Journal of Network and Information Security
12 (1) 2024, 01-07
http://www.publishingindia.com/jnis

Unveiling Cyber Wellness Awareness: A Study among College Educators

Sanjana Sasankan[1*], Agosh Shaji[2] and Abhishek A. G.[3]
[1]Kristu Jayanti College Autonomous, Bangalore North University, Bangalore, Karnataka, India.
Email: 22mfor21@kristujayanti.com
[2]Kristu Jayanti College Autonomous, Bangalore North University, Bangalore, Karnataka, India.
Email: 22mfor05@kristujayanti.com
[3]Kristu Jayanti College Autonomous, Bangalore North University, Bangalore, Karnataka, India.
Email: 22mfor03@kristujayanti.com
[*]Corresponding Author

Abstract: The importance of cyberspace is acknowledged by almost everyone as a given in daily life. Due to its widespread use, size, and reach, cyberspace has evolved into a vital aspect of our world, changing practically everyone's reality in the developed world and, to a greater extent, that of the developing world. The present Case Study presents the initial findings from a quantitative survey designed to ascertain the level of awareness and excitement among educators at Kristu Jayanti College regarding cybersecurity education. It is imperative that educational institutions teach children about cybersecurity in order to help them use technology safely. Institutions have been working to help instructors learn about cyber safety, and there has been a noticeable increase in interest lately in comprehending the ideas of cybersecurity. 50 instructors from Kristu Jayanti College in Karnataka, India participated in an online survey that was used in this study to determine their degree of knowledge regarding cybersecurity. From the results of the survey, it can be concluded that creating cybersecurity awareness among teachers, especially including various terminologies in cybersecurity and newly implemented cybersecurity laws has great importance. The findings also imply that only a few faculty members could not recognize the significance of cybersecurity and understand the importance of information security principles to apply them in real-world situations as part of their jobs. However, this weakness may be remedied by creating extensive awareness-raising and training programs, in addition to adopting crucial safety protocols across the institution to ensure the security of faculty members. There could be negative effects on IT systems, how they are used, and user privacy in the future if these education and training programs are not adopted. Several important recommendations are put out to address this problem in light of the limitations that were found in this study.

Keywords: Cyberattacks, Cybercrimes, Cybersecurity, Cybersecurity awareness program, Cybersecurity laws, IT Act, Survey.

I. Introduction

Cybersecurity is now a crucial aspect of our everyday lives in today's connected world. We are constantly interacting with the digital world whether we are using social media to connect with friends, shopping online, or checking our emails. Because of the numerous possible hazards that come with being so widespread, it's now common practice to enter our personal information online in order to sell used furniture, join learning sites, or pursue pamphlets and web-based life records crucial to continue implementing strong cybersecurity procedures. As per the Data Security Council of India, India ranks

second globally in terms of cyberattacks, following the United States [1]. This information is based on the Indian Journal of Educational Technology Volume 2 No. 2, July 2020 [2]. Numerous cybercrimes, such as data misuse and privacy invasion, as well as student visits to dangerous websites, have been reported. Because of this, it is crucial to know how to use the internet safely. Cybersecurity is something that must be learned and practiced in order to protect the privacy of our personal information as well as that of instructors and students in learning environments. Cybercriminals frequently use ransomware, emails, social engineering, phishing, fraud, identity theft, online chat forums, and ransomware to target their victims and launch cybersecurity attacks. Since the types, techniques, and instruments of cybersecurity attacks that prey on user weakness are always evolving and growing, the human factor in cybersecurity awareness and management has become more and more important. This means that in order to prevent cyberspace assaults that target human factors and protect information assets, users must be made aware of their duties and obligations through cybersecurity awareness programs. According to research, ignorance of the risk created by breaches in cybersecurity is one of the primary reasons for the increase in internet-related attacks [3]. This research's findings also demonstrate that educators in Karnataka colleges lack a fundamental understanding of cybersecurity laws and that no strategy has been put in place to raise their level of cybersecurity awareness. This study made clear why college educators need to implement a cybersecurity awareness program. Comparable studies were carried out to assess the state of cybersecurity in (1) Malaysia, (2) China, (3) California, and (4) the United States [4]. The findings of all these studies pointed to a lack of appropriate cybersecurity awareness, and a program to raise awareness and reduce successful cyberattacks is required.

