Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P. 27672-27678 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

A Study To Asses The Effectiveness Of Cybersecurity Awareness Program On Knowledge And Perception Regarding Cyber Security And Safety Among Nursing Students Of Sgt University

Ms. Nutan Kumari[1]*, Mr. Yogesh Yadav[2a], Ashish Dalal[2b], Gunjan Kaushik[2c]

[1]*: -Assistant Professor, Community Health Nursing, Faculty of Nursing, Shree Guru Govind Singh Tricentenary University
[2]-B. Sc Nursing Final Year Students, Faculty of Nursing, Shree Guru Govind Singh Tricentenary University

How to cite this article: Nutan Kumari, Yogesh Yadav, Ashish Dalal, Gunjan Kaushik(2024) A Study To Asses The Effectiveness Of Cybersecurity Awareness Program On Knowledge And Perception Regarding Cyber Security And Safety Among Nursing Students Of Sgt University. *Library Progress International,* 44(3), 27672-27678

ABSTRACT
Introduction – Nursing students' interactions on digital platforms make them both potential targets and defenders in the cybersecurity landscape. Their awareness and actions significantly impact online security, highlighting the need for effective cybersecurity education.
Objective – This study aims to assess the impact of a cybersecurity awareness program on the knowledge and perception of cybercrime and safety among nursing students at SGT University.
Methodology – This quantitative study uses a quasi-experimental design with a one-group pre-test and post-test approach. A total of 194 B.Sc. Nursing first-year students were selected via convenient sampling based on inclusion and exclusion criteria. A structured knowledge questionnaire and a perception checklist were developed to evaluate the program's effectiveness. Before the intervention, a pre-test was conducted to assess baseline knowledge. Following a seven-day cybersecurity awareness program, a post-test was administered to measure changes. Data were analysed using descriptive and inferential statistics. **Results** – The mean pre-test knowledge score was 15.46 ± 1.55, which significantly increased to 19.73 ± 1.62 in the post-test ($p < 0.001$). The mean perception scores also improved significantly from 5.68 ± 1.09 in the pre-test to 8.20 ± 0.776 in the post-test ($p < 0.001$). **Conclusion** – The study reveals a lack of cybersecurity awareness among nursing students and demonstrates the effectiveness of a structured awareness program. Regular cybersecurity training sessions are recommended to enhance knowledge and perception regarding cybersecurity among students.
Keywords: Effectiveness, Cybersecurity, Cybercrime, Awareness Program, Nursing Students

Introduction

In today's digital age, cybersecurity has become an essential component of personal and professional life. With rapid advancements in technology, individuals across various sectors face increasing exposure to cyber threats, ranging from data breaches to identity theft and phishing attacks. Students, especially those in professional programs such as nursing, are particularly vulnerable to these risks due to their frequent use of digital platforms for academic, social, and professional purposes. As future healthcare professionals, nursing students will handle sensitive patient data and are expected to maintain high standards of confidentiality and security. However, a lack of knowledge and awareness regarding cybersecurity can increase their vulnerability to cyber-attacks, potentially compromising both personal information and patient data.

The role of cybersecurity awareness has gained significant importance in educational settings, where students are equipped not only with academic knowledge but also with essential skills to navigate digital environments safely.

Cybersecurity awareness programs are designed to improve individuals' knowledge, attitudes, and practices related to cybersecurity, enabling them to recognize and respond appropriately to cyber threats. By fostering a strong foundation in cybersecurity principles, such programs aim to build a culture of security awareness that enhances students' ability to protect both personal and institutional information.

This study assesses the effectiveness of a cybersecurity awareness program specifically tailored for nursing students at SGT University. By evaluating the program's impact on students' knowledge and perception of cybersecurity, the research seeks to determine whether such initiatives can effectively empower students to understand and mitigate cyber risks. This study's findings will provide valuable insights into the potential benefits of integrating regular cybersecurity training into nursing education, ultimately supporting a safer digital environment within healthcare settings and beyond.

Need of the study

cybersecurity awareness programs play a vital role in enhancing individuals' understanding of cyber threats and safe online practices. these programs can significantly improve knowledge and attitudes towards cybersecurity, equipping students with the skills needed to recognize and respond effectively to potential risks. for nursing students, such awareness not only aids in protecting their personal information but also prepares them to handle sensitive data responsibly in clinical environments. the healthcare industry faces unique cybersecurity challenges due to the value of patient data, making it even more critical for nursing students to develop a proactive approach to cyber safety early in their careers.

this study aims to address this gap by evaluating the effectiveness of a cybersecurity awareness program in improving knowledge and perception of cyber safety among nursing students at sgt university. the findings will provide valuable insights into the impact of cybersecurity education, potentially supporting the integration of regular cybersecurity training into nursing curricula. this proactive approach can ultimately contribute to building a more secure healthcare environment, where nursing professionals are better prepared to uphold the highest standards of data security and privacy.

