awareness measures towards cybercrime and cybersecurity.

Keywords: Cybercrime; crime security; post graduate students; awareness level; difference.

1 Introduction

Although the digitalization of the world has many more benefits, it has also created a two-edged sword that poses both a threat and a benefit, which has had some negative effects on people. India has embraced digitalization on all fronts as a strong nation. This cyber realm has long posed a hazard, potentially harming users' security and finances by gaining access to their personal data. Cybercrime is a today based scenario which causes severe loss to the victim which is taking place using internet. it orders to prevent such crimes and threat the cyber space has developed cyber security measures which gives various safety measures in safe guarding the personal space of an individual. With the help of (I4C) of (Ministry of Home Affairs) cyber security antiquated developed. Internet consumption a growingly significant aspect of modern life. Everyone depends heavily on the internet, which opens up more opportunities for cybercrime. In the current environment, cybercrime is becoming a very serious problem. The internet becomes a staple in our life because it provides us joy and happiness, but it can also be a nightmare. Cybercriminals utilize many different methods to defraud people.

Everyone is becoming an expert in the cyber world, from businesspeople to government officials, high school kids to college students, and adults to elders. Various communication techniques have been developed worldwide. Consequently, public and private sectors have begun to offer more services and adopt new technologies to provide access to information anytime and anywhere upon request from customers. The key reason behind automating services and adopting new technologies is to support and satisfy a wide range of customers, whose number has been increasing rapidly owing to the increase in the usage of the Internet. In response, the number of hackers and organized cybercrime groups has grown exponentially. Krutika Bhate [1]. Ultimately, the most well-known online threats include malevolent programming (malware) such as Trojan horses, keyloggers, and viruses, as well as malicious techniques like phishing and social engineering that aim to steal personal information and cause financial and psychological harm to victims. Malware occasionally masquerades as a virus [2-4].

(Erbschloe, 2019; Kara & Aydos, 2019; Prem & Reddy, 2019; Chakraborty, 2019). According to Statista (2020), a study conducted on everyday Internet users in India in 2020, 73.00% of people between the ages of 16 and 24 are Internet users. The Digital 2021 India report also confirmed that young adults in India are heavy Internet users. Additionally, a comparison report listed the following among respondents who were enrolled in school: over 62.50% were in colleges or universities, 34.90% were in secondary schools, 02.40% were in lower elementary schools, and 00.20% were in other settings. This demonstrates that, in contrast to secondary and primary school pupils, higher education students are important Internet users. In a similar vein, this study demonstrates how quickly Indian young adults are accessing the Internet and extending their online time.

2 Review of Literature

Kumar Rajender [5], The awareness of cybercrime among male, female pupil and different locality pupils shows a significant difference. Male and urban pupils show higher levels of mindfulness of digital misconduct.

Wejdan Aljohani, Nazar Elfadil [6], The purpose of this study paper's questionnaire instrument is to gauge students at Fahad Bin Sultan University's (FBSU) current degree of cyber security awareness (CSA). The purpose of the questionnaire is to meet the aims and objectives of this research project. This paper's primary objective is to assess FBSU students' awareness of cyber security. Additionally, a few other cyber security awareness-related surveys were modified to create the cyber security students' awareness level questionnaire. 212 students in all have taken part in the poll. The study's conclusions indicate that students' understanding of cyber security is average and that male and female students have similar levels of awareness. Additionally, the results of the survey tool show that the module has been successful in measuring awareness.

Talal Alharbi, Asifa Tassaddiq [7], The purpose of this study was to employ a scientific questionnaire based on many Internet safety aspects to explore and assess Majmaah University undergraduate students' cybersecurity awareness and user compliance. We conducted a quantitative assessment of students' knowledge on cybercrime and protection in order to highlight the need of user awareness, education, and training. In this study, we evaluated and analysed the hypotheses using a quantitative research technique and a variety of statistical tests, including ANOVA, Kaiser–Meyer–Olkin (KMO), and Bartlett's tests. This study thoroughly evaluated safety risks related to pop-up windows, computer viruses, phishing, faked adverts, electronic emails, and further online outbreaks. Lastly, we offer suggestions based on the information gathered to address this typical.

