IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPARTING THE CYBER SECURITY AWARENESS AMONG THE STUDENT TEACHERS

Author

Mrs. Tamil Selvi P,

Full time Research Scholar,

Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai- 600117.

Co-author

Dr. R. Meenakshi,

Professor in Education,

Vels Institute of Science, technology & Advanced Studies, Pallavaram, Chennai- 600117.

Corresponding author

Dr. K. Sheeba,

Associate Professor in Education,

Vels Institute of Science, technology & Advanced Studies, Pallavaram, Chennai- 600117.

Abstracts

Contemporary technologies, such as web-based learning, mobile learning, and the exploitation of smart boards, are the only means by which the educational process may be made easier in this age of digitalization. Both cyber and security are considered to be components of cybersecurity, which can be understood in two different ways. Information technology that includes computer systems, computer networks, computer software, and data is referred to as cyber. Ensuring the availability, integrity, and confidentiality of data should be the primary focus of any cybersecurity plan. The current investigation utilized a survey method known as normative surveying. As a sample for the research project, the researchers used students from the Education department at Vels College, which is located in the Chennai area. This survey collects information from 77 students, including those who are currently enrolled in Bachelor of Science in Education, Bachelor of Education, and Bachelor of Education programs. There appears to be a significant gap between the qualifications of students and the amount of time they spend online, according to the findings of the current study. The results of the study show that the factors that were selected have a substantial link with one another. In light of the fact that students are the workforce of the future, it is inevitable that the future cybersecurity landscape will be influenced by the digital behaviours and expertise that they currently possess.

Keywords: Cyber security, Cyber security awareness, Social media

INTRODUCTION

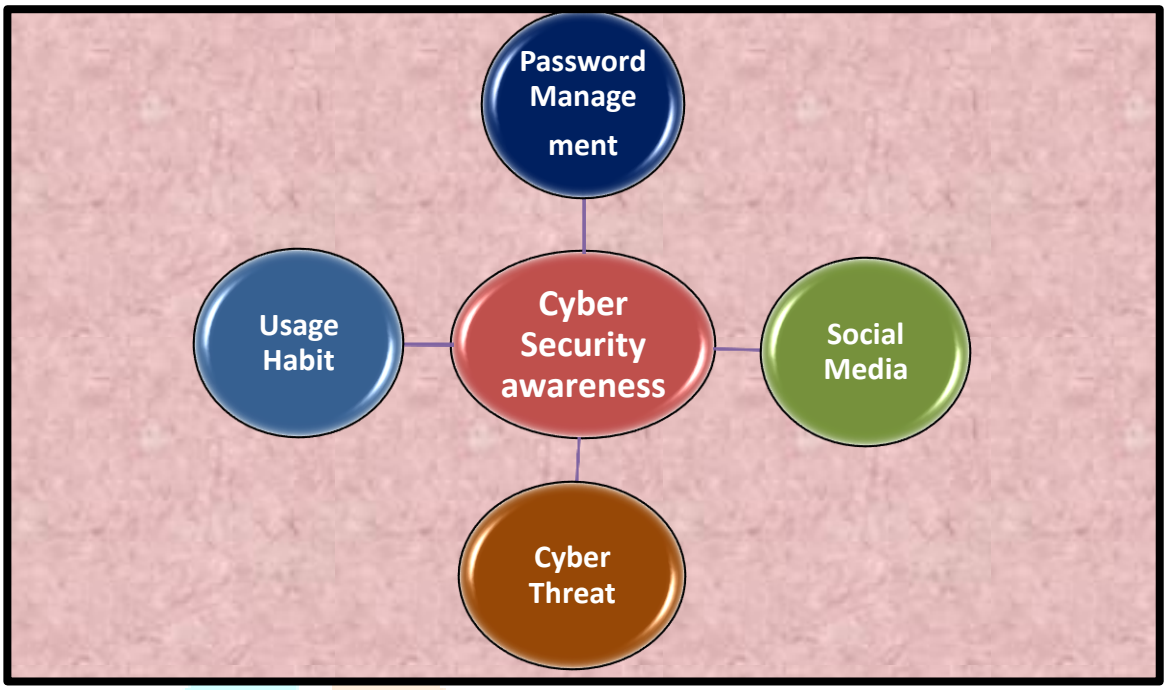
In the digital era, education can solely occur through the utilization of advanced internet-based technologies, including mobile learning, web-based learning, and smart boards for instruction. The internet, being integral to all types of online education, is also susceptible to hacking. Has there been a data breach, rendering security a significant concern? Cybersecurity can be understood through two components: security and cyber. Cyber encompasses systems, networks, programs, and data. Security encompasses information, applications, networks, and system protection. It is occasionally termed information technology security or electronic information security. Contemporary mobile or website users must possess knowledge of social media, password management, usage patterns, cybersecurity, and awareness of cyber threats to effectively counter hacking and associated challenges.