Students play a critical role in the cyber security landscape. Students' interactions on digital platforms potentially make them both targets and defenders against cyber threats. Every action, every click, and every piece of information shared online can significantly impact cybersecurity. A social media post, for example, might unwittingly provide cybercriminals with the information they need to breach a network. On the other hand, implementing secure online practices, such as employing robust passwords and exercising caution with emails, can significantly reduce your chances of falling victim to cyber threats. Cyber-attacks have been a trend in the few past years as companies and large organizations encountered cata- strophic impact from such attacks including the loss of information assets, business disruption, equipment dam-age and revenue loss. As it is expected that the number of cyber-attacks will grow in the near future, the notion that organizations need to be cyber resilient is becoming increasingly popular. On almost a daily-basis cyber-attacks and exploits are conducted, exploiting miscellaneous vulnerabilities. In contrast, defensive mechanisms are also being innovated to cope up with such a rapid pace to guarantee optimum levels of Information security; which is turning out to be a tough task as technology keeps advancing.

Objectives of the study

1. To assess the pre-test knowledge and perception of cyber security among students.
2. To evaluate cyber security awareness program on knowledge & perception regarding cybercrime & safety.
3. To find association between post-test knowledge score with selected demographic variables of students.
4. To find association between post-test perception score with selected demographic variables of students.

MATERIAL AND METHODS

A quasi-experimental research approach with a descriptive research design to evaluate the effectiveness of a cybersecurity awareness program on nursing students' knowledge of cybersecurity and cyber safety. The study was conducted among 1st year B.Sc. Nursing students currently enrolled at SGT University, Haryana. The study sample was selected using a convenient sampling technique. A total of 194 participants were included, with the sample size determined based on a literature review to achieve 95% confidence, 5% precision, and 80% statistical power. Convenient sampling was employed to select participants who met the inclusion criteria. The study sample consisted of students willing to participate, who had internet access, and a mobile, computer, or laptop facility.

- **Inclusion Criteria:**
  - Students enrolled in the third-year B.Sc. Nursing program at SGT University.
  - Students willing to participate in the study.
  - Students with access to the internet and a mobile phone, computer, or laptop.
- **Exclusion Criteria:**
  - Students not enrolled at SGT University.
  - Students who did not provide informed consent to participate in the study.

Variables

- **Dependent Variable:** Knowledge of cybersecurity among nursing students.
- **Independent Variable:** Teaching intervention through an informational guide on cybersecurity.

Data Collection Method

Ethical clearance for the study was obtained from the Institutional Ethics Committee, and formal permission was granted by the Dean of the Nursing Faculty at SGT University. A total of 194 B.Sc. Nursing first-year students were recruited for the study based on predefined inclusion and exclusion criteria. Participants were selected through purposive sampling to ensure that only eligible and willing students were included. The researcher approached the selected students prior to the data collection to explain the study's purpose, objectives, and procedures. Informed consent was obtained from each participant, ensuring their willingness to be part of the study. Students were assured of confidentiality and informed that their participation was voluntary. After obtaining consent, a Google Form link containing the pre-test questionnaire was shared with the participants via WhatsApp. The pre-test assessed baseline knowledge, perceptions, and factors influencing students' understanding of cybercrime and cyber safety. The average time for students to complete the form was approximately 20 to 30 minutes. Following the pre-test, an informational guide covering essential concepts of cybersecurity, cyber threats, safe online practices, and data protection techniques was provided to the students. This intervention aimed to enhance students' understanding of cybersecurity and improve their awareness of cyber safety. One week after administering the informational guide, a post-test was conducted to measure any changes in students' knowledge and perception of cybersecurity. The same Google Form was used to administer the post-test, allowing for a direct comparison of pre- and post-intervention knowledge levels.

RESULT OF THE STUDY

SECTION-I

The maximum sample in the area of age group 17-18 years , 60% of the participants of BSc nursing are female and the 40% are male , Majority of the participants are from middle class i.e. 89% , 6% are from upper class , 5% are from lower class majority participants father education 28% are up to senior secondary , 26% are up to secondary and remaining 3% are uneducated, With regards of daily used device, almost half of the participants (104) were using cell phone followed by 45 participants with tablet and laptop. Data revealed that 87 participants had ever experienced the cybercrime before and 107 participants had not experienced the cybercrime .

