ISSN:2229-6107

INTERNATIONAL JOURNAL OF
PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 14,Issuse 1.Feb 2024

CYBER-SECURITY AWARENESS IN INDIA: HOW MUCH STUDENTS OF HIGHER EDUCATION ARE AWARE

RAVI KIRAN KUMAR TERA 1, J S ARUN PRAKASH 2, BITRA SAI AKASH 3, VEERANKI RAJYA LAKSHMI 4, NIMMALAGARI KUMAR 5,

ABSTRACT The concept and notion of cyber security have become more important nowadays as the Internet has paved every aspect of the daily lives of individuals and organizations. Internet is acting like blood in modern lifestyle and communication systems. Due to the increased use of the Internet, several threats to cyber security have come into existence in the cyber world. The need for cyber security cannot be underestimated due to the continuously evolving technologies of Information and Communication Technology (ICT) and our dependence on the Internet. This research studies cyber security awareness among students of higher education on some primary demographic and educational grounds such as gender, place of residence, level of study, etc. The data for this study was obtained through the Internet by graduates, masters, and research students from many universities and colleges at the national level. The difference was not found in students based on gender and the nature of the course. A significant difference was found in the cyber security awareness on the basis of the residential location and disciplines of the students. Students living in urban areas were found to be more aware of cyber security than students living in rural areas. However, no significant difference was found between them based on the level of study. In conclusion, the results of this study cannot be considered conclusive as a generalization is not possible due to some natural and uncontrolled limitations of research. But nevertheless, the results of observations found in this study may provide some support in the general body of knowledge and future research.

KEYWORDS- Awareness, Cyber-crime, Cyber-security, Higher Education students

1.INTRODUCTION

“We are currently living in an age where the use of the Internet has become second nature to millions of people”. (Kritzinger & von Solms, 2010). Information and Communication Technology (ICT) has penetrated every aspect and domain of our lives. As a result, ICT is providing us with uncountable opportunities and facilities that make human life more comfortable. However, there are some challenges associated with these opportunities and facilities. Cyber security is an idea centered on ensuring that advanced information and resources have a place with people and organizations in the virtual world. (Prasad & Rohokale, 2020; Van Schaik et al., 2017; von Solms & von Solms, 2018). Similarly, Mack (2018) characterized cyber security as the procedures of protecting personal computers and devices in organizations, programming, and information from unapproved access or assaults that point to abuse. Taylor, Fritsch, & Liederbach (2015) broadly defined cybercrimes. Moreover, they quoted cybercrimes as crimes being committed with a computer's help.

ASSISTANT PROFESSOR 1, UG SCHOLAR 2,3,4&5
DEPARTMENT OF CSE, MNR COLLEGE OF ENGINEERING AND TECHNOLOGY, MOHD.SHAPUR, TELANGANA 502285