Dr. Geni Philiposel, Mr. Karthik [8], This study explores the level of knowledge that students who finished their schooling during the COVID-19 pandemic have about cybercrime. Technology and the internet have significantly improved education, but they have also made people more susceptible to criminal activity.Users must be aware of the hazards involved and take preventative action since cybercriminals take advantage of the flaws in digital systems. Students at the Hindustan Institute of Technology and Science were surveyed as part of the study to learn more about their perceptions of internet security and their understanding of cybercrime. The results of this study may make it easier to create focused campaigns to increase public awareness of cybercrime and promote a safer online environment.

Ravi Kant [9], This study examines the understanding of cyber security among college students based on several key educational and demographic factors, including gender, domicile, study level, and so forth. Graduates, master's degree holders, and research students from numerous national institutions and colleges provided the data for this study over the Internet. Students did not differ according to their gender or the type of course. According to the students' academic specialities and residence locations, there were notable differences in their awareness of cyber security. It was discovered that pupils in urban regions had a greater awareness of cyber security than those in rural areas. Based on the study level, no discernible difference was discovered between them, though. Because of several inherent and uncontrollable research constraints, the findings of this study cannot be regarded as definitive. However, the findings of the observations made in this study might offer some support for future research and the body of public knowledge.

Krutika Bhate [1], A cyber security awareness campaign is required in order to address the awareness of cyber security among female students in higher education institutions. The Maharaja Sayajirao University of Baroda's female students' awareness of cyber security was examined in this survey, which also educates them about the risks and difficulties that are common in cyberspace. Purposively chosen, 167 female students participated in the experimental study. Data were gathered using an online survey, which required extensive follow-up because students did not complete it. The study's conclusions showed that female students knew less about phrases like phishing, cyberbullying, cyberstalking, and other terms associated with cybercrime. While students are less conscious of browser security, they are cognisant of social media and password security. The awareness-raising session proved successful in educating female university students about cybercrime and cybersecurity. Fewer pupils showed up for the lesson, but those who did should know how important cyber security is. The study comes to the conclusion that students need to be made far more aware of cyber security. The study's conclusions suggest that colleges should provide their students with instruction on cyber security.

Mamta sahu, Prabhavati Shukla [10], Finding out how aware pupils are of cybercrime in the Chhattisgarh region is the goal of the current study. Today's environment demands technology for everything from household chores to managing a global corporation and maintaining national security. Technology does indeed make life easier, but it also comes with risks. One such risk is cybercrime, which includes fraud, violence, bullying, sexual harassment, and phishing. Students need to know that being knowledgeable of cyber security is essential to preventing all forms of cybercrime. To gain insight into the level of cyber-awareness among Chhattisgarh

students, we gathered data from Pt. Ravishankar Shukla University located in Raipur. A questionnaire-based survey method was utilised to assess students' awareness of cybercrime using the cyber-crime awareness scale developed by Dr. S. Rajasekar (2011).

2.1 Research gap

There are numerous studies conducted on the different target population and the studies has been analyzed on the awareness and the challenges. Even though there are studies found among students and other population of the world towards the cyber-crime and cyber security. There are no such studies found among the commerce post graduate students as target population and there are no such studies conducted which has been taken as the research gap and the current study has been made an attempt study the level of awareness among Post Graduate students of commerce stream on cybercrime and cyber security in Coimbatore district of Tamilnadu, India for understanding the exact clear picture of how much and how well the students are aware of the crimes happening in and around them and the safety measures taken by the policy makers to control and avoid the crimes against cyber activities.it becomes essential in understanding the knowledge level and the awareness level of the commerce students hence they are from the commerce and they must be much aware and intellect on the cybercrime and cyber security. This study will bring out an overview of how well the students are really aware of the current trend on crime and security matter of cyberspace.

