International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Hygiene, Password Management and Cyber Security of Future Teachers

Mrs. Tamil Selvi P[1], Dr. R. Meenakshi[2], Dr. K. Sheeba[3]

[1]Full time Research Scholar, Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai- 600117.
[2]Professor in Education, Vels Institute of Science, technology & Advanced Studies, Pallavaram, Chennai- 600117.
[3]Associate Professor, Vels Institute of Science, technology & Advanced Studies, Pallavaram, Chennai-600117.

ABSTRACTS

In this digital era, online learning, mobile learning, and the utilization of smart boards are all examples of the cutting edge technology that have revolutionized education in the modern digital age. Today citizen both the students and teachers are using the social media for teaching and learning process. Hence the investigator felt that to study about the cyber hygiene, password management and cyber security of the student teachers from B.Ed., and B.Sc.B.Ed., course. Data is collected form the 90 student teachers, including those pursuing B.Sc., B.Ed., and B.Ed. degrees. The data were calculated using the SPSS package. The findings revealed that there is significant difference between the type of social media, gender and course with respect to cyber hygiene, password management and cyber security. Further is also revealed that there is a positive and significant relationship among the variables such as cyber hygiene, password management and cyber security.

Keywords: Cyber security, Cyber hygiene, Password Management and Student Teachers

INTRODUCTION

Instruction and acquisition of knowledge in the contemporary digital age necessitate the utilization of advanced internet-based technologies, encompassing mobile learning, web-based education, and the application of smart boards in pedagogy. Given that numerous forms of online education utilize the internet, hacking is also prevalent. Has the data been hacked, rendering security a primary concern? Cybersecurity can be comprehended through the examination of two components: security and cyber. Cyber pertains to systems, networks, initiatives, and data, among other technological concepts. Security encompasses the protection of information, tools, networks, and systems. It is often referred to as electronic information security or information technology security. To combat hacking and associated challenges, contemporary smartphone or website users must possess knowledge of social media, password management, usage patterns, cybersecurity, and cyber risk awareness.

Cyber Hygiene: Cyber hygiene is frequently likened to personal cleanliness. Similar to how an individual adopts personal hygiene activities to sustain health and well-being, cyber hygiene measures can safeguard and secure data. This facilitates the maintenance of correctly working devices by safeguarding them from external threats, such as malware, which might impede functionality. Cyber hygiene pertains to the

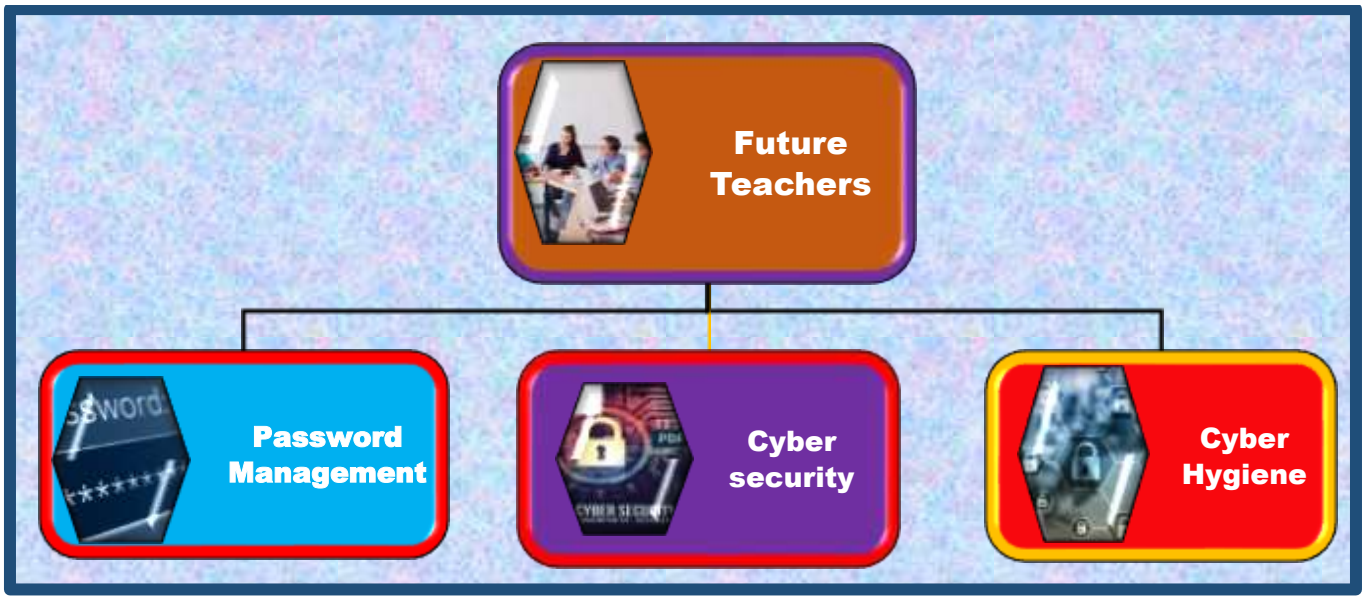
procedures and precautions employed by users to maintain sensitive data in an orderly, safe, and secure manner against theft and external threats.