Importance of Cybersecurity

Improving employee security awareness is crucial for an organization's cybersecurity efforts. When employees receive high-quality training in cybersecurity, they become better equipped to recognize potential risks and understand the importance of safeguarding personal information. This heightened awareness plays a critical role in establishing robust defence mechanisms against cybercrime. Moreover, comprehensive cybersecurity training fosters a culture of compliance within the company. By ensuring that workers understand and adhere to the organization's data protection policies, the likelihood of security breaches and data leaks is substantially reduced. Having an informed and cooperative staff serves as the frontline defence against online attacks [5]. Cybersecurity training also minimizes liability and reduces potential financial and legal ramifications. A well-trained staff is more likely to react appropriately in case of a data breach. Employees who understand cybersecurity best practices are less likely to break industry standards and data protection legislation, which lowers the possibility of legal issues [6]. Moreover, cybersecurity education increases worker productivity. When employees are aware of their responsibilities for protecting company information, they become more vigilant and efficient in their work. This leads to improved security and operational efficiency, resulting in cost savings and overall productivity gains for the organization [7]. Furthermore, cybersecurity training can boost staff confidence. When employees feel equipped to safeguard sensitive information, their morale and job satisfaction increase. A confident workforce is more likely to deliver optimal performance, foster a positive work environment, and demonstrate loyalty to the company.

In summary, investing in cybersecurity training enhances security, promotes the well-being and productivity of the organization's most valuable asset - its employees, and minimizes the risk of cyberattacks, data breaches, and legal issues.

II. Objectives of the Study

- To find out how knowledgeable college teaching staffs are about cybercrime, cybersecurity, and cybersecurity regulations.
- To investigate how college instructors' awareness of cybersecurity differs depending on their:

- Age
- Gender: both male and female instructors
- Experience in teaching

III. Methodology

A. Research Sampling

For this study, an online questionnaire-based survey is designed utilizing a quantitative methodology to gather data. The questions were designed to find out how aware the targeted participant was about cybersecurity. Teachers at colleges are the participants. College instructors received the survey link from first week of October till it's third week. The questionnaire contained 40 multiple-choice questions about usage frequency, safety protocols, handling cybersecurity threats at schools, internet safety, passwords, cyberattacks, antivirus software, and privacy threats in schools. The survey should take a participant between five and ten minutes to complete. The questions were created with the intention of answering the paper's goal; the main areas of attention include cybersecurity awareness programs, basic cybersecurity knowledge, trust, privacy, and password management. Data was gathered via distributing the questionnaire online [8]. The study employed a questionnaire that was specifically designed to preserve the respondent's anonymities. The need for ethics approval is waived because no records pertaining to the respondents' individual identities or other information were maintained. The survey was conducted using a tablet device that had the questionnaire loaded on it. The results database is built to continuously summarize each person's performance according to several areas. Thus, clear transparency and anonymity are provided by storing a summary of the values rather than the teacher's individual data in any manner. No personal information was requested including name, ethnicity, institution name, or birthdate.

Based on age, the participants were split up into 5 categories:

Category 1: 20–25-year-olds

Category 2: 25–30-year-olds

Category 3: 30–35-years-olds

Category 4: 35–40-years-olds

Category 5: over 40 years of age

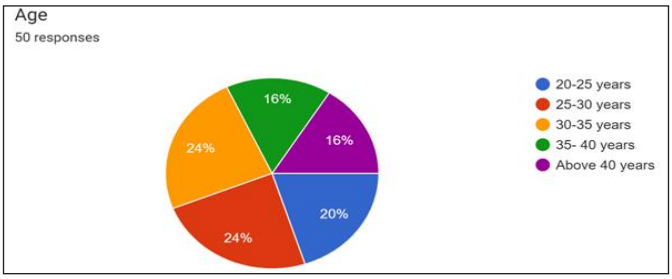

Fig. 1: Age-Group Wise Participation Percentile

Table I: Statistics of Age and Gender-Wise Participation

Age	Male	Female	Total	Ratio
20-25	1	9	10	20%
25-30	1	11	12	24%
30-35	4	8	12	24%
35-40	5	3	8	16%
Above 40	4	4	8	16%

Table I presents a full breakdown of the participants. The majority of participants 24% are from 2 age groups of 25-30 year and 30-35 years, and minority are from age group between 20-25 years and 35-40 years with 16% and the age group above 40 years are with 20% participants. It is crucial for this kind of survey to have a balanced gender participation rate in order to determine the relevance of the questions about gender [10].