SECTION-II

Table:1

Assessment Knowledge of regarding Cyber Security & Safety among nursing students.

N=194

Score		Mean score	Mean %	SD
owledge score	e-test	15.46	52.3%	1.55
	st Test	19.73	73.64	0.776

Maximum knowledge score: 30
Maximum perception score: 10

Table number -1 Revels that In the pre-test, participants scored an average of 15.46, equating to a mean percentage of 52.3%, with a standard deviation of 1.55. After the intervention, the post-test results show a marked improvement, with a higher mean score of 19.73, representing a mean percentage of 73.64%, and a reduced standard deviation of 0.776. This suggests that participants' knowledge significantly increased after the

intervention, while the lower standard deviation in the post-test indicates more consistent performance across participants.

Table: -2

Assessment of Perception of regarding Cyber Security & Safety among nursing students.

(N=194)

SCORE		MEAN SCORE	MEAN %	SD
PERCEPTION SCORE	Pre-test Score	5.68	55.6%	**1.62**
	POST TEST SCORE	**8.20**	**84%**	**0.776**

Table 2 reveals In the **pre-test**, the average perception score was 5.68, corresponding to a mean percentage of 55.6%, with a standard deviation of 1.62. This score suggests that participants initially had a moderate level of positive perception. Following the intervention, the **post-test** results reveal an increased mean score of 8.20, with a mean percentage of 84% and a standard deviation of 0.776. This improvement in the post-test indicates a substantial positive shift in participants' perceptions, with the lower standard deviation suggesting that the post-test scores were more consistent across participants.

