# FUTURE TEACHERS AWARENESS IN CYBER SECURITY

**Mrs. Tamil Selvi P,** Full time Research Scholar, Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai- 600117.
**Dr. K. Sheeba,** Associate Professor in Education, Vels Institute of Science, technology & Advanced Studies, Pallavaram, Chennai- 600117.

***Abstracts***

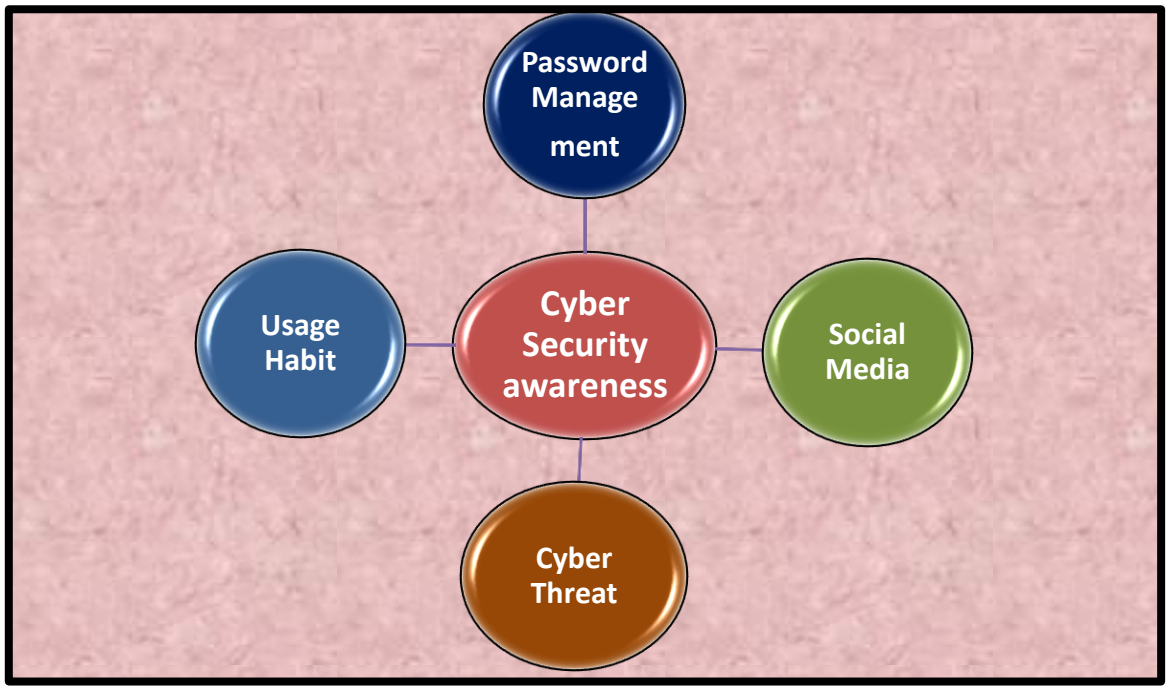
*In the digital age, the educational process is facilitated exclusively through contemporary technologies such as web-based learning, mobile learning, and in the utilization of smart boards. Cybersecurity can be interpreted as comprising two components: cyber and security. Cyber pertains to technology encompassing systems, networks, software, and data. The objective of any cybersecurity plan is to guarantee confidentiality, data integrity, and availability. The current study employed a normative survey method. The study utilized students from the Education department at Vels College in Chennai district as the sample. Data is gathered from 77 students, including those enrolled in B.Sc. B.Ed., and B.Ed. programs, for this study. The results of the current study suggest a considerable disparity in student qualifications and time spent online. The chosen variables in the study exhibit strong correlation with one another. Students represent the future workforce, and hence, the forthcoming cybersecurity landscape will inevitably be influenced by their present digital behaviors and expertise.*

**Keywords**: Cyber security, Cyber security awareness, Social media

## INTRODUCTION

In this digital age, teaching and learning can only take place through the use of cutting-edge internet-based technologies, such as mobile learning, web-based learning, and the use of smart boards for instruction. Because the internet is utilized for all forms of web-based schooling, hacking also takes place. Has there been a breach of the data, making security a major concern? Two components can be used to interpret cybersecurity: security and cyber. Systems, networks, programs, and data are all included in the category of technology known as cyber. Information, apps, networks, and system protection are all included in security. It is sometimes referred to as information technology security or electronic information security. Today's mobile or website user needs to be aware of social media, password management, usage habits, cyber security, and awareness of cyber risks in order to combat hacking and related difficulties.