Cyber hygiene encompasses the practices and measures employed by users of computers and other devices to preserve system integrity and enhance online security. These techniques are frequently incorporated into a regimen to safeguard users' identities and other information that may be compromised or corrupted. Similar to physical cleanliness, cyber hygiene is routinely practiced to prevent natural degradation and prevalent dangers.

Password Management: Users can safely save and retrieve passwords with the help of a password management system. All passwords can be securely stored in a password manager or web browser. This enables us to use strong, unique passwords for each of our essential accounts rather than using the same password for all of them, which is something you should never do. The method that allows for easy, secure password storage and quick access when needed is known as password management.

Cyber Security: The implementation of measures to protect computers, servers, mobile devices, electronic systems, networks, and data against hostile attacks is what we mean when we talk about cyber security. Alternatively, it may also be referred to as electronic information security or information technology security. The phrase "cybersecurity" can be applied in a wide range of settings, from the realm of business to that of mobile computing, and it can be placed into a few categories that are generally accepted.

Diagrammatic representation of Cyber Hygiene and Password Management is needed for Cyber Security



A significant number of people in today's society, including students, teachers, and other elements of society, have profiles on various social media platforms. Because of these social media platforms, the activities that users engage in on a daily basis are strongly impacted by all of the categories of users. On occasion, the social media profiles of individuals may be utilized in order to fool them and gain the personal information required to identify them. Through the use of social media platforms, both educators and students are increasingly engaging in communication and interaction with one another. This analysis, which evaluated the manner in which prospective educators employ their computers and mobile devices

for the purpose of teaching and learning, raises concerns regarding privacy and cyber security in the context of social media utilization. Specifically, the investigation focuses on how these individuals use social media.

The word "social media" is used to refer to the process of creating, sharing, and/or exchanging ideas and information within online communities and networks. This process encompasses a wide range of activities forms of interaction. Password administration involves the management and safeguarding of passwords from their inception to their termination, following a series of sustainable procedures. This is achieved by utilizing password managers, which have secured repositories for the storage of sensitive credentials. The password is a crucial element of security that protects data and information while providing access to authenticated systems. Passwords should be a minimum of 12 characters long, incorporate both uppercase and lowercase letters, and contain at least one symbol or special character. The inquiry examines the extent to which prospective instructors comprehend the principles of password security and their management of credentials.

REVIEW OF LITERATURE

People don't have to worry about their safety when engaging in online activities. However, there are still many unidentified cyber threats and attack kinds. Their presence and personal data are in significant danger. Additionally, there are no age restrictions and cyberspace is available to people of all ages. Ignoring this problem will lead to the emergence of new cybercrimes and the escalation of current ones. The degree of cyber security situational awareness among Malaysian parents, educators, and secondary school students is examined in this study by **ZahidahZulkifli et al. (2020).** Both online and offline survey approaches were used in the data collection process. The three primary groups of interest were students (here defined as secondary school students between the ages of 13 and 16), teachers, and guardians. A distinct set of questionnaires was developed for every category. The study covered topics such as digital citizenship and Internet familiarity. Participants were chosen by hand from the Malaysian Klang Valley. Although most respondents are aware of the risks and threats associated with cyberspace, very few really take precautions to keep themselves safe when using the internet.

