RESEARCH
www.commprac.com
ISSN 1462 2815

EFFECTIVENESS OF AWARENESS ON CYBER-ATTACKS AND DEFENSES AMONG ADULTS IN SELECTED URBAN AREA IN TAMIL NADU, INDIA

Dayana B.A.A [1]*, Natya. P. Kumar [2], Oviya. K [3], Natarajan. S [4], Priyadarsini. A [5], Jagadesswari. J [6] and Cecyli. C [7]

[1] Department of Medical Surgical Nursing, Saveetha College of Nursing,
Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India.
[2,3,4] B.Sc (Nursing) IV Year Student, Saveetha College of Nursing,
Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India.
[5] Department of Child Health Nursing, Saveetha College of Nursing,
Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India.
[6] Department of Obstetrics and Gynaecological Nursing, Saveetha College of Nursing,
Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India.
[7] Department of Medical Surgical Nursing, Saveetha College of Nursing,
Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India.
*Corresponding Author Email: diana.joann@gmail.com

DOI: 10.5281/zenodo.12580264

Abstract

The aim of this study was to assess the effectiveness of awareness on cyber-attacks and defenses among adults in a selected urban area in Kanchipuram district, Tamil Nadu, India. A quantitative research approach with a quasi-experimental research design was used. A total of 60 samples who met the inclusion criteria were selected by using convenience sampling technique. The experimental and control groups were assessed by using self-structured knowledge questionnaires. In the pretest of Group I, 21(70%) had poor knowledge and 9(30%) had moderate knowledge and in the post test, 19(63.33%) had moderate knowledge and 11(36.67%) had adequate knowledge regarding cyber-attack and defenses. The demographic variables, the type of family (X2=6.006, p=0.050), and the other demographic variables had not shown statistically significant in association with post-test level of knowledge. The findings suggest these strategies could serve as a guide for others to assess and mitigate cyber threat vulnerabilities. The study highlights the significance of promoting awareness and providing education to foster a safe online environment.

Keywords: Cyber-Attacks, Defenses, Information Technology, Cyber Threat, Awareness, Online.

INTRODUCTION

The field of Information Technology has experienced an enormous upsurge in the decade preceding the present, with a substantial increase in global internet usage by individuals and other entities, including academia, government, and industrial sectors. In the past decade, the advent of information technology, including mobile devices and digital applications, has significantly altered everyday living, enabling a wide range of lifestyles in several domains. The widespread adoption of technology and the growing need for online connectivity in various sectors such as education, retail, tourism, and autonomous vehicles have greatly increased worldwide internet usage opportunities. Some of the use of these devices include accessing digital newspapers, browsing the internet, using search engines to find specific material, using recommender systems as decision assistance tools, and using social media, among others. [1,2] "Mobile Communication and Society" explores the impact of wireless networks on daily life, politics, and culture. The book examines the reasons behind people owning wireless technology, socioeconomic disparities, and societal ramifications. It explores the emergence of a mobile youth culture, flash mobs, and the potential political ramifications of communication. The authors also examine the correlation between communication and development and the potential for developing nations to adopt wireless and satellite technology directly. The book spans across various regions, examining the shift towards a mobile network society. [3]

The rapid advancement of computing and communications has transformed our daily lives and business practices. Information technology allows businesses to expand their customer base, introduce new products, and collaborate globally. [4] Nevertheless, despite the significant growth in internet usage due to advancements in information technology, many internet users, frequently referred to as netizens, still lack sufficient knowledge about different online risks, sometimes known as "cyber hazards." Indeed, individuals frequently lack the essential information necessary to safeguard their electronic devices. In the direst circumstances, individuals have a complete absence of awareness regarding cyber hazards. Therefore, they have little willingness to employ defensive cyber security measures.[5]

Information security vulnerabilities are prevalent due to various threats, ranging from minor to severe attacks. Individuals' awareness can be categorized as low, moderate, or high. Awareness of cyber security is a key factor, with low awareness resulting in inattentiveness, medium awareness causing inappropriate use, and high awareness requiring deep understanding of risks and effective prevention measures. Cyber-attacks pose an imminent threat to the security of information. With the rising rates of data usage and internet consumption, the need for cyber awareness has become increasingly critical. Internet users have sufficient understanding of cyber threats but typically only implement basic and commonly used preventative measures. The level of cyber wisdom is directly linked to the level of cyber awareness, regardless of the respondent's nation or gender. Furthermore, awareness is also linked to protective measures, but not to the information they were willing to reveal. Organisation worldwide detected a total of 493.33 million ransomware assaults in the year 2022. Phishing continues to be the prevailing kind of cyber-attack, with an estimated 3.4 billion spam emails sent every day. In 2022, the average cost of a data breach worldwide was $4.35 million. [5,6]

India records 18% surge in weekly cyber-attacks in Jan-Mar 2023 reports that " In the first quarter of 2023, India experienced a significant increase of 18 percent in average weekly attacks compared to the same period in 2022. Each organisation, on average, faced 2,108 attacks per week." [7] Hence, this study focused to assess the effectiveness of awareness on cyber-attacks and defences among adults in a selected urban area in Kanchipuram district, Tamil Nadu, India.