They further divide these crimes into four categories. The first category of cybercrimes is crimes where computers or networks are the main targets of a crime, such as refusal of service attacks—the second is when computers are used as tools to perform crimes, including fraud and cyber harassment. The third type of crime is one in which computers are used as a product of the crime. Money laundering, for example, might occur with or without computers. The fourth and last category is crimes that occur due to the widespread use of computers. Intellectual property infringement, counterfeiting, and identity theft are all types of cybercrime. Finally, the most well-known digital dangers incorporate malevolent programming (malware) like Viruses, key loggers, and Trojans, and malicious strategies, for example, Phishing and Social Engineering intended to hurt people financially and mentally and to take individual data; here and there, it likewise comes as virus hoax. (Chakraborty, 2019; Erbschloe, 2019; Kara & Aydos, 2019; Prem & Reddy, 2019). Cyber security is characterized as the "capacity to secure or guard the utilization of the internet from cyber-attacks" (CNSS, 2010). Cyber professionals agree that users in any organization unaware of cyber crimes are the weakest link for cyber-attacks. Man (Jourdan, 2007). According to the EDUCAUSE 2015 survey, cyber-security, also known as information security, remains a “strategic importance” concern and is identified as the fourth most significant concern. Because of our developing reliance on advanced hardware and software programs to deal with our regular day-to-day existences, including the transmission and capacity of individual data, cyber security is becoming increasingly important. This digital world offers many benefits but also introduces new threats that are sometimes overlooked. The pace of growth of the Internet exceeded expectations and predictions by early Internet developers. Early Internet developers' hopes and forecasts for the Internet's development were far surpassed (Chouchri, Madnick, and Ferwerda, 2014). Perhaps because of the Internet's sudden rapid development, users are unaware of cyber security issues. Organizations and society did not prepare, develop, and disseminate cyberspace education rapidly enough to keep up with the growing use of cyberspace. As a result, regular Internet/technology users (including current college students, the majority of whom were raised in a cyber-world) are unaware of the threats to their safety and personal details posed by the unsecured use of electronics. According to Kim (2013), heavy users of digital devices are typically the ones who are least educated and aware of cyber security concerns and prevention. While most people are concerned about protecting their physical bodies, property, and space, they are not concerned about protecting their information and property in cyberspace. Students can be considered as most vulnerable internet users to cyber-attacks since they are sometimes sloppy and often irresponsible in their computer use and invest a significant amount of time in it (Aliyu, Abdallah, Lasisi, Diyar & Zeki, 2010). Furthermore, individuals are further exposed to online risks due to their psychological need to stay linked through many mobile devices (Mochiko, 2016). As indicated by a report by Pramod and Raman (2014), higher education students know about security issues around cell phones; however, they are unaware of all security weaknesses and required security rehearses. After finding vulnerabilities in mechanical control frameworks because of clients' unreliable secret critical security, unapplied program fixes, and obsolete or uninstalled against infection and malware protection. Pretorius and Van Niekerk (2015) suggested training and awareness programs. These findings show how there may be inconsistencies in cyber-security perceptions, skills, and behavior. Aliyu et al. (2010) noted that Malaysian college students were critical violators of online ethics and security, as they were reliably crazy when moving digital content and looking. Moreover, they were frequently busy with unlawful use through sharing and downloading of suspicious applications, TV shows, and movies. In addition, the students were found not to be practicing healthy computing for various reasons, including laziness and economic status (Aliyu et al., 2010). Individuals should have sufficient knowledge and skills to maintain personal cyber security to fulfill all of their needs safely and work for different purposes in the virtual world without harm (Furnell & Vasileiou, 2017; Kemper, 2019; Smith & Ali, 2019). At last, it can be said that the capacity to keep up advanced protection in the digital world has become like a sinequanon for anyone with a presence in the virtual environment for various purposes Individuals and organizations seeking unauthorized access to information have arisen as the output of digital data has increased, and the value of information has increased. Because of the rising number of cyber-attacks worldwide, cybercrime will continue to be a significant concern in the coming years, putting about 5.2 trillion dollars in global value at risk. (World Economic Forum, 2019). Even though cyber-security is a significant issue influencing Internet clients in India and globally, this examination plans to investigate the digital protection conduct among Indian Higher education students. This is because of the accompanying reasons: (i) Indians matured 16 to 24 years of age are the most enthusiastic Internet clients; and (ii) Higher education students in India, who are typically matured between 18-25 years of age, have a place with this age classification. As explored by Statista (2020), a study of Internet users daily in India in the year 2020 showed that 73.00% of individuals between the age of 16-24 are Internet clients. Report of Digital 2021 India likewise upheld the way that youthful grown-ups in India are weighty Internet clients. A comparative report moreover itemized that among school-going respondents, over 62.50% were in universities or colleges, 34.90% were in secondary schools, 02.40% were in lower grade schools, and 00.20% were in others. This affirms that higher education students are significant Internet clients, standing apart from students at the secondary and primary levels. This report similarly shows that the amount of Indian young adults getting to the Internet and the total amount of time spent on the Internet is extending rapidly. It might be contemplated that growing Internet usage among this group opens them to digital protection dangers. The present circumstance warrants an examination to investigate the digital protection conduct among Indian higher education students, considered the vulnerable group. As indicated by an investigation directed among higher education students, the participants' digital protection conduct was unsuitable, and a portion of the dangers they confronted could be kept away from if they knew about them (Muniandy, Muniandy & Samsudin, 2017). India's Ministry of Electronics and Information Technology fostered the National Cyber Security Policy in 2013, which is an approach system pointed toward protecting the public and private framework from digital assaults and defending "data, like individual data (of web users), financial and banking data, and sovereign information." This involves utilizing a blend of organizational structures, individuals, frameworks, innovations, and collaboration to get data and data assets on the Internet, foster abilities to dissuade and react to digital assaults, moderate weaknesses, and limit harm from digital frauds. This study aims to examine the cyber-security awareness levels of individuals currently enrolled in higher education. Therefore, this study focuses on the influence of demographic factors, if any, on the cyber-security awareness level and any possible relationships associated with the background of individuals. Due to the recent COVID-19 pandemic, the education system in India is entirely dependent on the Internet; due to this, the subject of cyber security is more important in the context of students. To further investigate the cyber-security awareness level of individuals in an academic setting; this study addresses the following research questions-