The awareness study's conclusions and suggestions are essential for creating a model that aids secondary school pupils in comprehending the dangers and risks associated with Internet security while they are in class. Proactive education and awareness programs targeted at promoting positive internet behaviors can benefit Malaysian millennials and their communities. Cybersecurity is a global topic that presents complicated sociotechnical challenges for both organizations and governments. Because technology is always evolving, cyberattacks can take many various forms, occur at different rates, and affect different individuals. The great majority of alleged cyberattacks are the result of human error. Increasing consumers' understanding of cybersecurity is one of the best defensive strategies, according to research, but this depends on their level of experience and the context. Intangible characteristics, socio-technical interdependencies, ongoing technological advancements, and unpredictable consequences make it challenging to develop effective solutions for enhancing communication and preventing cyberattacks.

The development of risk-aware proprietary cultures has been the focus of business research. Conversely, while cybersecurity awareness should be at the core of any school's mission to prepare its graduates to protect against cyberattacks, the majority of scholarly research has concentrated on how students' attitudes and behaviors change after specific programs cover this topic. **Khader, Karam, and Fares (2021)** provide a conceptual Cybersecurity Awareness Framework to aid in the development of systems to increase

college graduates' awareness of cybersecurity. This framework's components are intended to enhance cybersecurity knowledge generation, integration, delivery, and evaluation across a university's curriculum and academic program majors; consequently, this structure will motivate all recent college graduates who will soon be joining the workforce to be more aware. By tailoring the framework to their particular goals, academic institutions can utilize it as a guide to develop or update current cybersecurity awareness design and evaluation policies and procedures.

In light of the fact that the Internet is becoming increasingly intertwined into the day-to-day lives of individuals and businesses, cybersecurity has become an increasingly significant concern. The Internet is essential to the functioning of modern communication and lifestyle networks, which would not be possible without it. As the number of people using the internet continues to rise, there has been an increase in the number of cybersecurity risks that are present in the digital realm. Because our lives are becoming more and more dependent on the Internet, and because information and communication technology is continuously advancing, cybersecurity is of the utmost importance. The research study conducted by **Ravi Kant (2023)** examines the level of cyber security knowledge among college students by taking into account factors such as gender, place of residence, and level of education. Researchers, master's students, and graduates from a wide variety of universities in the United States contributed to the data collection that was used in this analysis through the usage of the internet. Students were not discriminated according to gender or the sort of course they were taking. Students' levels of awareness regarding cyber security differed greatly depending on the academic major they were pursuing and the region in which they were located. The level of cybersecurity awareness displayed by pupils who lived in urban regions was significantly higher when compared to their counterparts who lived in rural areas. When it comes to the amount of research that was conducted, however, there was no noticeable difference between the two institutions. Generalization is not possible because of the inherent and uncontrolled research limitations; hence, the findings of this study cannot be deemed conclusive without further investigation. In spite of this, the findings of this study have the potential to direct subsequent investigations and contribute to the existing body of knowledge.

PURPOSE OF THE STUDY

When it comes to assisting their students with their homework as well as extracurricular activities, instructors have a lot on their plates in this day and age of digital technology. As a result of the rapid growth of technology, it is now invading every aspect of our life, including the field of mental health. This pertains to both the students and the teachers, and it is connected with the administration of the classroom and the learning objectives. In spite of the increasing use of social media for educational and recreational purposes, there has been an increase in the number of cybercrime incidents, with schools being a regular target for assaults that target both kids and teachers. Since this is the case, it is imperative that the existing student instructors have a solid understanding of cybersecurity awareness. Educating kids about cybercrime and other online threats, as well as assisting them in using social media applications that incorporate additional safety precautions, is a component of this. Students will have a greater sense of safety when using the internet and social media if we emphasize the need of adopting passwords that are difficult to guess.

Due to the fact that students will be the workforce of the future, the current cybersecurity landscape will surely be impacted by the digital habits and understanding of students. As a consequence of this, it is of the utmost importance for the community of cybersecurity professionals, educational institutions, and

aspiring educators to increase awareness about the significance of learning cybersecurity in the classroom. Students in higher education who are majoring in education would gain a great deal from participating in a cyber security program that is designed to deepen their understanding of the subject matter. In contrast to what one may initially believe, there are straightforward cybersecurity topics that can be taught in a classroom setting. Providing children with instruction on cybersecurity is the first step in encouraging the development of online habits that are responsible and safe for them to use.

By "social media," we are referring to the numerous online communities and networks that allow individuals to meet, communicate with one another, and cultivate relationships via the exchange of information and ideas. It is important for future educators to be aware of the potential adverse impacts that social media applications may have on their students when they are working with them in their educational field of internship. When it comes to studying, it is imperative that students make proper use of these applications. The process of systematically applying long-term solutions to secure and manage passwords for social media platforms is collectively referred to as password management. This process begins with the generation of passwords and concludes with the deletion of passwords.