- **SocialMedia:** Digital technology known as social media makes it possible to share concepts and knowledge—including text and images—through online groups and networks. User-generated material is frequently seen on social media, and it encourages interaction through likes, shares, comments, and discussions.
- **Password Management:** Users can safely save and retrieve passwords with the help of a password management system. All passwords can be safely stored in a web browser or password manager. This enables you to use strong, different passwords for every significant account (instead of having the same password for all of them, which is something you should never do). A method that makes it easy and secure to store passwords and retrieve them quickly when needed is known as password management.
- **Usage Habit:** Make sure you use distinct passwords for every account. For work-related and personal activities, use distinct passwords. When websites or apps request that you remember your password, click "no." When feasible, employ strong authentication methods like multi-factor authentication (MFA), fingerprints, and tokens.
- **Cyber Threats:** Cybersecurity threats are actions executed by individuals with malicious intent, aimed at data theft, inflicting damage, or disrupting computing systems.
- **Cyber Security Awareness:** Cyber awareness denotes the degree of comprehension and knowledge that end users has regarding cybersecurity best practices and the cyber hazards confronting their networks or businesses daily.




**REVIEWOFRELATEDLITERATURE**

Individuals have the autonomy to engage online without concern for the jeopardization of their presence. Nonetheless, several unidentified cyber hazards and diverse sorts of assault threats loom ahead. Their presence, along with personal data, is perilously at risk. Furthermore, access to cyberspace is boundless and uncontrolled for all age groups. If this condition is disregarded, it will lead to the emergence of unforeseen cybercrimes and exacerbate existing ones. The research conducted by **ZahidahZulkifli et al. (2020)** investigates the degree of cyber security situational awareness among secondary school pupils, their teachers, and their parents in Malaysia. Both physical and online survey methodologies were utilized to conduct the data collection process. The target groups were classified into three categories: students (secondary students aged 13 to 16 years), teachers, and parents. A distinct questionnaire set was developed for each category. The survey encompassed themes related to Internet and digital citizenship knowledge. Participants were chosen from specific regions within the Klang Valley in Malaysia. The results indicate that the majority of respondents are cognizant of the cyber hazards and risks associated with cyberspace; nonetheless, only a small number use security measures for online safety. The results and suggestions from the awareness study are essential for creating a model that enables secondary school pupils to comprehend the security dangers and threats linked to the Internet during their academic tenure. Proactive exposure and knowledge will facilitate the establishment of good cyber habits among millennials and their surroundings in Malaysia.

Cybersecurity is a complicated worldwide issue that poses intricate socio-technical challenges for both governments and the business sector. The continuous evolution of technology results in diverse forms and frequencies of cyberattacks, impacting various people in distinct manners. The preponderance of documented cyberattacks can be attributed to human errors. Although contingent upon knowledge and surroundings, research indicates that enhancing users' cybersecurity awareness is among the most effective defensive strategies. Nonetheless, the intangible characteristics, socio-technical interdependencies, perpetual technological advancements, and unclear repercussions complicate the formulation of effective strategies for enhancing communication and countering cyberattacks. Research in the industrial sector concentrated on developing proprietary cultures that are cognizant of risk. Conversely, in academia, where cybersecurity awareness ought to be central to an institution's mission to prepare graduates with the skills to counter cyberattacks, the majority of research has concentrated on analyzing students' attitudes and behaviors following the integration of cybersecurity awareness topics into select courses within a program. **Khader, Karam, and Fares (2021)** present a conceptual Cybersecurity Awareness Framework to facilitate the development of systems aimed at enhancing the cybersecurity awareness of graduates in academic institutions. This framework consists of components aimed at the ongoing enhancement of the development, integration, delivery, and evaluation of cybersecurity knowledge within a university's curriculum across various disciplines and

majors; consequently, this framework will foster greater awareness among all university graduates, the future workforce. The framework can be modified to function as a blueprint that, when tailored by academic institutions to align with their missions, directs these institutions in formulating or revising their policies and procedures for the design and evaluation of cybersecurity awareness.

The topic of cybersecurity has gained significance as the Internet permeates many facets of daily life for individuals and organizations. The Internet functions as the lifeblood of contemporary lifestyle and communication networks. The proliferation of Internet usage has given rise to numerous risks to cybersecurity in the digital realm. The necessity of cyber security is paramount, given the incessantly advancing technologies of Information and Communication Technology (ICT) and our reliance on the Internet. The research study by **Ravi Kant (2023)**examines cyber security awareness among higher education students based on major demographic and educational factors, including gender, residence, and degree of study. The data for this study was acquired via the Internet by graduates, master's students, and researchers from various institutions and colleges nationwide. No differences were observed among students for gender and course type. A notable disparity was observed in cyber security awareness based on students' living locations and academic specialties. Students residing in metropolitan regions had greater awareness of cybersecurity compared to their rural counterparts. Nonetheless, no substantial difference was identified between them about the amount of study. In conclusion, the findings of this study cannot be deemed definitive, as generalization is unattainable due to inherent and uncontrolled research constraints. Nonetheless, the findings from this study may contribute to the existing body of knowledge and inform future research.

## PURPOSEOFTHEPRESENT STUDY

Students represent the future workforce, and hence, the future cybersecurity landscape will inevitably be influenced by their present digital practices and expertise. Consequently, enhancing students' cybersecurity understanding is not merely a matter of personal safety but also a vital strategic need for academic institutions, policymakers, and the broader cybersecurity community.A cyber security awareness program is necessary to enhance cyber security knowledge amongcollege students at higher education institutions.