METHODS AND MATERIALS

The main study was conducted at in selected area after an authorized setting permission was obtained from the selected area in Kanchipuram district, Tamil Nadu, India. A quantitative research approach with a quasi-experimental research design was used. A total of 60 samples who met the inclusion criteria is selected by using convenience sampling technique. After selecting the sample, the investigator introduced him-self and explained the purpose of the study to the adults. Informed consent was obtained from the Participants after assured confidentiality. The Demographic variables were collected by using multiple choice questionnaires. The experimental and control group were assessed by using self-structured knowledge questionnaires. Group I was an experimental group, those who underwent intervention of awareness on cyber-crime and Group II was Control Group, those who did not undergo any intervention. The data was organized, tabulated and analyzed according to the objectives.

RESULTS AND DISCUSSION

The results have drastic differences after implementing knowledge to the samples. Figure 1 shows that, In the pretest of Group I, 21(70%) had poor knowledge and 9(30%) had moderate knowledge and in the post test, 19(63.33%) had moderate knowledge and 11(36.67%) had adequate knowledge regarding cyber-attack and defenses. In contrast, figure 2 depicts that, in the pretest of Group II, 23(100%) had poor knowledge and 7(23.33%) had moderate knowledge and in the post test, 14(46.6%) had moderate knowledge and 5(16.67%) had adequate knowledge and 11(36.6%) had poor knowledge regarding cyber-attack and defences**.**

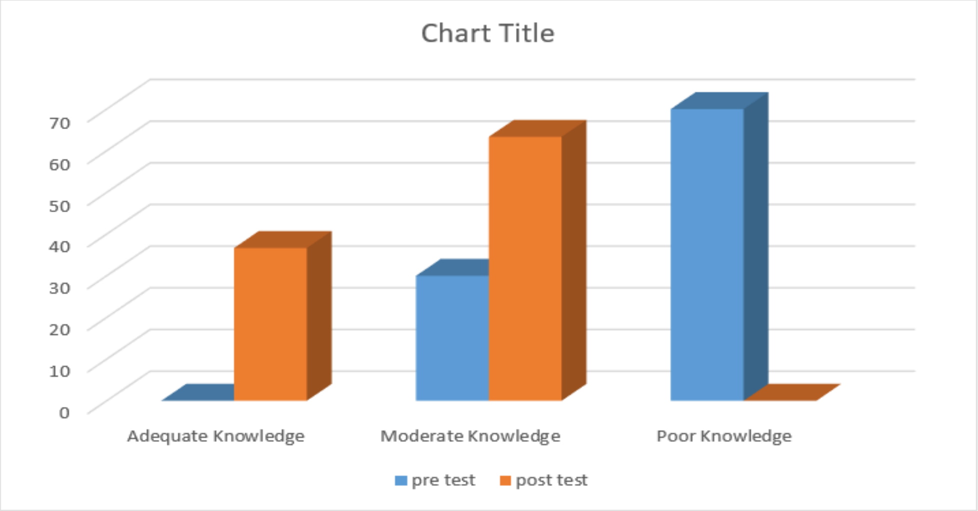

Figure 1: Percentage distribution of knowledge regarding cyber-attack and defences in the Group I (Experimental group)

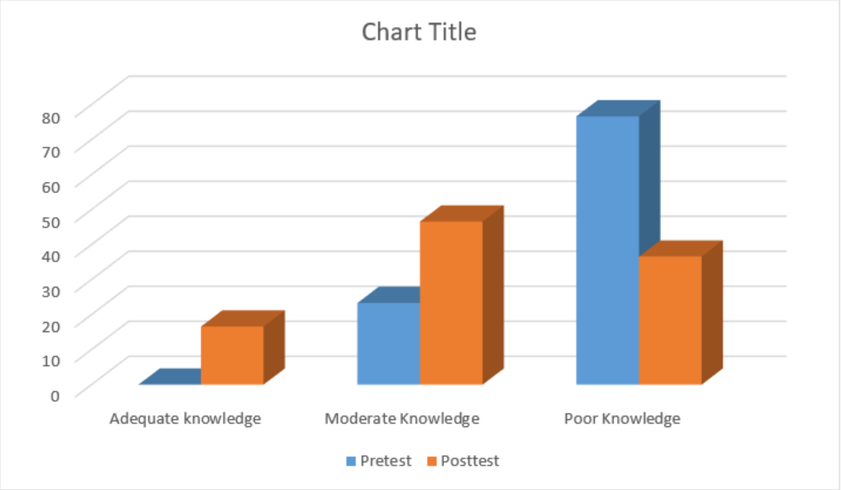

Figure 2: Percentage distribution of knowledge regarding cyber-attack and defences in Group II (Control group)

The Table 1 below showcases that the pretest mean score of knowledge in the Group I was 142.66±11.12 and post-test mean score was 119.53±7.56. The pretest mean score of knowledge in the Group II was 143.33±10.61 and post-test mean score was 127.0±10.22. The calculated paired 't' test value of t = 15.689 was statistically significant at p>0.001 level. This clearly shows that after the intervention of awareness programme, the knowledge regarding cyber-attack and defenses was significantly improved among the adults in the Group I.