1. Is there any difference between cyber-security awareness based on gender?
2. Does cyber-security awareness differ based on their residential location?
3. Is there any difference between cyber-security awareness based on the nature of the courses students studying?
4. Is there any difference between cyber-security awareness based on the student's level of study?
5. Is there any difference between cyber-security awareness based on the discipline of their study?

2. Method & Procedure

Research Design The study used a modified version of the Theory of Planned Behaviour (TPB). Icek Ajzen's TPB framework was judged to be appropriate since it has been used to investigate individuals' ethical behavior and decisions concerning the adoption and compliance with computer security measures (Ifinedo, 2012; Lee & Kozar, 2005; Leonard, Cronan, & Kreie, 2004). As far as the nature of the research design of the present investigation is concerned, it is descriptive research. A quantitative method was adopted in this study because quantitative research in the social sciences refers to the systematic and empirical investigation of quantitative properties and phenomena and their relationships.

Research Method The questionnaire-based survey used in this study is designed to utilize a quantitative methodology to collect data online. The questions were constructed to determine the participant's familiarity with cyber security issues. Students in various colleges and universities were invited to participate in the study. Students were chosen for this study because they use this knowledge regularly and because they represent the future workforce of any company or institution

Population Indian Education System is one of the largest education systems in the world. With 993 universities, 10725 standalone institutions, and 39931 colleges, Indian Higher Education is continuously growing (Statista, 2021). Therefore, all students registered in these institutions were considered the population of the study.

Participants This research was carried out after the lockdown due to COVID-19 when all educational institutions were open. The link to the questionnaire was sent through emails, WhatsApp, and other social media platforms to the students registered in all courses of all levels of Higher Education Institutions. Participants were encouraged to share this link with as many people as possible. Participants were automatically led to details about the study and informed consent after obtaining and clicking the connection. After accepting the survey, they filled in the demographic details. Then a set of several questions appeared sequentially, which the participants were to answer. As it was an online study, participants with access to the internet could participate. A total of 550 dully filled and valid responses were received. There were 299 males and 251 females who filled the online questionnaire. Following is the detail description of the participants-

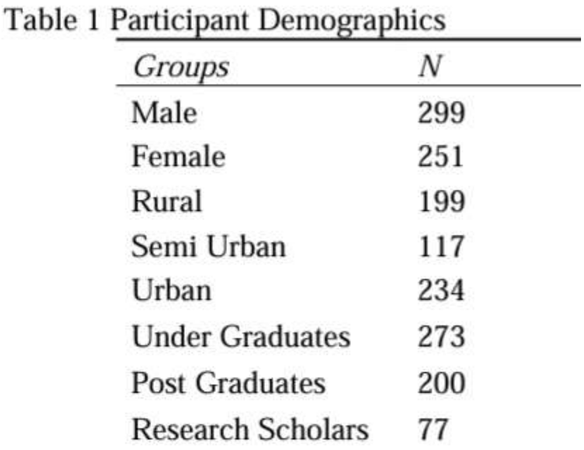

Table 1 Participant Demographics

Groups	*N*
Male	299
Female	251
Rural	199
Semi Urban	117
Urban	234
Under Graduates	273
Post Graduates	200
Research Scholars	77