There are four sections on four distinct aims in the study questionnaire. Personal data (gender, age, and year of teaching experience) is gathered in the first part [8], [11]. Ten questions about using the internet make up the second segment. Ten questions about cybercrimes and cybersecurity precautions make up the second and third sections. Next, the fourth portion highlighted cybersecurity laws and awareness. To collect quantifiable data, a few of the questions were open-ended. But most of the questions had a yes/no response choice, therefore they were closed. After applying data purification procedures to the collected data, descriptive statistics were extracted.

IV. Internet Usage in Educators

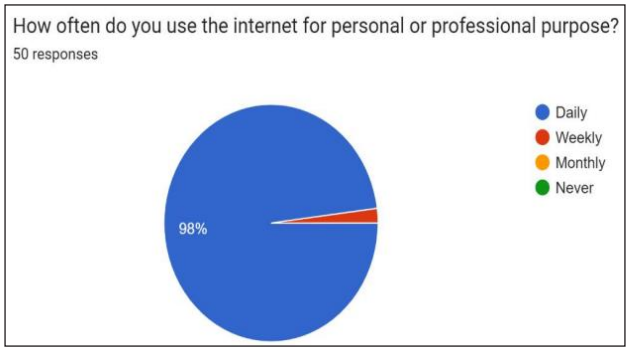

Fig. 2: Percentage of Internet Use by Participants

Due to the widespread usage of the internet in higher education, instructor's today have more chances for both work and learning. Teachers use the internet for both personal and professional purposes. From Fig. 2, the majority 98% of educators use cyberspace on daily basis. Colleges were among the first to employ the technology, and years later, campus adoption of the Internet reached previously unheard-of levels [1].

V. Cybersecurity Awareness in Educators

The answers to a variety of queries about cybersecurity are shown in this section.

A. Knowledge of Terminology Related to Cybersecurity

The purpose of this question was to gauge the participants' general knowledge of cybersecurity concepts. Basic phrases like "online fraud" and hacking" were mixed together with more technical ones like "phishing" and identity theft warning while browsing" in the inquiry. The assessment focused more on term familiarity than comprehensive subject understanding.