2.2 Statement of the problem

Increasing technological development as well as advancement have paved way for the cybercrime which is an unlawful act which either targets the internet and computer. Apart from this there are cyber wars and cyber terrorism which is beaming in the global scenario. The increasing level of crimes through cyberspace is because of lack of awareness and understanding the issues associated with the internet form of threat which is leading to the cyber-attacks and threat. This study aims to focus on the young population in society in analyzing their awareness towards cybercrime and cyber security measures by analyze the level of awareness among Post Graduate students of commerce stream on cybercrime and cyber security in Coimbatore district based on demographic factor the paper examines the awareness level based on the demographic factors which determines their understanding on cyber space which becomes necessary for the entire nation in preventing the threat.

The above problem is discussed using research questions:

- Are the post graduate students under commerce stream aware about the cybercrime and cyber space?
- If yes this there any difference among the students based their demographic factors?

2.3 Hypothesis

- H1 = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Gender.
- H2 = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Course of Study
- H3 = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Year of Study.
- H4 = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Gender.
- H5 = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Course of Study
- H6 = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Year of Study.

3 Methodology

The study is empirical in nature. And quantitative study has been carried out to analyse the results.

3.1 Variables and measures

For investigating the data, the awareness of post graduate students under commerce steams has its Dependent Variable. Were the demographic variables being independent on the level of awareness. Due to increasing usage of technology and electronic gadgets for communications, it becomes necessary to be aware of the crimes and security measure towards the technology development in the world. The level of awareness on cybercrime is measured with 5 variables such as "Malware Attack"," SQL Injection Attack", "Website spoofing", "Ransomware", "IOT hacking". And the Cyber security is measured using the variables such as "Cloud Security", "End point security", "Mobile security", "IoT security password attack", "Application Security", and "Zero Trust Security". These factors are majorly depending on the demographic factors in deciding the association and difference in understanding the cybercrime and cyber security measures by the students. The above select variables are taken from the official website of (Ministry of Electronics and Information Technology), (Government of India), National Crime Records Bureau based on the crimes and security measures taken against them to prevent.

3.2 Data source and data collected for the study

Analysis is depending on Key (Primary) and Central (Secondary) references of data. Key information is accumulated using Questionnaire specially designed for the analysis which was framed using the past review of literature. The questionnaire contains of 5 variables indicating cybercrime threats and 6 variables towards cyber security for analysing the awareness of cybercrime and cyber security among commerce graduate students. The first part covers the demographic parts and the second part covers the variables based on awareness level. Central information is accumulated from Official website of (Ministry of Electronics and Information Technology), (Government of India), National Crime Records Bureau and also from various books and journals. The study uses the Census methodology for data collection. The survey was conducted by personally circulating the questionnaire for the targeted audience. The information from 178 respondents Coimbatore District collected through well-structured questionnaire and the respondents response collected after asking their willingness to take part in the survey and they informed consent to participate freely in the survey. Further the data scrutinized and validated, suggestions and comments were incorporated as the nature of question.

3.3 Data interpretation

SPSS software is used on the data accumulated, the removed values for missing items were carried through. The further analysis was carried assisting the qualitative tools such as Reliability analysis, Validity Analysis and Anova to test their cause and effect of their test variables and the difference prevailing with respect to the demographic profile.

4 Results and Discussion

Table 1. Enumeration of participant profile

Elements	Variable	Number of Participants
Gender	Male	52
	Female	126
Age	18-25	176
	25-30	2
Course of Study	M.Com (Finance and Computer Application)	52
	M.Com (Finance and Accounting)	70
	M.Com (Financial Technology)	56
Year of Study	I year	76
	II year	102

The features of the participants are broken down in the table. The bulk of respondents—126, or 70.78 percent—are female and rest of the respondents are male with 52 responses at 29.54 percent, and 99.8 percent of them are younger than the age of 18–25 under the age group covering the category of 18-25 and respondents under the age

group of 25-30 covers only 2 responses at 1.12 percent. Around 70 respondents of, 39.32 percent of them are working towards their M. Com. (Finance and Accounting) degree apart from that there are respondents from the course of M. Com (Finance and Computer Applications) covers 52 responses at 29.21 percent and M. Com (Financial Technology) covering 56 responses at 31.46 percent. Additionally, their pursuit under the second year of study at 102 at 85.39 percent and respondents from the 1st year of covers the response level of 76 at 42.69 percent.