- **Social Media:** It is now possible to communicate ideas and information, including text and photos, through online groups and networks thanks to a type of digital technology called as social media technologies. On social media, user-generated content is frequently visible, and it fosters participation through the use of likes, shares, comments, and conversations when it is shared.

- **Password Management:** With the use of a password management system, users may securely save and recover passwords. Any password can be securely saved in a password manager or web browser. Instead of using the same password for all of your important accounts, which is something you should never do, you can use strong, unique passwords for each one. Password management is a technique that makes it simple, safe, and quick to store passwords and immediately recover them when needed.
- **Usage Habit:** It is imperative that you implement unique passwords for each and every account. Use different passwords for activities linked to work and activities relevant to your personal life. In the event that websites or applications ask you to remember your password, you should respond with a "no." Strong authentication mechanisms, such as multi-factor authentication (MFA), fingerprints, and tokens, should be utilized whenever it is practical to provide them**.**

- **Cyber Threats:** Cybersecurity threats are acts that are carried out by individuals with the intention of stealing data, causing harm, or disrupting computing systems. These actions are carried out by individuals with malicious plans.

- **Cyber Security Awareness:** Cyber awareness refers to the extent of understanding and knowledge that end users possess concerning cybersecurity best practices and the cyber threats facing their networks or enterprises on a regular basis.



REVIEW OF RELATED LITERATURE

Individuals has the autonomy to participate online without fear of compromising their presence. Nevertheless, several unidentified cyber dangers and various types of attack risks are imminent. Their presence, along with personal data, is critically endangered. Moreover, access to cyberspace is limitless and unregulated for individuals of all ages. Neglecting this circumstance will result in the proliferation of unanticipated cybercrimes and intensify current ones. The study by Zahidah Zulkifli et al. (2020) examines the level of cyber security situational awareness among secondary school students, their educators, and their parents in Malaysia. Both physical and digital survey approaches were employed to execute the data collection process. The target groups were categorized into three segments: students (secondary students aged 13 to 16 years), educators, and parents. A unique questionnaire was created for each area. The study included topics pertaining to Internet and digital citizenship knowledge. Participants were selected from certain areas throughout the Klang Valley in Malaysia. The findings reveal that most respondents are aware of the cyber threats and risks linked to cyberspace; nonetheless, only a limited percentage use security measures for online protection. The findings and recommendations from the awareness research are crucial for developing a model that allows secondary school students to understand the security risks and threats associated with the Internet throughout their educational experience. Proactive engagement and awareness will promote the development of sound cyber practices among millennials and their communities in Malaysia.

Cybersecurity is a complex global topic that presents sophisticated socio-technical challenges for both governments and the private sector. The ongoing advancement of technology leads to varied types and frequencies of cyberattacks, affecting individuals in different ways. The majority of recorded cyberattacks can be ascribed to human errors. Research suggests that improving consumers' cybersecurity awareness is one of the most effective defensive tactics, albeit it depends on knowledge and context. However, the intangible attributes, socio-technical interdependencies, continuous technological progress, and ambiguous

consequences hinder the development of effective measures for improving communication and mitigating cyberattacks. Research in the industrial sector focused on creating proprietary cultures that are aware of risk. In academia, where cybersecurity awareness should be integral to an institution's mission to equip graduates with the skills to combat cyberattacks, most research has focused on examining students' attitudes and behaviors after incorporating cybersecurity awareness topics into specific courses within a program. Khader, Karam, and Fares (2021) propose a conceptual Cybersecurity Awareness Framework to aid in the creation of systems designed to improve the cybersecurity awareness of graduates at academic institutions. This framework comprises components designed for the continuous improvement of the development, integration, delivery, and assessment of cybersecurity knowledge inside a university's curriculum across multiple disciplines This framework will consequently enhance awareness among all university graduates, the future workforce. The framework can be used to serve as a blueprint that, when customized by academic institutions to correspond with their missions, guides these institutions in developing or changing their policies and procedures for the design and assessment of cybersecurity awareness.