The findings of the study were found to be consistent with the study findings conducted by Kimberly Diane Cook, 2017, a study on Effective Cyber Security Strategies for Small Businesses. This case study examines the strategies of four Melbourne, Florida-based small- and medium-size enterprises (SMEs) who successfully protected their businesses from cyber-attacks. The findings suggest these strategies could serve as a guide for others to assess and mitigate cyber threat vulnerabilities. Implementing these strategies could boost economic growth by employing local residents and boosting consumer confidence, ultimately leading to greater economic prosperity. [8]

Table 1: Comparison of the pretest and post-test level of knowledge on awareness regarding cyber-attacks and defences among adults.

n= 60(30+30)

Group	Pretest		Post Test		Paired 't' test & p-value
	Mean	S.D	Mean	S.D	
Group-I (Experimental Group)	142.66	11.12	119.53	7.56	**t = 15.689 p>0.0001, S*** **
Group-II (Control Group)	143.33	10.61	127.00	10.22	

The demographic variables not shown statistically significant in association with post-test level of knowledge regarding cyber-attacks and defences among adults in Group I (Experimental group). In contrast, the demographic variable, the type of family (X2=6.006, p=0.050) had shown statistically significant in association with post-test level of knowledge regarding cyber-attack and defences among adults at p<0.05 level and the other demographic variables had not shown statistically significant in association with post-test level of knowledge regarding cyber-attack and defenses among adults in Group II (Control group).

Similarly, the study was found to be consistent with the study findings conducted by Noluxolo Kortjan, 2013, "A study on A Cyber Security Awareness and Education Framework for South Africa". The objective of this study is to present a framework for enhancing cyber security awareness and education in South Africa (SA) with the goal of fostering a culture of online safety among internet users. This statement emphasises the importance of adopting a comprehensive strategy to cyber security and investigates the efforts made by developed nations in this field. The study highlights the significance of promoting awareness and providing education to foster a safe online environment. [9]

CONCLUSION

The investigator analysed the data and it could be concluded that the awareness had significant effect on the knowledge of cyber-attack and defenses that is the knowledge improved through awareness programme among the adults.

Acknowledgement: We would like to extend our gratitude to the authorities of Saveetha College of Nursing, and to all the adults participated in the study.

Authors Contrıbutıon: All the authors actively participated in the work of the study. All authors read and approved the final manuscript.

Conflıcts of Interest: The authors declare no conflicts of interest

References

1) Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. 1998. A Brief History of the Internet. Available online at <http://www.isoc.org/internet/history/brief.html>, Version 3.1, February 20.

2) National Academies of Sciences, Engineering, and Medicine. 1999. Funding a Revolution: Government Support for Computing Research. Washington, DC: *The National Academies Press*. https://doi.org/10.17226/6323.

3) Castells, Manuel & Fernández-Ardèvol, Mireia & Qiu, Jack & Sey, Araba. (2006). Mobile Communication and Society: A Global Perspective. 10.1111/j.1944-8287.2008.tb00398.x.

4) Berisha-Shaqiri, Aferdita. (2015). Impact of Information Technology and Internet in Businesses. Impact of Information Technology and Internet in Businesses. 1.

5) Zwilling, Moti & Klien, Galit & Lesjak, Dusan & Wiechetek, Łukasz & Çetin, Fatih & Basım, H. Nejat. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems.* 62. 82-97. 10.1080/08874417.2020.1712269.

6) 50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted, Date of access: 16/01/2024. https://www.techopedia.com/cybersecurity-statistics

7) India records 18% surge in weekly cyber-attacks in Jan-Mar 2023: Check Point, Date of access: 06/05/2023. https://cio.economictimes.indiatimes.com/news/digital-security/india-records-18-surge-in-weekly-cyber-attacks-in-jan-mar-2023-check-point/100026695

8) Cook, Kimberly Diane. (2017) "Effective Cyber Security Strategies for Small Businesses". *Walden Dissertations and Doctoral Studies.* 3871. https://scholarworks.waldenu.edu/dissertations/3871

9) Kortjan, Noluxolo & Solms, Rossouw. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*. 52. 10.18489/sacj.v52i0.201.