Table 2. Reliability analysis for the awareness level of post graduate students on Cyber Crime and cyber security in Coimbatore District

Reliability Statistics	
Cronbach's Alpha	**N of Items**
.891	11

Source: computed using spss

The table denotes Cronbach's alpha value of .891 is higher than the required value, demonstrating good consistency among the items and the validity of the instruments created for the study. All variables are trustworthy and appropriate, it can be said.

Table 3. KMO and Bartlett test for goodness of fit awareness level of post graduate students on Cyber Crime and cyber security in Coimbatore District

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		**.850**
Bartlett's Test of Sphericity	**Approx. Chi-Square**	1033.597
	df	55
	Sig.	**.000**

Source: computed using spss

Table indicates the KMO statistic value is above.850, according to the table. it exceeds the threshold 0.5. The size of the sampling is sufficient for factor analysis, and Bartlett's test for sphericity yields a significant result of.000 that justifies running additional tests.

Table 4. Descriptive statistics for the awareness level of post graduate students on Cyber Crime in Coimbatore District

Descriptive Statistics			
	N	Mean	Std. Deviation
Malware Attack	178	2.38	1.203
SQL Injection Attack	178	**2.90**	1.434
Website Spoofing	178	2.12	1.175
Ransomware	178	**2.91**	1.367
IOT hacking	178	2.22	1.172

Source: computed using spss

The table displays descriptive statistics for the district of Coimbatore's postgraduate students' knowledge of cybercrime and cybersecurity. The SQL Injection Attack and the Ransomware Attack had the highest mean values, respectively, at 2.90 and 2.91. which means the students are much aware or unaware of the particular variables as per their response based on the questionnaire.

The Table 5 presents descriptive statistics regarding postgraduate students' understanding of cybersecurity and cybercrime in the Coimbatore district. The highest mean values were for End Point Security and Zero Trust, with 2.52 and 2.83, respectively. which means the students are much aware or unaware of the particular variables such as "End point Security" and "Zero point security" as per their response based on the questionnaire.

Table 5. Descriptive statistics for the awareness level of post graduate students on cyber security in Coimbatore District

Descriptive Statistics	N	Mean	Std. Deviation
Cloud security	178	1.75	.966
End Point Security	178	**2.52**	1.294
Mobile security	178	1.73	.820
IoT Security Password Attack	178	2.04	1.124
Application Security	178	2.06	1.158
Zero Trust Security	178	**2.83**	1.338

Source: computed using spss

$H0_1$ =There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Gender.

Table 6. Test of Difference in the awareness level on Cybercrime of post graduate students in Coimbatore district based on Gender

ANOVA		Sum of Squares	df	Mean Square	F	Sig.
Malware Attack	Between Groups	3.825	1	3.825	2.669	.104
	Within Groups	252.198	176	1.433		
	Total	256.022	177			
SQL Injection Attack	Between Groups	.288	1	.288	.140	.709
	Within Groups	363.891	176	2.068		
	Total	364.180	177			
Website Spoofing	Between Groups	.464	1	.464	.335	.563
	Within Groups	244.058	176	1.387		
	Total	244.522	177			
Ransomware	Between Groups	.301	1	.301	.160	.690
	Within Groups	330.261	176	1.876		
	Total	330.562	177			
IOT hacking	Between Groups	1.878	1	1.878	1.371	.243
	Within Groups	241.133	176	1.370		
	Total	243.011	177			

Source: computed using spss

The table displays the findings of a one-way ANOVA that compared postgraduate students in the Coimbatore district's gender to their awareness of cybercrime. Regarding awareness of cybercrime based on gender , the significant value is more than 0.05 for all the factors. Since there is no discernible difference between postgraduate students in the Coimbatore district's according to gender and their awareness of cybercrime they are equally associated or different in their opinion on cybercrime, Hence the hypothesis is accepted that there is no difference with the Awareness level on Cybercrime of post graduate students in Coimbatore district based on Gender.

