IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Pilot Study: Cyber Crime Awareness In College Going Students In KMCL University

Sunita Maurya [1] & Dr. Priyanka Suryavanshi [2]

[1]Ph.D Research Scholar

Department of Home Science

Khwaja Moinuddin Chishti Language University

Sitapur-Hardoi Bypass Road, Lucknow,

U.P. 226013, Telephone no. 0522-2774041

[2] Associate Professor

Department of Home Science

Child Development Discipline, SOCE, IGNOU Delhi.

ABSTRACT

A cyber awareness programme's main goal is to inform individuals about potential online dangers and help them prevent a data breach. No solution, however, can ensure total security from assaults, but it can help lessen their frequency and give end users and experts the knowledge they need to avoid such threats. In the study that has been provided, an effort has been made to understand how cybercrime affects teenagers. There are 60 participants in the study, 30 of whom are males and 30 of whom are girls. In the analysis, percentages and the t test were used. It was determined by evaluation that girls are less aware of cybercrime than boys, indicating a need for awareness among them.

KEYWORD: Cyber crime, girls, boys.

INTRODUCTION

Cybercrime Definition:

Cybercrime is the most recent and conceivably most difficult problem the internet world is currently dealing with. There is no legal definition of "cybercrime" in India. In actuality, the Indian Penal Code never once mentions "cybercrime," even after being amended by the Information Technology (Amendment) Act 2008, sometimes known as the Indian Cyber law. A deliberate attack on information, computer systems, computer programmes, and data that has political motivations and culminates in violence against private property, the government, and the general public is referred to as cyber terrorism. or "acts subject to the penalties of the Information Technology Act." India's Information Technology Act of 2000 deals with the problem of cybercrime. It covers the following topics: electronic commerce, the usage of digital signatures to define various cybercrimes, and economic transactions conducted online. Today, everyone uses websites and e-mail as forms of communication. (2008) (Lane, J., Heus, P., & Mulcahy) It makes it possible for information to be exchanged and disseminated nearly instantly. It includes both unpleasant information and informative and useful content. (2011) (Mishna, F. et al. These have their roots in information technology inventions that, in an effort to improve new economic and social chances, compromise our security and privacy prospects. We are already all connected as humans thanks to information technology. Everyone uses electronics and technology. All social systems are now completely interconnected thanks to the "Internet of Things." For all of these potentially interconnected systems, standards are developing. Life quality is improving thanks to information technology. Automation in infrastructure is increasing. The two main issues are security and privacy. Attacks can be used to cause disruption and unauthorised access. (R. L. Kugler, 2009) In the modern online era of cyber threats, it is challenging to limit a large number of cyber threats and their impact, along with understanding them at the initial stage of the attack. (Hale, C. 2002). Without limiting other definitions by Member States, the United Nations defines 'youth' as people between the ages of 15 and 24 for statistics purposes. Approximately 27.5% of Indians aged 15 to 29 make up the youth population. Online hazards like addiction, cyber bullying, and sexual solicitation are thought to have a harmful impact on young people. It is important to remember that not all youth use technology. (2014) Broad hurst et al. One of the simplest ways to categorise youth is by age group, but not all youth are equally vulnerable, and additional study is required to both identify the youth who are most at risk and to design efficient interventions. (Subrahmanyam, K., & Guan, S. S. A., 2009). Cybercrimes are crimes committed online or through the use of the Internet. These encompass a wide range of prohibited actions. Cybercrime is a catch-all phrase that can be used to gather together a variety of criminal behaviours. Due to the anonymity of the Internet, there are a number of troubling actions taking place in cyberspace that could allow the culprits to engage in a variety of criminal activities that are referred to as cyber crimes. Technology is the tool used in cybercrimes; hence, those who commit them are typically technically adept individuals who have a solid understanding of the Internet and computer programmes. Cyber stalking, cyber terrorism, email spoofing, email bombing, cyber pornography, cyber defamation, etc. are some of the more recent cybercrimes. If a traditional crime is committed using the Internet, it might also be considered a cybercrime. For instance, the IPC, 1860, makes theft, fraud, cheating, mischief, misrepresentation, intimidation, etc. punishable offences. Internet-connected, similar to the neurons in a massive brain. In truth, the internet has been both a blessing and a curse for modern society. Nowadays. Additionally, as the need for the internet grows, the need to protect our data and information has emerged. Whether you own a business, are a frequent internet user, or are both, you should be aware of how to reduce risks, dangers, and cybercrime. You should also be vigilant. Proactive and keep up with online criminals. Because of the development of technology, man now relies entirely on the internet. Man may now easily access everything while seated in one location thanks to the internet. Everything a man can imagine can be done online, including social networking, online shopping, data storage, gaming, online learning, and online employment.