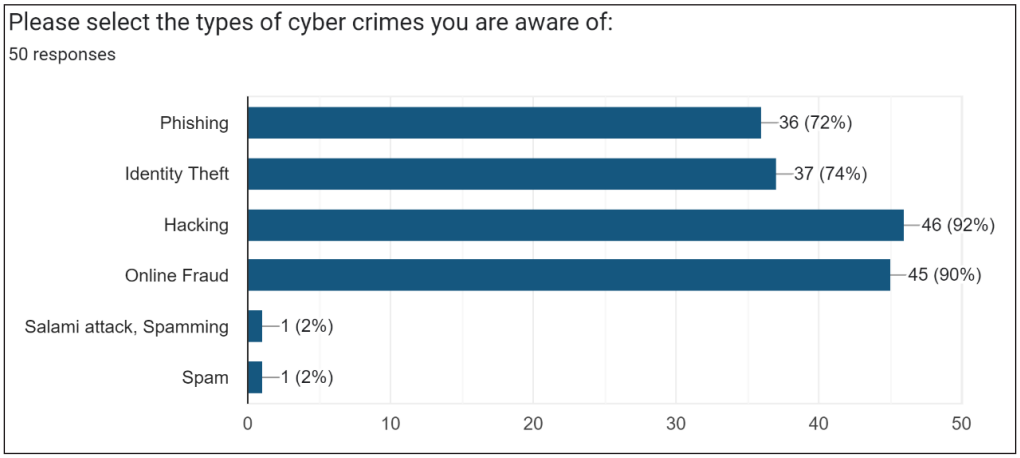

Fig. 3: Graph Depicting Participants' Response to Cybercrime Awareness

Hacking and online fraud were the terms that all age groups knew the most about, followed by identity theft and fishing. The respondents in the 30-35 age group were not quite familiar with phishing and Identity theft only few of them knows the terms. It was intriguing to note that all age groups had relatively minimal awareness of other cyberattacks. This highlights even more the possibility that one should become familiar with other areas of cyberattacks, as they will be one of the main causes of breaches in cybersecurity.

B. Awareness on Cybersecurity Enforcement Agencies

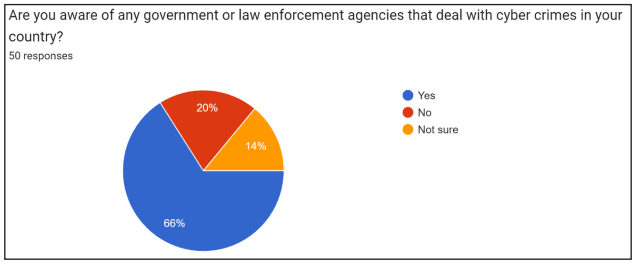

Fig. 4: Awareness Rate of Participants on Cybersecurity Enforcement Agencies

The majority of nations have made cybersecurity a top priority, and some have even established rules for both the public and private sectors. Programmes for training in cybersecurity have been initiated in response to increase the public's understanding of the potential consequences of cyberattacks or breaches. For example, in an attempt to enhance its citizens' long-term cybersecurity mindset, The National Initiative for Cybersecurity Education was established by the US to address workforce structure, professional training, formal education, and awareness [3]. Throughout the entirety of law enforcement responses The Ministry of Public Security (MPS) has taken all necessary steps to address the growing threat of cybercrime under the administration and control of VCP and the Government [8]. To a certain degree, according to the rules in place and according to official information, this section will evaluate the efforts made by law enforcement to three pillar domains to combat cybercrime: task force deployment, prevention, and investigation as well as global affairs [4]. As the (Fig. 3) shows majority 66% of educators are aware of law enforcement agencies that deal with cybercrimes in our country and rest of 20% don't know and 14% were not sure about their information that they have. The level of awareness of law enforcement agencies dealing with cybercrime in India differs from the general public [12]. Some people, especially those with a technical background or a specific interest in cybersecurity, may have a better understanding of these companies. To increase knowledge about the law enforcement agencies coping with cybercrimes in India, it is vital for both authorities and non-government companies to have interaction in public schooling campaigns, workshops, and seminars. These tasks can offer records on a way to file cybercrimes, the function of various companies, and satisfactory practices for online protection and cybersecurity.

C. Awareness on Cybersecurity Measures

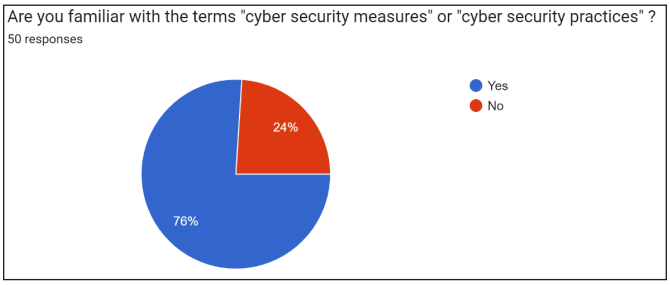

Fig. 5: Percentage of Participants Awareness on Cybersecurity Terms

The evaluation of users' understanding of security concerns and their duties is the third and most important section of this survey. Majority 76% of participants are familiar with the terms "cyber-security measures" or "cybersecurity practices".