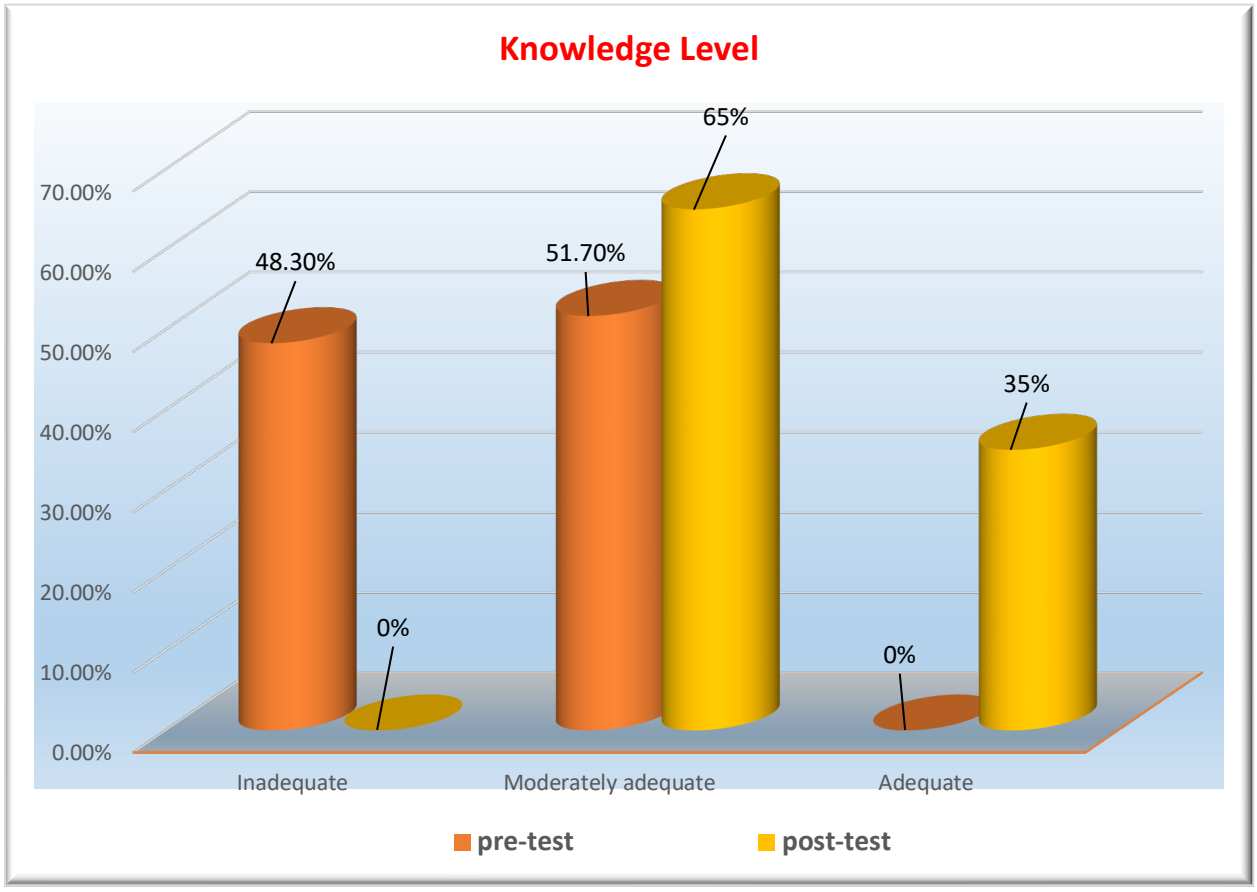


Figure 3: Level of knowledge of students regarding cyber security & safety.

The graph illustrates the knowledge levels of participants before and after an intervention, In the pre-test, 48.3% of participants had an *Inadequate* knowledge level, 51.7% were at a *Moderately Adequate* level, and none were in the *Adequate* category. This indicates that prior to the intervention, most participants had low to moderate

knowledge.

In the post-test, no participants were in the *Inadequate* category, showing an improvement. The majority, 65%, reached a *Moderately Adequate* knowledge level, and 35% attained an *Adequate* knowledge level. This shift from *Inadequate* to higher levels indicates a positive impact of the intervention, with an overall increase in knowledge levels among participants.