The use of the internet is widespread. The idea of cybercrime emerged along with the rise of the internet and its benefits. Different ways of committing cybercrimes exist. Prior to a few years ago, few people were aware of the crimes that could be committed online. India is not far behind other nations where the rate of cybercrime incidence is also rising daily in terms of cybercrime problems. Based on the most recent official statistics. India has seen a sharp surge in cybercrime cases in 2019 of 63.5%. According to data from the National Crime Record Bureau (NCRB), 44.540 cybercrimes were reported in 2019, up from 28.248 in 2018. Karnataka recorded the most cyber crime cases (12.020), and Uttar Pradesh (11.416) was close behind

(12.020). Among the Union Territories are Telangana (2.001), Assam (2.231), and Maharashtra (4.967). Delhi was the scene of 78% of all cybercrime.

Information Technology Act 2000:

As of right now, there is no statute or law that provides a precise definition of cybercrime. The term "cybercrime is not even included in the IT Act, 2000. However, it is more accurate to define cybercrimes as those types of crimes in which a computer either serves as the target of the crime, the subject of the crime, or even both. Cybercrime encompasses any conduct that makes use of a computer as a tool, target, or means of committing more crimes.

Cybercrime's nature:

The word "cyber" comes from the word "cybernetics," which denotes the study of communication and human and machine control. The new frontier for information and global human communication is cyberspace, which is governed by machines. As a result, crimes committed online must be handled as such. In a broader sense, cybercrime refers to any crime committed online, such as hacking, terrorism, fraud, gambling, cyber stalking, cybercrime, cyber theft, the spread of viruses, etc. Both computer-related and computer-generated crimes are referred to as cybercrimes. The reason there is tension around the world is that it is growing every second. Therefore, law enforcement organisations need to be well-versed in the many types of cybercrime. Although the use of new technologies by crooks is nothing new, we must acknowledge that cybercrime is a considerably new phenomenon in the age of liberalism and globalisation, with global political, social, and economic implications. Cybercrime poses a threat to the socioeconomic, political, and security systems on a national and international level.

Included in Cybercrimes:

E mail bombing: This is a serious offence where someone sends several emails to the target system's or person's mailbox. The space allowed on an email server for the users' emails will typically be filled by mail bombs, which might cause the email server to crash.

Hacking: It is the most serious and hazardous form of internet and e-commerce-related criminality. The act of entering a computer system and stealing important data without authorization is known as hacking. The question of who does hacking now emerges since hackers can fake data and information and are present between client and server. counterfeiting the IP address.

Spreading computer virus: It is a collection of commands with the ability to carry out some destructive actions. Viruses prevent the entire computer system from functioning normally, as well as the system programmes. They can also damage or screw up your system, rendering it useless without an operating system reinstallation. Emails, CDs, pen drives (secondary storage), multimedia, and the Internet can all be used to transmit computer infections.

Phishing: Phishing is the term used to describe the online theft of data such as usernames, passwords, credit card numbers, etc. Phishing is frequently done through instant messaging and email spoofing. In this kind of crime, hackers create a direct link that leads to a phoney page or website that appears and feels exactly like the real one.

Identity theft: Essentially, it is to deceive or trick people into believing they are someone else. In accordance with Section 66-C of the Information Technology (Amendment) Act of 2008, it entails stealing money or obtaining benefits by pretending to be someone else. Identity theft is the illicit or dishonest use of another person's password, electronic signature, or other distinctive aspect of identification. In addition to a possible fine of one lakh rupees, the offender will be punished with imprisonment of either kind for a time that may last up to three years.