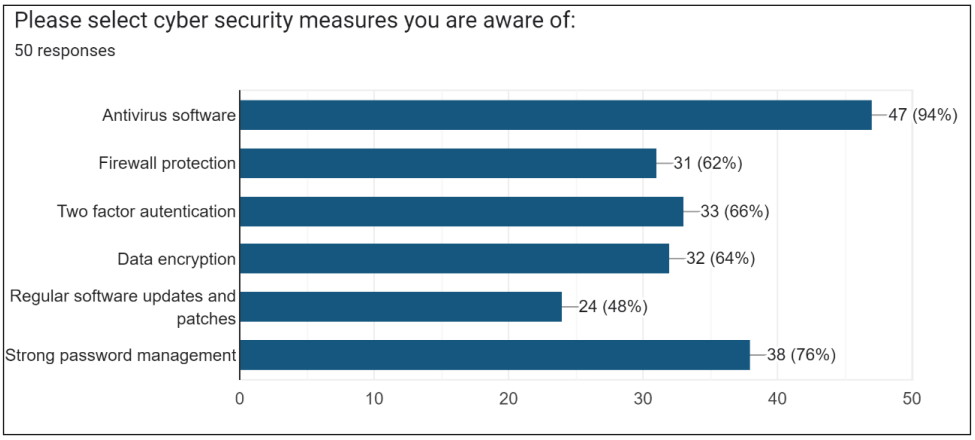

Fig. 6: Awareness Rate of Participants on Cybersecurity Measures

It is clear from the results in Fig. 5 that participants all are aware of several cybersecurity precautions. The majority of internet users know how to set up antivirus software and create secure passwords. Increasing attention of cybersecurity measures among teachers is crucial to safeguarding sensitive

scholar records and promoting a steady getting to know surroundings. Teachers should apprehend the significance of information protection, understand common cyber threats like phishing, and undertake practices which includes robust password control and the use of stable networks [11]. They ought to be educated on safe on-line behaviour and reminded to file any cybersecurity incidents right away. Additionally, they are able to play a role in teaching college students about online safety and responsible digital conduct. Regular expert development, education, and collaboration with educational establishments are vital in preserving instructors knowledgeable about evolving threats and preserving a cybersecurity-aware way of life in the education system.

D. Awareness on Cybersecurity Laws

Given the growing prevalence of technology in the classroom, educators should be well-versed in the legal frameworks governing online gaming, data security, and internet safety [6]. Some educators may only have a limited understanding of these rules or, in certain situations, remain largely oblivious, others may be well-versed in them and aware of their consequences for both themselves and their students [13]. The realization that comes from this research is the most significant and noteworthy result, all participants faculties are aware of The Information Technology Act, 2000 which is one of the most famous cyber protection laws due to its wide scope and relevance to various elements of virtual existence.

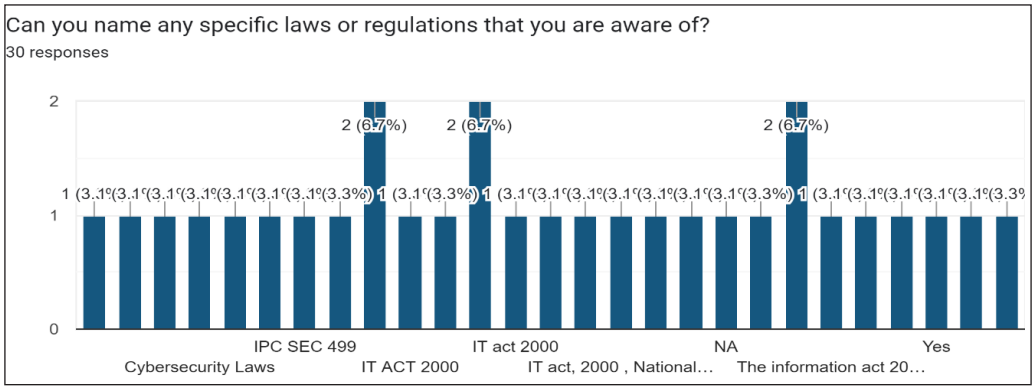

Fig. 7: Graph Depicting Participants' Response to Cybersecurity Laws

Academic institutions must invest in professional development and training programs that address these cybersecurity rules and their practical applications in order to ensure a secure and responsible digital learning environment. Providing teachers with this knowledge is essential for more than just safeguarding sensitive documents [13].