$H0_2$ = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Course of Study.

The one-way ANOVA that compares course of study of postgraduate students in the Coimbatore district to their knowledge of cybercrime are shown in the Table 7. For elements like a SQL Injection Attack, website spoofing, and ransomware, the significant value for awareness of cybercrime is above 0.05 indicating that there is no difference, concluding that the Null hypothesis is accepted. The tentative statement is taken up as result since no appreciable difference between the postgraduate students' awareness of cybercrime and their course of study in the Coimbatore district is found. Malware attack and IOT hacking, however, have significant values below 0.05, which implies the tentative statement is disapproved and stated that student differences in cybercrime depend on their chosen academic path.

Table 7. Test of difference in the awareness level on Cybercrime of post graduate students in Coimbatore district based on Course of the study

ANOVA						
		Sum of squares	df	Mean Square	F	Sig.
Malware Attack	Between Groups	11.027	2	5.513	3.938	**.021**
	Within Groups	244.996	175	1.400		
	Total	256.022	177			
SQL Injection Attack	Between Groups	8.896	2	4.448	2.191	.115
	Within Groups	355.284	175	2.030		
	Total	364.180	177			
Website Spoofing	Between Groups	2.830	2	1.415	1.025	.361
	Within Groups	241.692	175	1.381		
	Total	244.522	177			
Ransomware	Between Groups	.307	2	.153	.081	.922
	Within Groups	330.255	175	1.887		
	Total	330.562	177			
IOT hacking	Between Groups	10.789	2	5.395	4.065	**.019**
	Within Groups	232.222	175	1.327		
	Total	243.011	177			

Source: computed using spss

$H0_3$ = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Year of Study.

Table 8. Test of difference in the awareness level on Cybercrime of post graduate students in Coimbatore district based on Year of the study

ANOVA						
		Sum of squares	df	Mean square	F	Sig.
Malware Attack	Between Groups	7.412	1	7.412	5.247	**.023**
	Within Groups	248.611	176	1.413		
	Total	256.022	177			
SQL Injection Attack	Between Groups	3.135	1	3.135	1.528	.218
	Within Groups	361.044	176	2.051		
	Total	364.180	177			
Website Spoofing	Between Groups	.000	1	.000	.000	.997
	Within Groups	244.522	176	1.389		
	Total	244.522	177			
Ransomware	Between Groups	11.969	1	11.969	6.612	**.011**
	Within Groups	318.592	176	1.810		
	Total	330.562	177			
IOT hacking	Between Groups	2.739	1	2.739	2.006	.158
	Within Groups	240.272	176	1.365		
	Total	243.011	177			

Source: computed using spss

The table displays the findings of a one-way ANOVA that related postgraduate students' knowledge of cybercrime to their year of the study in the Coimbatore district. For components like a SQL Injection Attack, website spoofing, and IOT hacking, the significant value for awareness of cybercrime is more than 0.05. Since there is no discernible relationship between the Coimbatore district postgraduate students' awareness of cybercrime and their degree of study, the tentative statement is the taken up for conclusion is accepted. It is determined that student disparities in cybercrime depend on their selected academic path because Malware attack and Ransomware, on the other hand, have significant values below 0.05, indicating the tentative statement is rejected which means there is a difference in the awareness level of students.

$H0_4$ = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Gender.

Table 9. Test of difference in the awareness level on cyber security of post graduate students in Coimbatore district based on Gender

		Sum of squares	df	Mean square	F	Sig.
Cloud security	Between Groups	.036	1	.036	.038	.846
	Within Groups	165.088	176	.938		
	Total	165.124	177			
End Point Security	Between Groups	4.679	1	4.679	2.822	.095
	Within Groups	291.770	176	1.658		
	Total	296.449	177			
Mobile security	Between Groups	.985	1	.985	1.469	.227
	Within Groups	118.071	176	.671		
	Total	119.056	177			
IoT Security Password Attack	Between Groups	2.537	1	2.537	2.019	.157
	Within Groups	221.104	176	1.256		
	Total	223.640	177			
Application Security	Between Groups	.257	1	.257	.191	.663
	Within Groups	237.181	176	1.348		
	Total	237.438	177			
Zero Trust Security	Between Groups	1.243	1	1.243	.693	.406
	Within Groups	315.701	176	1.794		
	Total	316.944	177			