Malicious software: These are software or programmes that run through the Internet and are used to interfere with networks. The software is used to break into a system in order to steal confidential data or information or to harm any installed software.

Cyber warfare: It is a war that takes place online and involves politically motivated attacks on computer systems. Among many other possibilities, cyber warfare attacks can take down official websites and networks, interfere with or shut down crucial services, take classified data, and corrupt financial systems.

Domain hijacking: It is the process of altering a domain name's registration without the original registrant's consent.

SMS spoofing: Text message recipients' names or phone numbers can be changed using SMS spoofing.

Voice phishing: The phrase combines the words "voice" and "phishing." To get sensitive, private, and financial information from the general population, voice phishing is used. To obtain information, voice phishing calls a landline number.

Cyber trafficking: It could be human, drug, or weapon trafficking that has a significant negative impact on a huge number of people.

Objective:

- To study level of cyber crime awareness among college going students.
- To study gender difference in level of cybercrime awareness among college going students.

Hypothesis:

- There is no gender difference in level of cybercrime awareness among college going students.

REVIEW OF LITERATURE

Marcum, Higgins, and Ricketts (2010), have shown that more effective policies and procedures may be formed to instruct children and adults about protecting themselves online. Teenagers should be careful who they communicate with online and avoid giving out any personal information to people they do not know and trust. Additionally, further research into youths' bad behaviour on social networking sites and their understanding of deceptive Internet practises will raise awareness of teenagers' online habits and behaviours. With this knowledge, stronger safety procedures and techniques may be developed to protect teenagers online.

In their study, Oksanen and Keipi (2013) examined cybercrime, a significant subject throughout the previous two decades. Cybercrime is more likely to target young societies. In addition to age, additional factors such as gender, education, financial situation, and coercive victimisation are related to being a victim of cybercrime. The use of decent offline social networks helped protect women from online harassment. Younger victims of cybercrime were more likely to worry about future harassment. They demonstrated how important it is to comprehend both psychosocial threat factors in offline interactions and patterns of uncertain online behaviour.

Hamsa S. et. al. (2018), “Study on effect of social networking sites on the young world of cyber crime” Online data transmission, electronic commerce, electronic communication, electronic governance, and mobile communication have all become increasingly commonplace thanks to the internet. Everyone uses them now. The goal of the paper is to comprehend the typical cybercrimes that people encounter and to learn how aware young people are of them. The entire research process is organised and specified in detail. It contains a thorough literature review. The material and data used in this research come from both primary and secondary sources. Privacy seems to be disappearing as all of us become digital citizens in the cyber world and are equipped with data that is available about our whereabouts and activities. Security concerns have a direct

connection to technological challenges. The report presents a conceptual analysis of teenage cybercrime on a broad scale. The majority of the 100 respondents indicated that frequent use of social media can truly result in addiction and adverse repercussions. On the other hand, other respondents thought it was a useful platform. The vast majority of respondents expressed interest in both personal and professional information. It is least preferred for educational purposes. Additionally, people favour entertainment above educational goals. The most well-known social media networking app is WhatsApp, followed in order by Facebook, Instagram, YouTube, and YouTube. The vast majority of respondents are aware of this and refuse any friend requests from strangers. 40% of respondents think it's okay to talk to random people. The majority of respondents, which indicates a very low level of awareness among young people, don't mind revealing sensitive information like their password to family and friends. The majority of young people use social networking sites to make acquaintances of the opposite sex, which can be deceptive and have bad impacts. Because of their parents' fears, the majority of respondents haven't told them anything about the cybercrime they've experienced, which again demonstrates the need to gauge how well-informed people are about the dangers of cybercrime.

Kumar S. et.al. (2015), "Present scenario of cybercrime in India and its preventions" India's internet usage is expanding quickly. It has sparked new opportunities in a variety of industries, including entertainment, business, sports, and education. Every coin has two sides, and the internet is no exception. One of the biggest drawbacks of using the internet is cybercrime, which is a universal truth. We can define cybercrime as any unlawful behaviour carried out over a computer network, particularly the internet. Additionally, cybercrime involves the invasion of privacy or destruction of computer system components like files, web pages, or software. In India, educated individuals conduct the majority of cybercrimes (some of which call for competence). Therefore, an in-depth understanding of cybercrime and its prevention is necessary. Additionally, the majority of crimes committed in India are unintentional or the result of ignorance. In this essay, I've covered a variety of cybercrimes, including those performed out of ignorance or occasionally with malicious purpose. Additionally, I made several recommendations for defences against these illegal actions in daily life.