The subject of cybersecurity has become increasingly important as the Internet infiltrates numerous aspects of everyday life for individuals and organizations. The Internet serves as the essential foundation of modern life and communication systems. The increase in Internet usage has led to many cybersecurity vulnerabilities in the digital domain. The importance of cyber security is critical due to the continuously evolving technologies of Information and Communication Technology (ICT) and our dependence on the Internet. The research conducted by Ravi Kant (2023) investigates cyber security awareness among higher education students, including significant demographic and educational variables such as gender, residence, and field of study. The data for this study was obtained online by graduates, master's students, and researchers from diverse institutions and colleges around the country. No disparities were noted among students for gender and course type. A significant difference in cyber security knowledge was noted according to students' residential areas and fields of study. Students living in urban areas had superior awareness of cybersecurity than those in rural locations. Nevertheless, no significant difference was observed between them regarding the volume of study. In conclusion, the results of this study cannot be considered conclusive, as generalization is impossible due to intrinsic and uncontrolled research limitations. Nevertheless, the results of this study may enhance the current body of knowledge and guide future research endeavors.

PURPOSE OF THE PRESENT STUDY

Students are the workforce of the future; hence, the future cybersecurity landscape will unavoidably be influenced by the digital behaviours and expertise that students currently possess. Consequently, boosting students' cybersecurity understanding is not just an issue of personal safety but also a key strategic requirement for academic institutions, legislators, and the broader cybersecurity community. In order to improve the level of cyber security knowledge existing among college students attending higher education institutions, it is required to implement a cyber security awareness program

Social media is condemned for facilitating hate speech and disinformation, despite the fact that it is widely acknowledged for its ability to promote community. The use of social media is becoming an increasingly important component of the marketing tactics employed by a huge number of businesses. A system that offers a clear and secure manner of storing passwords and retrieving them quickly when necessary is referred to as a password management system. Customers in both home and commercial settings can benefit from the robust cybersecurity and user-friendliness offered by password management systems. When it comes to successfully storing and managing passwords, users should adhere to certain principles and best practices that are included in the realm of password management. The goal of this practice is to protect credentials from being accessed by unauthorized parties and to reduce the risk of cyber risks.

In order to protect internet-enabled devices from threats posed by cybercriminals, cybersecurity functions as a protective measure. The term "cybersecurity awareness" refers to the level of grasp and insight that individuals have regarding the protection of digital systems and data. Recognizing cyber threats, gaining an understanding of the risks associated with them, and putting security policies into action are all required. Each and every occurrence that has the potential to have a negative impact on an asset, such as a loss, a disruption in service, or illegal access, is referred to as a cyber threat.

METHODOLOGY

The approach of normative surveying is utilized for the study that has been developed. The students that participated in the study were those who were enrolled in the education department at Vels Institute. Those who participated in the study were both B.Sc. B.Ed. students and B.Ed. student teachers. With regard to the research project, a sample size of roughly 77 pupils was chosen. Both the researcher and the research supervisor were responsible for the construction of the tool.

RESEARCH QUESTIONS

1. Is there is any significant difference among the qualification of future teachers from B.Sc.B.Ed., and B/Ed., course namely H. Sc, Under Graduate and Post Graduate?
2. Is there is any significant difference among the future teachers from in spending time on online?
3. Is there is any significant relationship among all the selected variables?

ANSWER TO THE RESEARCH QUESTIONS

1. ***Is there is any significant difference among the qualification of future teachers from B.Sc.B.Ed., and B/Ed., course namely H. Sc, Under Graduate and Post Graduate?***

Variable	Qualifications of students						'F' Value	Level of Significance	Groups differed significantly
	H.Sc (N= 24)(1)		UG (N=35)(2)		PG (N= 18)(3)				
	Mean	S.D	Mean	S.D	Mean	S.D			
Social Media	9.50	1.978	10.49	2.331	12.17	1.465	8.751	0.001	(3,1), (3,2)
Password Management	17.04	4.768	19.69	5.057	24.22	4.278	11.596	0.001	(3,1), (3,2)
Usage Habit	16.33	3.409	17.63	2.991	20.33	2.544	9.117	0.001	(3,1), (3,2)
Cyber Threats	8.63	2.499	11.09	3.302	13.44	2.640	14.143	0.001	(1,2),(2,1),(3,1)
Cyber security awareness	17.17	3.964	24.77	6.553	26.17	5.659	17.222	0.001	(3,1), (3,2)

It has been noted that post graduate students outperform the undergraduate and upper secondary pupils in terms of social media, password management, usage habits, cyber threats ad in overall cyber security awareness. It is also noted that they are to be significant at the 1% level.