The utilization of integrated encrypted vaults for the storage of essential credentials can make this process easier to accomplish. To gain access to particular places or systems, potential instructors are need to be familiar with passwords, which can be words, phrases, or codes that are kept secret. Before a computer or computer system can be used, a password is a set of instructions that must be entered. This is the most technical definition of the term "password." In order to secure themselves, their data, and their devices, every educator and student who utilizes technology, particularly smartphones, needs to be informed of the most typical sorts of fraudulent and illegal behavior, as well as the ways in which they may protect themselves. Educators should stay current on the various forms of attacks that are now occurring in order to defend themselves, their pupils, and the institution as a whole.

The implementation of password protection and the activation of multifactor authentication, for example, are both basic actions that will result in major outcomes. The importance of prioritizing cybersecurity for aspiring educators cannot be overstated. This includes maintaining a state of constant awareness and collecting knowledge about the most efficient strategies to protect both themselves and their students. Therefore, the researcher came to the conclusion that it is essential for prospective teachers to have a solid awareness of cyber security in order to make use of social media in a secure manner and to efficiently manage passwords while using the internet.

METHODOLOGY OF THE PRESENT STUDY

For the purpose of this investigation, the survey method is being utilized. At Vels Institute of Science, Technology, and Advanced Studies in Pallavaram, Chennai, the participants are students teachers who are currently in their last year of the Bachelor of Education (B.Ed) and Bachelor of Science in Education (B.Sc.B.Ed) programs who are interested in pursuing a career in education. In order to acquire data, a procedure known as random sampling is utilized. An estimated eighty student teachers were involved in the collection of the data. The tool was developed through a collaborative effort between the researcher and the research supervisor.

RESEARCH QUESTIONS

1. Is there is any significant difference between the whatsapp or Instagram user in all the selected variables for the student teachers?

2. Is there is any significant difference between the Male and Female student teachers in variables such as Cyber Hygiene, Password Management and cyber security?
3. Is there is any significant difference between the Course of the student teachers like B.Sc. B. Ed and B. Ed student teachers in variables such as Cyber Hygiene, Password Management and cyber security?
4. Is there is any significant relationship among all the selected variables?

ANSWER TO THE RESEARCH QUESTIONS

1. Is there is any significant difference between the whatsapp or Instagram in all the selected variables for the student teachers?

Variable	Type of social media				't' Value	Level of Significance
	Whats app (N= 48) (1)		Instagram (N=42) (2)			
	Mean	S. D	Mean	S. D		
Cyber Hygiene	10.52	2.294	11.03	1.892	4.305	0.001
Password Management	20.43	5.016	21.00	5.442	2.024	NS
Cyber security	18.33	3.812	20.56	3.232	5.753	0.001

It is inferred from the above table that student teachers who are Instagram usage have better Cyber Hygiene and Cyber security compared to the WhatsApp users. Furthermore, it has been noted that they exhibit statistical significance at a 1% level. Further, it is observed that Password Management is similar for both the WhatsApp and Instagram user of the student teachers.

2. Is there is any significant difference between the Male and Female student teachers in variables such as Cyber Hygiene, Password Management and cyber security?

Variable and Dimensions	Gender				't' Value	Level of Significance
	Male (N = 08) (1)		Female(N =69) (2)			
	Mean	S. D	Mean	S. D		
Cyber Hygiene	10.13	2.475	10.62	2.237	0.197	NS
Password Management	21.13	5.866	19.78	5.401	0.241	NS
Cyber security	16.63	1.188	23.43	6.779	8.710	0.001**

The above table suggests that female student teachers have better cyber security compared to male student teachers. Furthermore, it is noted that they exhibit statistical significance at a 1% level. Additionally, it has been noted that the social media and password management are identical for both the male and female student teachers.

3. Is there is any significant difference between the Course of the student teachers likeB.Sc. B. Ed and B. Ed student teachers in all the selected variables?