Swamy D. (2018), "Awareness of cyber crime among teenagers" Cybercrime is any type of criminal activity that uses a computer and the internet to steal, check, or disclose personal or public information. The most recent instance of cybercrime against society is the Blue Whale game. Large numbers of teenagers who committed suicide did so for no apparent reason. News on many forms of cybercrime, such as exam cheating, bank robbery, plagiarism of research papers, etc., can be found in daily newspapers. The IT Act of 2000 was a step taken by the government to combat cybercrime. Finding out whether kids who use the internet are aware of cybercrime was the major goal of the research. For the study, 300 samples were chosen at random from the internet. The researcher conducted some initial studies. The work was finished using Dr. S. Rajasekar's structured questionnaire. Teenagers generally engage in cybercrime without being aware of it. By implementing different policies, there are several strategies to combat cybercrime. Results show that kids who use the internet know less about cybercrime. Even they engage in unknowing cybercrime of some sort.

Agarwal (2015), Criminals are using the internet's convenience and quick internet connection to carry out extensive and varied illicit activities. She argued in her paper that it is now everyone's responsibility to be aware of cybercrime and the laws designed to address it. She has also covered the many forms of cybercrime, which can aid victims in identifying the crime they have fallen victim to.

Parmar and Patel (2016), they deduced from their study that the majority of netizens, whether or not they worked in the IT industry, were unable to actively keep themselves abreast of the most recent information about cyber law and computer security. They believed that among internet users who are not involved in the IT industry, the situation would get even worse. They advised instilling fundamental moral principles in online users while raising understanding of India's cyber regulations. According to Singharavelu and Pillai (2014), B.Ed. students in Tamil Nadu's Perambalur district showed a result that was clearly comparable. Without understanding and awareness of cybercrimes, Singaravelu and Pillai (2014) believed that this condition should not assist them in becoming good teachers.

Mehta and Singh (2013), It was determined that there is a considerable difference between the awareness level of male and female users of internet services when it comes to knowledge of cyber regulations, with male netizens being more knowledgeable than female users. In contrast to the results above, a study on "cybercrime awareness in Malaysia" by Hasan et al. (2015) indicated that female students were more aware of cybercrime and viewed the risk differently than male students.

Aparna and Chauhan (2012), A study on cybercrime awareness in Tricity has shown that raising knowledge of cybercrime might be a useful approach for reducing or preventing cybercrime. To maintain a safe, secure, and reliable computing environment, both the government and internet users are nevertheless liable.

Senthilkumar K. and Easwarwmoorthy S. (2017), "A Survey on cyber security awareness among college students in Tamil Nadu" The study's goal is to examine the degree to which college students in Tamil Nadu are aware of various internet security issues. Cybercrime has become a significant threat to public safety, personal privacy, and national security in recent years. Everyone needs to be aware of their personal security and safety procedures in order to protect themselves from becoming victims of cybercrime. College students' knowledge of cyber security will be examined using a well-structured questionnaire survey method. This study will be implemented in Tamil Nadu's major cities with a focus on various online security concerns, including spam, viruses, phishing, bogus advertisements, pop-up windows, and other intrusions. This poll looks at college students' understanding of security risks and their level of awareness of them, and it offers some solutions. According to the survey's findings, Tamil Nadu's college students are more knowledgeable than the national average about the threats posed by the internet, which can help them defend against cyber attacks. Because fully developed cyber awareness will enable pupils to defend themselves against hackers, awareness must be raised to a higher level.