Social media is recognized for fostering community yet criticized for enabling disinformation and hate speech. Social media is becoming an increasingly vital component of numerous companies' marketing strategies. Password management is a system that enables a straightforward and secure method for storing passwords and retrieving them swiftly when necessary. Password management systems provide strong cybersecurity and simplicity for both residential and business customers. Password management encompasses concepts and best practices that users should adhere to while storing and managing passwords effectively, aiming to safeguard them against unauthorized access and mitigate cyber hazards.

Cybersecurity serves as a protective measure for internet-enabled devices against cybercriminals. Cybersecurity awareness refers to the comprehension and insight individuals possess regarding the safeguarding of digital systems and data. It entails identifying cyber dangers, comprehending related risks, and implementing secure practices. Cyber threats refer to any incident that may adversely impact an asset, such as loss, disruption of service, or unauthorized access.

## METHODOLOGY

For the prepared study, the normative survey method is used. The study's participants were the education department's students at Vels Institute. The study included both B.Sc. B. Ed. and B. Ed. student teachers. For the study, a population of approximately 77 students was selected. The tool was constructed by theresearcher and the research supervisor.

## RESEARCHQUESTIONS

1. Is there is any significant difference among the qualification of future teachers from B.Sc.B.Ed., and B/Ed., course namelyH.Sc, Under Graduateand PostGraduate?
2. Is there isanysignificant differenceamongthe future teachersfrominspendingtime ononline?
3. Is thereisanysignificantrelationshipamongalltheselectedvariables?

**ANSWERTOTHERESEARCHQUESTIONS**

***1. Is there isanysignificantdifferenceamongthequalificationof future teachers from B.Sc.B.Ed., and B/Ed., course namelyH.Sc, Under Graduateand PostGraduate?***

| Variable | Qualificationsofstudents | | | | | | 'F' Value | Level of Significance | Groupsdifferedsignificantly |
|---|---|---|---|---|---|---|---|---|---|
| | H.Sc (N=24)(1) | | UG (N=35)(2) | | PG (N=18)(3) | | | | |
| | Mean | S.D | Mean | S.D | Mean | S.D | | | |
| SocialMedia | 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) |
| UsageHabit | 16.33 | 3.409 | 17.63 | 2.991 | 20.33 | 2.544 | 9.117 | 0.001 | (3,1),(3,2) |
| CyberThreats | 8.63 | 2.499 | 11.09 | 3.302 | 13.44 | 2.640 | 14.143 | 0.001 | (1,2),(2,1),(3,1) |
| Cybersecurity 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,cyberthreats ad in overall cyber security awareness. It is also noted that they are to be significant at the 1% level.

***2. Is there isanysignificant differenceamongthe future teachers frominspendingtime ononline?***

| Variable andDimensions | Spendingtime ononline | | | | | | 'F' Value | Level ofSignificance | Groups differedsignificantly |
|---|---|---|---|---|---|---|---|---|---|
| | Below1 hr (N=20)(1) | | Between12hr (N=31)(2) | | Above 2hrs (N=26)(3) | | | | |
| | Mean | S.D | Mean | S.D | Mean | S.D | | | |
| SocialMedia | 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) |
| UsageHabit | 17.00 | 20555 | 16.74 | 2.840 | 19.85 | 3.619 | 8.331 | 0.001 | (3,1),(3,2) |
| CyberThreats | 9.70 | 2.904 | 9.74 | 2.977 | 13.12 | 3.166 | 10.820 | 0.001 | (3,1), (3,2) |
| Cybersecurity 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 thereisanysignificantrelationshipamongalltheselectedvariables?***

| **Dimensions** | **Social Media** | **Password Management** | **Usage Habit** | **Cybersecurity Awareness** | **Cyber Threats** |
|---|---|---|---|---|---|
| **SocialMedia** | 1 | 0.642** | 0.723** | 0.646** | 0.387** |
| **Password Management** | X | 1 | 0.687** | 0.481** | 0.701** |
| **UsageHabit** | X | X | 1 | 0.468** | 0.645** |
| **CyberThreats** | 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**

NeelimaBhatnagar,MichaelPry(2020).StudentsAttitudes,Awareness,andPerceptionsofpersonalprivacyandcybersecurity in the use of social media: An initial study. Information Systems Education Journal(ISEDJ) volume18(1) PP :48-58. ISSN:1545-679X

Kodey S. Crandall, Cherie Notebook, Omar EI- Gayar, Kolee Crandall(2019). High School Student's perceptions of cybersecurity.Anexplanatorycasestudy. Issues IinformationSystems.volume20(3).pp:74- 82.

Ganesh Talpe (2023). Cyber security Awareness Among College Students. International Research Journal of Modernizationin EngineeringTechnology&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, DusanLesjak, Kukiaszwiechetek, Fatihcetih (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

ZahidahZulkifli, 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