Source: computed using spss

The table displays the findings of a one-way ANOVA that compared postgraduate students in the Coimbatore district's gender to their awareness of cyber security. Regarding awareness of cyber security, the significant value is more than 0.05 for all the factors such as "cloud security", "End point security", "Mobile security, "IoT security password attack, "Application security" and "Zero Trust Security". Hence it is concluded that there is no discernible difference between postgraduate students in the Coimbatore district's with respect to gender and their awareness of cyber security, the hypothesis is accepted.

$H0_5$ =There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Course of Study.

Table 10. Test of difference in the awareness level on cyber security of post graduate students in Coimbatore district based on Course of Study

		Sum of squares	df	Mean square	F	Sig.
Cloud security	Between Groups	12.226	2	6.113	6.997	**.001**
	Within Groups	152.898	175	.874		
	Total	165.124	177			
End Point Security	Between Groups	2.442	2	1.221	.727	.485
	Within Groups	294.008	175	1.680		
	Total	296.449	177			
Mobile security	Between Groups	2.135	2	1.068	1.598	.205
	Within Groups	116.921	175	.668		
	Total	119.056	177			
IoT Security Password Attack	Between Groups	13.071	2	6.536	5.432	**.005**
	Within Groups	210.569	175	1.203		
	Total	223.640	177			

ANOVA		Sum of squares	df	Mean square	F	Sig.
Application Security	Between Groups	6.061	2	3.031	2.292	.104
	Within Groups	231.377	175	1.322		
	Total	237.438	177			
Zero Trust Security	Between Groups	23.836	2	11.918	7.116	**.001**
	Within Groups	293.108	175	1.675		
	Total	316.944	177			

Source: computed using spss

The table displays the findings of a one-way ANOVA that examined postgraduate students' courses of study and their understanding of cyber security in the Coimbatore district. The significant value for cyber security awareness is greater than 0.05 for components like End point security, mobile security and application security. Since there is no discernible difference between the postgraduate students' knowledge of cyber security and their course of study in the Coimbatore district, the tentative statement is the taken-up conclusion by accepting it . It is found that student disparities in cyber security depend on their selected academic path because cloud security, IOT security password attack, and zero trust security all have significant values below 0.05, indicating that the null hypothesis is rejected.

$H0_6$ = There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Gender.

Table 11. Test of difference in the awareness level on Cyber security of post graduate students in Coimbatore district based on Year of Study

ANOVA		Sum of squares	df	Mean square	F	Sig.
Cloud security	Between Groups	1.773	1	1.773	1.910	.169
	Within Groups	163.351	176	.928		
	Total	165.124	177			
End Point Security	Between Groups	2.638	1	2.638	1.580	.210
	Within Groups	293.811	176	1.669		
	Total	296.449	177			
Mobile security	Between Groups	3.585	1	3.585	5.464	**.021**
	Within Groups	115.472	176	.656		
	Total	119.056	177			
IoT Security Password Attack	Between Groups	7.930	1	7.930	6.471	**.012**
	Within Groups	215.710	176	1.226		
	Total	223.640	177			
Application Security	Between Groups	1.372	1	1.372	1.023	.313
	Within Groups	236.066	176	1.341		
	Total	237.438	177			
Zero Trust Security	Between Groups	1.782	1	1.782	.995	.320
	Within Groups	315.162	176	1.791		
	Total	316.944	177			

Source: computed using spss

The one-way ANOVA that linked Coimbatore district postgraduate students' understanding of cyber security to their year of study. The significant value for cyber security awareness is greater than 0.05 for components like Cloud security, End point security, Application security, and Zero Trust Security. The tentative statement is the taken-up result because there is no obvious correlation between the Coimbatore district postgraduate students' awareness of cyber security and their year of study by accepting the statement. Because mobile security and IOT security password attacks, on the other hand, have significant values below 0.05, suggesting the tentative statement is refused, it is found that student differences in cyber security rely on their chosen academic path. Concluding that there is a difference among the students.