K. M. mohammad et.al. (2012), "Nature of cyber crime and its impacts on young people: A case from Bangladesh" Cybercrime is a term used throughout the world to describe crimes done online. These days, it is a global issue that causes great concern. The type of cybercrime committed in Bangladesh is described in this essay. Internet-related crime is on the rise in Bangladesh, despite the fact that internet usage there is less widespread than in other wealthy nations. Exploratory in nature, the investigation 30 purposefully chosen respondents were used in a methodological triangulation (face-to-face interview and case study) to acquire pertinent data. The survey found that, while cybercrime is not a big problem in the study area, respondents occasionally become victims of hackers, pornographic websites, and computer viruses online. The vast majority of those in the study region are paying ever more attention to it.

Goel U. (2014), "Awareness among B.ED teacher training towards cyber crime a study" The goal of the current study is to ascertain the level of cybercrime awareness among B.Ed. teacher candidates. A sample of 120 B.Ed. students from the Sonipat area was chosen for this purpose. The information was gathered using the Dr. S. Rajasekar-created Cyber Crime Awareness Scale (CCAS-RS). According to the study, there is no discernible difference between boys and girls in terms of their awareness of cybercrime. There is no discernible difference between rural boys and females in terms of awareness of cybercrime. Urban boys and girls, science and art boys, and science and art girls have quite different perspectives on cybercrime awareness. The findings indicate that while gender, whether male or female, does not significantly influence awareness of cybercrime, both area, whether rural or urban, and stream, whether science or art, do considerably influence awareness.

Begum F. (2019), "Beware of cyber crime with awareness- a review" to raise awareness of the steps that need to be taken to combat cybercrime. The selection criteria led to the retrieval of fifteen articles from internet databases, with papers discussing various forms of cybercrime and countermeasures. The only way to combat cybercrime is through education about the many types of crimes and the steps that can be taken to stop and address them. Cybercrime is still developing, and there are new risks every year. The answer is not to stop using the Internet. Instead, it's critical to recognise cybercrime and comprehend the preventive and management approaches.

P. Martis L. P. and MSH A. (2018), "Cyber crime awareness among youth in Udupi District" The study's goal is to examine youth awareness of cybercrime in the Udupi district. In recent years, cybercrime has become a major problem everywhere. Everyone needs to be aware of cybercrimes and safety precautions in order to avoid becoming a victim of one. A well-structured questionnaire survey method was used to examine youths' knowledge about cybercrime. The sample size for this survey, which was done in the Udupi district, was 300 students. This poll investigates the youth's knowledge of cybercrimes, and some recommendations are made to address these problems. The survey demonstrates that the adolescents in the Udupi district do not have a thorough understanding of cybercrime. When it comes to protecting their laptops and personal computers, there is a glaring lack of awareness. Most users are unaware of crimes besides hacking, such as cyber stalking, mobile hacking, deep web crimes, copyright violations, cyber bullying, phishing, child solicitation and abuse, distributing alarming pornographic content, identity theft, cyber-squatting, etc.

Suryan V.S.K. and B. Sreeya (2019), "Public opinion on cyber crime" Cybercrime, sometimes known as computer-related crime, is criminal activity involving a laptop and a group of people. Only 38% of international organisations claim to be prepared for a sophisticated cyber attack. Cybercrimes are described as "offences that are committed against individuals or groups of individuals with a nefarious motive to intentionally damage the victim's reputation or cause bodily or mental harm, or loss, to the sufferer directly or indirectly, using current telecommunication networks, including the Internet (networks including but no longer limited to chat rooms, emails, message boards, and organisations) and cell phones (Bluetooth, SMS, and MMS)." The analysis is descriptive. 1480 samples are chosen using the convenience sampling approach. We employ independent variables like age, gender, and level of education. The study made use of percentage analysis, chi square, correlation, independent sample t test, and ANOVA.