3.DISCUSSION AND CONCLUSIONS

Even though the study's findings were intriguing, the study had several limitations. Therefore, when evaluating the study's conclusions, it is crucial to consider these limitations: 1. The study's data were constrained by the measurement instruments used. 2. The sample techniques utilized in the research may be regarded as a drawback of the study. Thus, the criterion sampling approach's ability to determine participants was constrained by the selection criteria, whereas the convenience sampling method has limitations in terms of population representation. 3. The research was limited because all participants came from the same educational institution. Based on the results of this study, it can be inferred that there was no significant difference in cyber-security awareness levels between male and female users of internet services and that male students are more aware of cyber-security than their female counterparts. However, there is a substantial difference in cyber-security awareness among the students belonging to different residential locations; it has been discovered that students residing in urban areas are more aware of cyber-security than those in semi-urban and rural locations. It was determined that students of the Law discipline possessed superior personal cyber security skills compared to other disciplines. It could be explained by the correlation between the required skills and their field of study or by the support and incentives provided to faculty members in this department specializing in Cyber-law. Additionally, this discrepancy could be explained by the law students' substantial personal experiences with cyber security in their daily life. (İnam & Öztürk, 2018; Şad & Nalçacı, 2015; Üstündağ, Güneş, & Bahçivan, 2017) Cyber-security is a broad subject becoming more relevant as the environment becomes increasingly interconnected, with networks being used to conduct sensitive transactions. Unfortunately, each new year, cybercrime and information protection diverge in separate directions. Organizations are being challenged not only by how they protect their infrastructure but also by how they need modern systems and resources to do so, thanks to the current and disruptive innovations and the new security techniques and challenges that emerge every day. There is no definitive solution to cybercrime, but we can do all we can to reduce it in order to maintain a safe and stable environment. This study shows that internet users in India are unaware of the current cybercrime and cyber security state. Because of the quick access to the internet, there is an increasing internet addiction in Indian cities. Moreover, smartphones and the internet are becoming increasingly intertwined and common. This means that cybercrime has a broader range of possibilities. Apart from malware, many users are unaware of crimes such as cyber harassment, hacking, online crimes, copyright infringement, cyberbullying, phishing, child solicitation, assault, uploading disturbing pornographic content, identity stealing, and so on. In addition, many internet users are unaware of whom to contact or complain to in the event of a security breach. Awareness activities can be scheduled regularly and spaced out for the year using formal and informal methods. While cyber-security training has had a minor effect on awareness, it is recommended that all students participate in various awareness activities and training before graduating. This would mean that students do not graduate from college with dangerous computer habits. Cyber-attacks remain one of the most severe threats to global security that we face today. Visiting malware-infected websites, responding to phishing e-mails, saving logging information in a third-party location, even exchanging sensitive information on the internet, and exposing personal information to social networking networks are all ways that ordinary people's personal information is stolen. According to the study results, Indian college students have an above-average level of knowledge about cyber-related threats, which can help them defend themselves from cyber-attacks. However, fully developed cyber awareness would allow students to defend themselves from hackers, and thus awareness must be raised to a higher degree.

REFERENCES-

1. Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 InternationalConference,https://www.academia.edu/4613831/Computer_security_and_ethics_awareness_among_IIUM_ students_An_empirical_study

2. Chakraborty, S. (2019). Malware attack and malware analysis: A research. International Journal of Scientific Research in Computer Science, 5(3), 268-272. doi:10.32628/CSEIT195379

3. Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 20(2), 96-121. DOI:10.1080/02681102.2013.836699

4. CNSS. (2010). National Information Assurance (IA) Glossary CNSS Instruction No. 4009. Washington DC: Committee on National Security Systems (CNSS) Glossary Working Group. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

5. Dunkels, E. (2008). ‘Children’s Strategies on the Internet.’ Critical Studies in Education; 49(2), 171-184. https://doi.org/10.1080/17508480802123914