VI. Conclusion and Future Work

This paper presents the findings from a survey that was given to teachers at Kristu Jayanti College in Bengaluru regarding their knowledge of cybersecurity and cybersecurity laws [12]. To find out how aware instructors are right now about cybersecurity, this study offers a questionnaire covering a range of topics. From the results of the survey, it can be concluded that creating cybersecurity awareness among teachers especially including various terminologies in cybersecurity and newly implemented cybersecurity laws has great importance. And the findings also imply that only few faculty members could not recognize the significance of cybersecurity. Also, regularly revisiting subjects and adding continuous awareness initiatives is critical to maintain end-user understanding of cybersecurity best practices. Without reinforcement, the institution would constantly need to rebuild instead of build upon.There are a number of limitations with the results this research presents. The results must be thoroughly analysed, and the important components

must be examined in more depth. This information may also be used to shape the creation of awareness programs for the curriculum and also be a will direct future research on cybersecurity awareness initiatives.

References

[1] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *Int. J. Child-Comput. Interact.*, vol. 30, p. 100343, Dec. 2021, doi: https://doi.org/10.1016/j.ijcci.2021.100343.

[2] P. Mıhcı Türker, and E. Kılıç Çakmak, "An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents," *Comput. Sch.*, vol. 36, no. 4, pp. 293-318, Oct. 2019, doi: https://doi.org/10.1080/07380569.2019.1677433.

[3] Mohd. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, no. 10, Oct. 2021, Art. no. 10, doi: https://doi.org/10.3390/info12100417.

[4] R. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Polic. Int. J. Police Strateg. Manag.*, vol. 29, no. 3, pp. 408-433, Jul. 2006, doi: https://doi.org/10.1108/13639510610684674.

[5] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82-97, Jan. 2022, doi: https://doi.org/10.1080/08874417.2020.1712269.

[6] P. J. Wisniewski, B. P. Knijnenburg, and H. R. Lipford, "Making privacy personal: Profiling social network users to inform privacy education and nudging," *Int. J. Hum.-Comput. Stud.*, vol. 98, pp. 95-108, Feb. 2017, doi: https://doi.org/10.1016/j.ijhcs.2016.09.006.

[7] N. Choucri, S. Madnick, and P. Koepke, 'Institutions for cybersecurity: International responses and data sharing initiatives," in H. Shrobe, D. L. Shrier, and A. Pentland (Eds.), *New Solutions for Cybersecurity*. The MIT Press, 2018, pp. 11-80, doi: https://doi.org/10.7551/mitpress/11636.003.0003.

[8] J. Curtis, and G. Oxburgh "Understanding cybercrime in 'real world' policing and law enforcement," *The Police Journal: Theory, Practice and Principles*, vol. 96, no. 4, pp. 573-592, 2023. Accessed: Oct. 25, 2023. [Online]. Available: https://journals.sagepub.com/doi/epub/10.1177/0032258X221107584

[9] H. Guo, and H. Tinmaz, "A survey on college students' cybersecurity awareness and education from the perspective of China," *J. Educ. Gift. Young Sci.*, vol. 11, no. 3, pp. 351-367, Oct. 2023, doi: https://doi.org/10.17478/jegys.1323423.

[10] R. M. Abdulla, H. A. Faraj, C. O. Abdullah, A. H. Amin, and T. A. Rashid, "Analysis of social engineering awareness among students and lecturers," *IEEE Access*, vol. 11, pp. 101098-101111, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3311708.

[11] D. A. C. Narahari, and V. Shah, "Cyber crime and security – A study on awareness among young Netizens of Anand (Gujarat State, India)," *IJARIIE*, vol. 2, no. 6, 2016.

[12] J. Alemany, E. Del Val, J. Alberola, and A. García-Fornes, "Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms," *Int. J. Hum.-Comput. Stud.*, vol. 129, pp. 27-40, Sep. 2019, doi: https://doi.org/10.1016/j.ijhcs.2019.03.008.

[13] J. Muhirwe, and N. White, "Cybersecurity awareness and practice of next generation corporate technology users," *Issues Inf. Syst.*, vol. 17, no. 2, pp. 183-192, 2016, doi: https://doi.org/10.48009/2_iis_2016_183-192.