Mathias P.A.D. and B. Suma (2018), A survey report on cyber crime awareness among graduate and post graduate students of government institutions in Chickmagaluru, Karnataka, India and a subsequent effort to educate them through a seminar" After 2007, when parents, politicians, and academics began to emphasise the importance of educating kids, teenagers, and young adults about internet safety, a greater worldwide awareness of cybercrime emerged. Computers and mobile devices are tools of cybercrime. Youth using these devices at an astonishing pace raises concerns since they may inadvertently commit crimes or become victims. This study seeks to survey undergraduate and graduate students at government institutions using a questionnaire and analyse the data to determine their degree of awareness regarding cybercrime and cyber security. The questionnaire primarily included three topics, including: 1) The fundamental reason for utilising the internet and related issues 2) The degree to which one understands cybercrime; and 3) The kind of education required for comprehending cybercrime and security. 250 students in the 17–21 age range were chosen at random to participate in the survey. 95% of students use their mobile devices to browse the internet, 29.6% download photos and videos, and 36.6% listen to music. 77.5% of internet users use it for social networking. 60% of them intended to learn about cybercrime through seminars, and on average, 50% or more of them had no idea what kinds of cybercrime existed.

Saini H. et.al. (2012), "Cyber crimes and their impacts: a review" The majority of information is now processed online, making it vulnerable to cyber dangers. Cyber dangers abound, and because it is difficult to predict their behaviour in the early stages of an attack, it is also difficult to stop them. Cyber attacks may be carried out purposefully or without any apparent reason. Attacks that are carried out intentionally are regarded as cybercrimes, and they seriously affect society by disrupting the economy, causing psychological problems, endangering national security, and other things. The ability to limit cybercrimes depends on an accurate understanding of their behaviour and the effects they have at different societal levels. As a result, the current article offers a comprehension of cybercrimes and their effects on society, as well as predictions for their future.

RESEARCH GAP:

The crimes related to cybercrime are increasing day by day. Even if crime is happening, people do not know so much about it, especially the youth who are using the internet but they do not know the right way to use it, due to which this problem is becoming more serious. All the previous research has not been as useful as today's new technology is making the youth a victim of cybercrime, so it is absolutely necessary to use the Internet as well as to give information related to it to the youth. In order to protect against cybercrime, there are new ways of cybercrime which include blue whale games or pornography as well as hacking the account of any person, etc. Therefore, in the research presented, the youth can be made aware of the following methods and by giving them appropriate suggestions. Cybercrime is increasing day by day due to which cybercrime attack is affecting modern functions in the society. There is a lot of information about cyber crime, but its reach to rural areas is very less in reach today. Currently, the victims of cyber crime are reaching educated youth because they have all the information related to internet and how to use them. Don't know Youth are the foundation of the society, if the youth is made aware, then our society will become aware on its own, so through this research, it will be tried to get information about what causes and what shortcomings of awareness. Promotes the victim of their cybercrime. Which youngsters need information about cybercrime nowadays.

METHODOLOGY OF THE RESEARCH WORK

This chapter clearly defines the research methods used to conduct the study. The data and information required to address the research objective and questions will be collected, presented and analyzed. To be studied for Pilot study: cyber crime awareness in college going students in KMCL University. The procedure that will be followed in the chapter is described in the following sections.

Type of research: Type of research is emprical research.

Research design: This study is a quantitative method (scale-structured questionnaire), which provides access to quantitative information.

Measurement tools: Cybercrime awareness on a standardized scale by Dr. S.Rajasekar will be used to study cybercrime awareness of youth. The questionnaire contains 36 statements. It will study.

1-To provide information about whether the college in KMCL University has information about cyber crime awareness.

Statistical tools: Data analysis will be performed by using SPSS.

Percentage, Frequency, T- test.

Population: Colleges going students.

Selection of Sample: Sample will consist of a subset of the units or subjects that compose the population. The sample will be around 60 youth within the group of UG enrolled in colleges.

Criteria for sample selection: Samples will be selected with predetermined criteria that youth (30 girls and 30 boys) in the age group of 18-20 can be attained.

Sampling technique: Cyber crime awareness for this study was independent variable. Standardized scale cyber crime awareness by Dr. S. Rajasekar was used to study cyber crime awareness of youth. There were 36 statements in the questionnaire.

Purposive sampling technique will be used.