2. ***Is there is any significant difference among the future teachers from in spending time on online?***

Variable and Dimensions	Spending time on online						'F' Value	Level of Significance	Groups differed significantly
	Below 1 hr (N= 20)(1)		Between1 2hr (N=31)(2)		Above 2hrs (N= 26)(3)				
	Mean	S.D	Mean	S.D	Mean	S.D			
Social Media	9.80	2.142	10.16	2.177	11.65	2.077	5.219	P<0.001	(3,1), (3,2)
Password Management	17.80	3.901	18.55	4.972	23.19	5.586	8.716	0.001	(3,1), (3,2)
Usage Habit	17.00	20555	16.74	2.840	19.85	3.619	8.331	0.001	(3,1),(3,2)
Cyber Threats	9.70	2.904	9.74	2.977	13.12	3.166	10.820	0.001	(3,1), (3,2)
Cyber security awareness	21.40	6.597	23.42	6.597	25.31	6.386	8.017	0.001	(3,1), (3,2)

Students who spend more than two hours on social media, manage their passwords better, have better usage habits, and are more aware of cyber security and hazards than those who spend one to two hours or less. Additionally, they are noted to be significant at the 1% level.

3. Is there is any significant relationship among all the selected variables?

Dimensions	Social Media	Password Management	Usage Habit	Cyber security Awareness	Cyber Threats
Social Media	1	0.642**	0.723**	0.646**	0.387**
Password Management	X	1	0.687**	0.481**	0.701**
Usage Habit	X	X	1	0.468**	0.645**
Cyber Threats	X	X	X	1	0.548**
Cybersecurity Awareness	X	X	X	X	1

The above table provides proof of the positive correlation and statistical significance between the aspects of social media, password management, usage habits, cyber threat and cyber security awareness. Furthermore, their significance at the 1% level is obvious.

CONCLUSION

The results indicate that postgraduate students are familiar with social media, password management, usage habits, cyber security, and cyber dangers. Future teachers spend more time on mobile devices and engage in web-based learning, which allows them to learn about cyber threats and how to defend themselves. Therefore, it is imperative that all students possess an awareness of cyber security. This will enable them to save their data on social media in a secure manner, by managing their passwords properly, and potentially outwit cyber threats.

REFERENCES

Neelima Bhatnagar, Michael Pry (2020). Students Attitudes, Awareness, and Perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Information Systems Education Journal (ISEDJ) volume 18(1) PP :48-58. ISSN:1545-679X

Kodey S. Crandall, Cherie Notebook, Omar EI- Gayar, Kolee Crandall (2019). High School Student's perceptions of cyber security. An explanatory case study. Issues I information Systems. volume 20(3). pp: 74- 82.

Ganesh Talpe (2023). Cyber security Awareness Among College Students. International Research Journal of Modernization in Engineering Technology & Science. Volume: 05(10). e - ISSN:2582-5208.

Khader, M.; Karam, M.; Fares, H.(**2021**) Cybersecurity Awareness Framework for Academia. Information, 12, 417. https://doi.org/ 10.3390/info12100417

Moti Zwilling, Dusan Lesjak, Kukiasz wiechetek, Fatih cetih (2022). Cyber Security Awareness, Knowledge and Behavior: A comparative Study. Journal of Computer Information System. Volume 62(1). PP: 1-16. ISSN: 0887-4417. DOI:10.1080/08874417.2020.1712269.

Ravi Kant(2023), Cyber-Security Awareness In India: How Much Students Of Higher Education Are Aware?, GESJ: Education Science and Psychology 2023 | No.2(67) PP : 59 – 72, ISSN 1512-1801

Zahidah Zulkifli, **Nurul Nuha Abdul Molok**, **Nurul Hayani Abd Rahim**, **Shuhaili Talib (2020),** Cyber Security Awareness Among Secondary School Students in Malaysia, *Journal*

of Information Systems and Digital Technologies, *2*(2), PP - 28–41. https://doi.org/10.31436/jisdt.v2i2.151