Variable	Course details				t' Value	Level of Significance
	B.Sc. B. Ed (N= 40) (1)		B. Ed (N=40) (2)			
	Mean	S. D	Mean	S. D		
Cyber Hygiene	9.88	2.166	10.92	2.361	1.785	NS
Password Management	17.80	5.196	20.76	4.994	3.009	NS
Cyber security	16.68	2.996	19.36	3.604	9.029	0.001

The above suggests that B. Ed student teachers possess a higher level of cyber security compared to B.Sc. B. Ed student teachers. Furthermore, it is noted that they exhibit statistical significance at a 1% level. Additionally, it has been noted that the cyber hygiene and password management are identical for both B.Sc.B.Ed and B.Ed., course student teachers.

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

Variables	Cyber Hygiene	Password Management	Cyber Security
Cyber Hygiene	1	0.642**	0.561**
Password Management	X	1	0.630**
Cyber security	X	X	1

The table clearly demonstrates a strong favorable correlation between cyber hygiene, password management, and cyber security. Furthermore, it is clear that they have a high level of significance and positive significance at the 1% level.

CONCLUSION

Teachers and students in this digital age are heavily reliant on the newest approaches, using a variety of technologies into their instruction. According to the results of this study, student teachers need to be more cautious when using various social media platforms, such as Instagram, and WhatsApp, and they should always keep their passwords private by utilizing secure password management. According to a recent survey, aspiring teachers who use mobile phones should be more vigilant about scams and cybercrime and take precautions to avoid them. Therefore, the current study concludes that aspiring educators should be knowledgeable about cyber security so they can help adolescent students who are at danger.

REFERENCES

1. Abomhara, M., & Koien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.
2. Ali ŞENOL, Tarık TALAN, Cemal AKTÜRK(2021) A RESEARCH ON UNIVERSITY STUDENTS' AWARENESS OF CYBER SECURITY: CASE STUDY OF PASSWORD USAGE, Research Gate,pp.46 – 56.

3. Alharbi, T.; Tassaddiq, A. (2021), Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cognitive Computing. Vol.5(23).pp. 1 – 15, https://doi.org/10.3390/bdcc5020023
4. Arwa A. Al Shamsi (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE, International Journal of Information Technology and Language Studies (IJITLS) Vol. 3(2), pp. 8- 29.
5. Aslay, F., (2017), Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, [Cyber Attack Methods and Current Situation Analysis of Turkey's Cyber Safety] International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1), 24-28.
6. DHS. (2014). A glossary of common cybersecurity terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. [Online]. Available: http://niccs.uscert.gov/glossary
7. Feray Küçükbaş Duman(2022), Determining Cyber Security-Related Behaviors of Internet Users: Example of the Faculty of Sport Sciences Students, European Journal of Education, Volume 5(1),PP.114 – 131.
8. Ganesh Talpe (2022), Cyber Security Awareness among College Students, International Research Journal of Modernization in Engineering Technology and Science (Peer- Reviewed, Open Access, Fully Refereed International Journal) Volume:05(10) , pp-2117 - 2121 Factor- 7.868 www.irjmets.com
9. Misbah Ahmed Al-Sahafi and Abdullah Mohammed Al-yateem(2020) A Suggested Model to Raise Awareness of Cybersecurity Among Computer Teachers in Public Education: An Analytical Study on Education Department in Jeddah Governorate, Technological Communication, Vol 13 No (4) Oct-Nov-Dec 2020 Pp 2271-2276
10. Mack, M. (2018). Cyber security. UK: ED-Tech Press.
11. Nabin Chowdhury1 · Vasileios Gkioulos1(2023), A personalized learning theory-based cyber-security training exercise, International Journal of Information Security Volume 22:1531–1546.
12. Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity
13. Prasad R., Rohokale V. (2020): Cyber Security: The Lifeline of Information and Communication Technology, Springer Series in Wireless Technology, Springer Nature Switzerland AG 2020. DOI: 10.1007/978-3-030-31703-4_16.
14. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cybersecurity and precautionary behaviour. Computers in Human Behavior, 75, 547-559.
15. Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? Information & Computer Security, 26(1), 2-9.
16. Yigit, M. F., & Seferoğlu, S. S. (2019). Investigating students' cyber security behaviors in relation to big five personality traits and other various variables. Mersin University Journal of the Faculty of Education, 15(1), 186-215.
17. Yesem Kurt Peker, Lydia Ray, Stephanie Da Silva, Nathaniel Gibson, Christopher Lamberson (2016), Raising Cybersecurity Awareness among College Students, Journal of The Colloquium for Information System Security Education (CISSE), pp 01- 17.