4.1 Discussion

Table 12. Explaining hypothesis along with results

SL.No.	Hypothesis	Results
H1	There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Gender	Accepted for All Variables
H2	There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Course of Study	Accepted for 3 Variables Rejected for 2 Variables
H3	There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cybercrime in Coimbatore district based on Year of Study.	Accepted for 3 Variables Rejected for 2 Variables
H4	There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Gender	Accepted for All Variables
H5	There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Course of Study	Accepted for 3 Variables Rejected for 3 Variables
H6	There is no significant difference in the level of awareness among Post Graduate students of commerce stream on cyber security in Coimbatore district based on Year of Study.	Accepted for 4 Variables Rejected for 2 Variables

For all the parameters, the significant value for gender-based cybercrime awareness is larger than 0.05. The hypothesis that there is no difference in the awareness level of cybercrime among postgraduate students in the Coimbatore district based on gender is accepted because there is no discernible difference between the genders of these students and how they perceive cybercrime. They are either equally associated with it or have different opinions about it. The significant value for awareness of cybercrime for items including ransomware, spoof websites, and SQL Injection Attacks is above 0.05, showing that there is no difference and supporting the acceptance of the null hypothesis. Since there is no discernible difference between the postgraduate students' awareness of cybercrime and their course of study in the Coimbatore district, the preliminary statement is accepted as the outcome.

However, the significant values for malware attacks and IOT hacking are less than 0.05, indicating that the tentative statement—which claimed that student variations in cybercrime depend on their selected academic path of course of study—is denied and the tentative statement is disapproved.In the case of elements such as impersonating websites, IOT hacking, and SQL Injection Attacks, the significant value for cybercrime knowledge is more than 0.05. The tentative statement is taken up for conclusion is accepted since there is no obvious correlation between the postgraduate students' awareness of cybercrime in the Coimbatore district and their field of study.

Malware attacks and ransomware, on the other hand, have significant values below 0.05, indicating the tentative statement is rejected, indicating there is a difference in the awareness level of students. This leads to the conclusion that student disparities in cybercrime depend on their chosen academic path. When it comes to cyber security awareness, all of the factors—cloud security, end point security, mobile security, IoT security password attack, application security, and zero trust security—have significant values greater than 0.05. Therefore, the hypothesis is accepted and it is concluded that there is no appreciable difference in gender or level of cyber security awareness among postgraduate students in the Coimbatore districts.

For elements like endpoint security, mobile security, and application security, the significant value for cyber security awareness is more than 0.05. The preliminary statement is the conclusion that has been accepted because there is no appreciable difference between the postgraduate students' knowledge of cyber security and their course of study in the Coimbatore district. Because cloud security, IOT security password attack, and zero trust security all have significant values below 0.05, showing that the null hypothesis is rejected, it is determined that student differences in cyber security depend on the academic path they choose.The tentative statement is the

accepted result because there is no clear correlation between the postgraduate students in the Coimbatore district's awareness of cyber security and their year of study.

On the other hand, because mobile security and IOT security password attacks have significant values below 0.05, suggesting the tentative statement is refused, it is determined that student differences in cyber security depend on their chosen academic path. This finding suggests that there are differences among the students and the hypothesis is rejected.

5 Conclusion

The increased use of technology year by year which is mostly impacting women and children, through the cyber threat an alarming issue faced by most of the people in society. even though the government is taking measures to enhance the cyber security, there is lack of awareness and understanding regarding the cyberspace which is still a drawback to attain the utmost safety from the cybercrime. hence the study is focusing on the level of awareness among Post Graduate students of commerce stream on cybercrime and cyber security in Coimbatore district based on demographic factors has made us understand that students are aware but not completely aware on cybercrime and cyber security, it shows the importance of conducting awareness and recognition among young population to avoid the further out break. Conversely, ransomware and malware assaults have significant values below 0.05, meaning the preliminary statement is rejected and suggesting a difference in students' knowledge levels. This suggests that differences in cybercrime among students are influenced by the academic path they have taken. All of the factors—cloud security, end point security, mobile security, IoT security, password attack, application security, and zero trust security—have significant values greater than 0.05 when it comes to cyber security awareness. Consequently, the hypothesis is accepted, and it is determined that postgraduate students in the Coimbatore districts do not significantly differ in terms of gender or degree of awareness regarding cyber security. Cybersecurity awareness is highly valuable for components such as application security, mobile security, and endpoint security. Since there is no discernible difference between the postgraduate students' knowledge of cyber security and their course of study in the Coimbatore district, the preliminary statement is the conclusion that has been accepted.