Dependent variable:

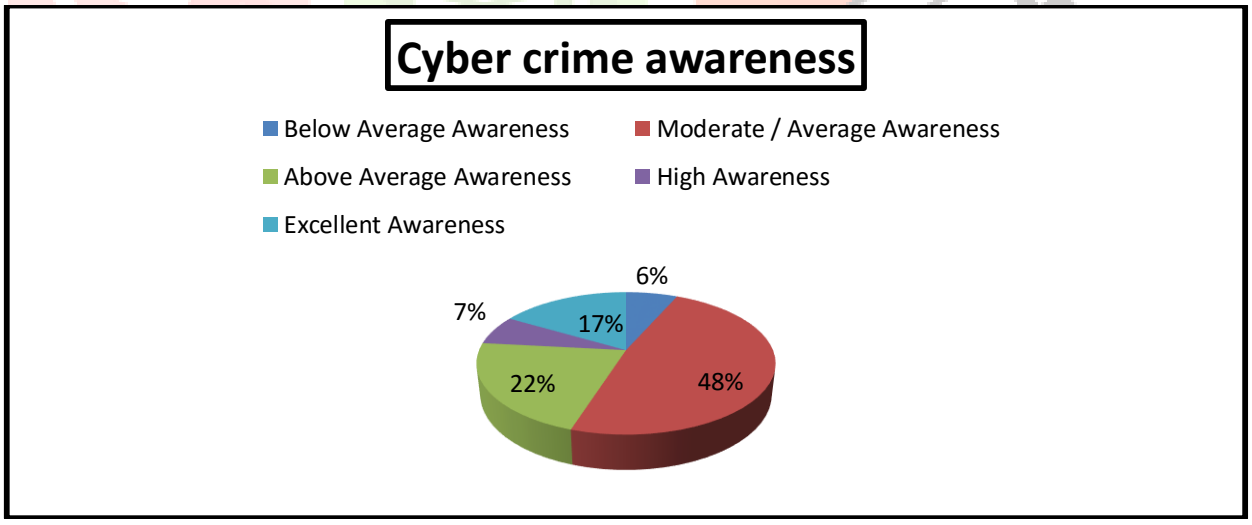
Scale Used: –Cyber crime Awareness Scale (CCAS) by Dr. S. Rajasekar.

Independent variable: Age, Sex/Gender, Rural area, Government College.

Result and discussion

Objective-1 To study level of cyber crime awareness among college going students.

cyber crime awareness					
			Percent	Valid Percent	Cumulative Percent
	Below Average Awareness	4	6.7	6.7	6.7
	Moderate / Average Awareness	29	48.3	48.3	55.0
	Above Average Awareness	13	21.7	21.7	76.7
	High Awareness	4	6.7	6.7	83.3
	Excellent Awareness	10	16.7	16.7	100.0
	Total	60	100.0	100.0	



From the above Cyber crime awareness it was clear that the majority of the youth were moderate/average awareness (48.3%), above average awareness (21.7%), excellent awareness (16.7%), high awareness (6.7 %) and below average awareness (6.7%).

Objective-2 To study gender difference in level of cybercrime awareness among college going students.

T-Test

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
Cyber crime awareness Male	30	4.20	1.215	.222
Cyber crime awareness Female	30	3.37	1.066	.195

One-Sample Test							
	Test Value = 0						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference		Hypothesis
					Lower	Upper	
Cyber crime awareness Male	18.936	29	.000	4.200	3.75	4.65	Rejected/significant
Cyber crime awareness Female	17.295	29	.000	3.367	2.97	3.76	Rejected/significant

CONCLUSION

The presented research concludes that students who attend universities have more cybercrime awareness than students expect. While there are average awareness in the girls. A cyber awareness programme's main goal is to inform individuals about potential online dangers and help them prevent a data breach. No solution, however, can ensure total security from assaults, but it can help lessen their frequency and give end users and experts the knowledge they need to avoid such threats. Training in cyber security awareness aids enterprises in reducing and preventing user risk. People can better appreciate the crucial role they play in preventing cyber attacks at work or at home with the aid of a security awareness programme. Major financial harm from cybercrimes can take many different forms: Businesses may close as a result of security breaches because your clients will no longer trust you as a security brand. Loss of competitive edge, such as if competitors learn about your pricing approach. 1930 is the number for the cybercrime helpline. The appropriate and safe use of information and communication technologies is known as cyber safety. It involves more than just keeping information safe and secure; it also involves handling it responsibly, showing consideration for others online, and following proper "netiquette" (internet etiquette).

REFERENCES

Hamsa S. et. al. (2018), "Study on effect of social networking sites on the young world of cyber crime" Annual Research Journal of SCMS, Pune Vol. 6, ISSN 2348–0661, Symbiosis Centre for Management Studies, Pune Annual Research Journal of Symbiosis Centre for Management Studies.

Lane, J., Heus, P., & Mulcahy, T. (2008), Data Access in a Cyber World: Making Use of Cyberinfrastructure. Trans. Data Privacy, 1(1), 2-16.

Mishna, F., Cook, C., Saini, M., Wu, M. J., & MacFadden, R. (2011), Interventions to prevent and reduce cyber abuse of youth: A systematic review. Research on Social Work Practice, 21(1), 5-14.

Kugler, R. L. (2009), Deterrence of cyber-attacks. Cyberpower and national security, 320.

Hale, C. (2002), Cybercrime: Facts & figures concerning this global dilemma. Crime and Justice International, 18(65), 5-6.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014), An analysis of the nature of groups engaged in cyber-crime.

Guan, S. S. A., & Subrahmanyam, K. (2009), Youth Internet use: risks and opportunities. Current opinion in Psychiatry, 22(4), 351-356.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010), Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. Deviant Behavior, 31(5), 381-410.

Oksanen, A., & Keipi, T. (2013), Young people as victims of crime on the internet: A populationbased study in Finland. Vulnerable children and youth studies, 8(4), 29.

Kumar S. et.al. (2015), "Present scenario of cybercrime in India and its preventions"

International Journal of Scientific & Engineering Research, Volume 6, Issue 4, page-1971 ISSN 2229-5518.

Swamy D. (2018), "Awareness of cyber crime among teenagers" International Journal of Recent Scientific Research Vol. 9, Issue, 5(I), pp. 27073-27075,

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2182.

Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering, August Vol 5, Issue8. https://www.ijarcsse.com/.

Senthilkumar K. and Easwarwmoorthy S. (2017), "A Survey on cyber security awareness among college students in Tamil Nadu" IOP Conf. Series: Materials Science and Engineering 263 (2017) 042043 doi:10.1088/1757-899X/263/4/042043.

K. M. mohammad et.al. (2012), "Nature of cyber crime and its impacts on young people: A case from Bangladesh" Asian Social Science; Vol. 8, No. 15; 2012 ISSN 1911-2017 E-ISSN 1911-2025 Published by Canadian Center of Science and Education, URL: http://dx.doi.org/10.5539/ass.v8n15p171.

Goel U. (2014), "Awareness among B.ED teacher training towards cyber crime a study" Learning Community: 5(2 and 3): 107-117 New Delhi Publishers.DOI Number: 10.5958/2231-458X.2014.00013.X.

Begum F. (2019), "Beware of cyber crime with awareness- a review" International Journal of Science and Healthcare Research Vol.4; Issue: 3; www.ijshr.com, ISSN: 2455-7587.

P. Martis L. P. and MSH A. (2018), "Cyber crime awareness among youth in Udupi District" Vol.-8,ISSN: 2476-1311, J Forensic Sci & Criminal Inves 8(5): JFSCI.MS.ID.555750.

Suryan V.S.K. and B.Sreeya (2019), "Public opinion on cyber crime" International Journal Of Innovative Technology And Exploring Engineering (IJITEE) Issn: 2278-3075, Volume-8 Issue-11.

Mathias P.A.D. and B. Suma (2018), A survey report on cyber crime awareness among graduate and post graduate students of government institutions in Chickmagaluru, Karnataka, India and a subsequent effort to educate them through a seminar" International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 9, Issue 6, pp. 214–228, Article ID: IJARET_09_06_023 http://www.iaeme.com/IJARET/issues.asp, ISSN ISSN Online: 0976-6499.

Saini H. et.al. (2012), "Cyber crimes and their impacts : a review" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, pp.202-209.

http://deity.gov.in/sites/upload_files/dit/files/downloads/ita ct2000/itbill2000.pdf.

https://cybercrimelawyer.wordpress.com/category/ 66c-punishment-for-identity-theft/.