 It is concluded that student disparities in cyber security depend on the academic path they pick because cloud security, IOT security, password attack, and zero trust security all have significant values below 0.05, demonstrating that the null hypothesis is rejected. Since there is no discernible relationship between the postgraduate students' year of study and their awareness of cyber security in the Coimbatore district, the tentative statement is the accepted finding. By raising social media knowledge, the government or policy makers working on cybercrime and cybersecurity can increase the initiation. which implies that social media platforms like Facebook, Instagram, WhatsApp, and Twitter can now have a brief video or pop-up advertisement. Information on recent incidents and news about cybercrime, as well as how to prevent and reduce it, can raise awareness among the general public and students about the dangers of frequenting social media platforms, where many crimes have been reported.

6 Recommendations

Government or the policy makers working on cybercrime and cyber security can increase the initiation through boosting social media awareness. which means a short duration video or advertisement pop up message can be added to the social media platform such as Facebook, Instagram, WhatsApp, Twitter. On news and events of cybercrime been made and how far it can be avoided and minimized such information can boost awareness of not only students but general public how regularly use social media where the large number of crimes are been recorded.

Make Informational Pamphlets regarding the current situation and the need for being aware of the cybercrime and the measure taken by the policy makers to protect the crime made on cyber platform through cyber security techniques which can reach out the public. Government should focus on entire population of the country to make sure the cyber security measures are reaching out to all the citizens of the society. This measure must be made available in regional and local languages to make it much more convenient and comfortable all the citizenry to read and understand. Government may use both personnel and non-personnel medium of communication.

Disclaimer (Artificial Intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

Competing Interests

Authors have declared that no competing interests exist.

References

[1]   Krutika Bhate. A study on Awareness about cyber security among the female university students, International Journal on Emerging Technologies. 2023;14(2):13-19.
      ISSN-2249-3255.

[2]   Alharbi T, Tassaddiq A. Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing. 2021 May 10;5(2):23.

[3]   Alzahrani L. Statistical analysis of cybersecurity awareness issues in higher education institutes. International Journal of Advanced Computer Science and Applications. 2021;12(11).

[4]   Alzubaidi A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon. 2021 Jan 1;7(1).

[5]   Kumar Rajender. A study of cyber crime awareness among B.Ed. And M.Ed. Students of Sirsa District. International Economic Society. 2020;11(3):74-86.

[6]   Wejdan Aljohani, Nazar Elfadil. Measuring cyber security awareness of students:A Case study at Fahad Bin Sultan University, International Journal of Compuetr Science and Mobile Computing. June 2020;9(6):141-155.
      ISSN-2320-088X.

[7]   Talal Alharbi, Asifa T Tassaddiq. Assessment of Cybersecurity Awareness among students of Majmaah University. 2021;5(2).
      Available:https://www.mdpi.com/2504-2289/5/2/23#

[8]   Geni Philiposel, Karthik. Assessing cybercrime awareness and internet usage among students: Implications for policy and Education, Eur. Chem. Bull. 2022;11(11).
      ISSN 1147-1153.

[9]   Ravi Kant. Cyber security awareness in India: How Much Students of Higher education are Aware?, GESJ: Education Science and Psychology. 2023;2(67).
      ISSN1512-1801.

[10] Mamta Sahu, Prabhavati Shukla. A study on cyber crime awareness among students in Chhattisgarh, Journal of Ravishankar University. 2024;30(1).
      ISSN-0970-5910.