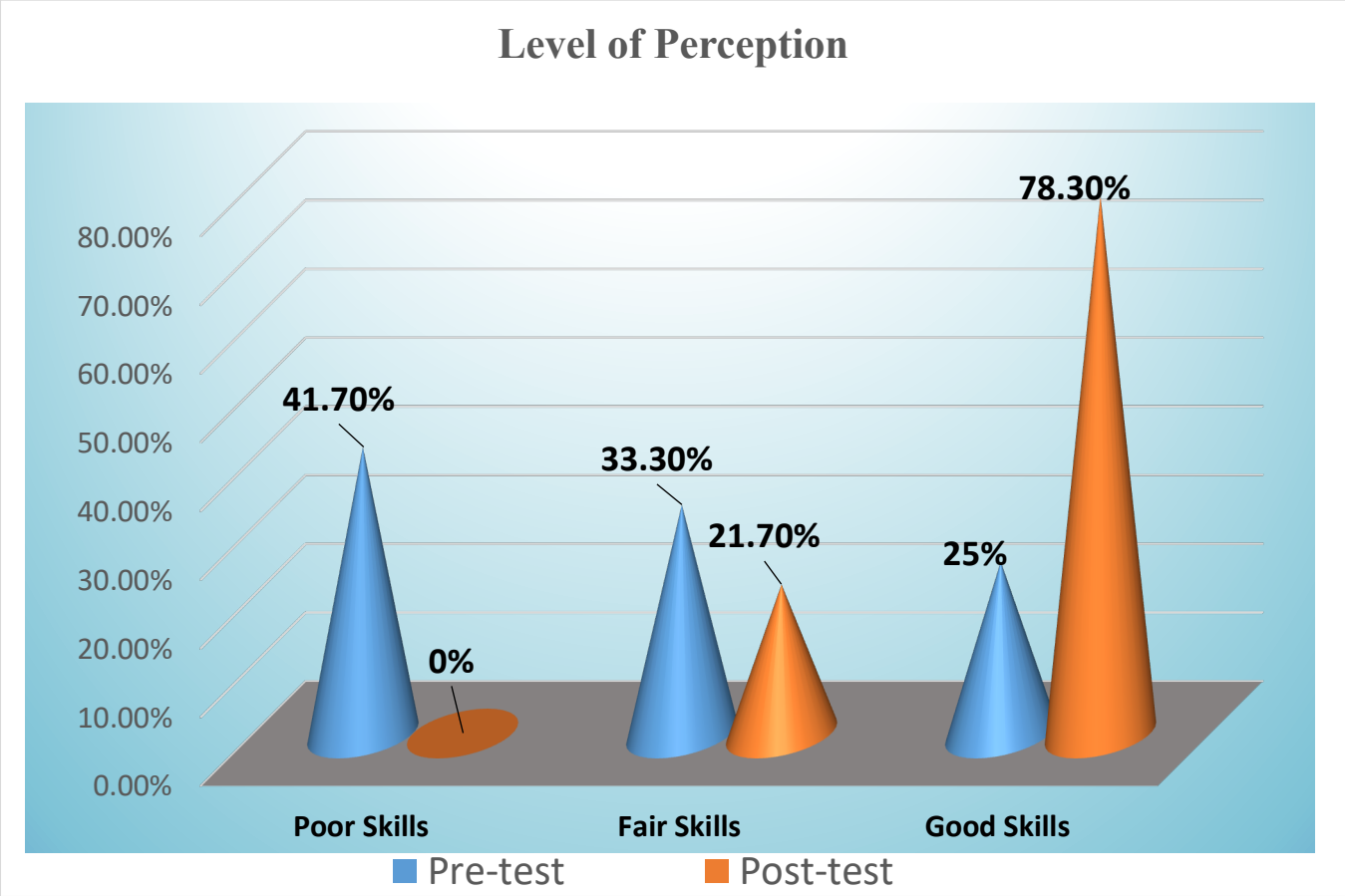


Figure 4: Perception level of students regarding cyber-Security& Safety.

The graph shows participants' levels of perception, comparing pre-test and post-test results across three categories: -In the pre-test, 41.7% of participants were rated as having *Poor Skills*, 33.3% had *Fair Skills*, and only 25% exhibited *Good Skills*. This distribution indicates that prior to the intervention, most participants had limited perception skills. In the post-test, none of the participants remained in the *Poor Skills* category, showing improvement. The percentage with *Fair Skills* decreased to 21.7%, while those with *Good Skills* increased significantly to 78.3%. This shift suggests that the intervention positively impacted participants' perception skills, with a substantial increase in those achieving a higher level of perception.

Section IV

Table: - 3

Effectiveness of Cyber Security Awareness Program on the knowledge and perception among nursing students

(N-194)

Category	Over all	Mean	Mean %	SD	Increased mean	't' value	'p' value
Knowledge	Pre- test	15.46	52.3%	1.55	4.27	18.31	**0.000***
	Post- test	19.73	73.65%	1.62			
Perception	Pre- test	5.68	55.2%	1.09	1.41	8.76	**0.000***
	Post- test	8.20	84%	0.776			

Table Number-3 Reveals that For the Knowledge category: In the pre-test, the mean score was 15.46, corresponding to a mean percentage of 52.3%, with a standard deviation of 1.55. In the post-test, the mean score increased to 19.73, representing 73.65% with a standard deviation of 1.62. The increase in mean score (4.27) was statistically significant, with a *t* value of 18.31 and a *p* value of 0.000, indicating a significant improvement in knowledge after the intervention.

For the Perception category: The pre-test mean score was 5.68, corresponding to a mean percentage of 55.2%, with a standard deviation of 1.09. The post-test mean score increased to 8.20, representing 84% with a standard deviation of 0.776. The mean increase (1.41) was also statistically significant, with a *t* value of 8.76 and a *p* value of 0.000, indicating a significant improvement in perception following the intervention. Hence the Research Hypothesis is accepted and Null Hypothesis is Rejected.

Section V:

association between post-test knowledge score and Perception with selected demographic variables of nursing students.

Knowledge demographic variables (age, gender, device usage, education level, experience with cybercrime, or type of cybercrime experienced) not showed statistically significant differences in mean scores, as indicated by p-values above the typical threshold of 0.05. This suggests that these factors did not significantly influence the participants' responses. Perception of participants revealed that there is no significant association between post-test perception and demographical variable expect for gender. Data showed that males students have better perception of cyber security & safety as compared to female students. But the obtained p-value for the gender is less than 0.05%, which indicates that there is a significant association between perception score with the gender.

Discussion: - The above findings of this study were supported by a study conducted by Ms. Chelsea Angelina Simon (2023) The study's aims to examine the level of awareness on cyber security and to understand the level of basic knowledge about cyber security among female college students in in Coimbatore city. The data were gathered through questionnaire and the sample size of 106 female students. The descriptive research design was used for this study and the sample was collected using a simple random sampling method. The chi-square test and Spearman's rank correlation coefficient were used in the study. The study concludes that, there is a growing awareness of cyber security among female college students, but still there is lack of knowledge when it comes to implementing the necessary security measures to ensure their online safety and security. **Samaher Al-Janabi and Ibrahim Al-Shourbaji (2018**) conducted a study of Cyber Security Awareness in Educational Environment in the Middle East. The main goal of this paper is to analyses the information security awareness among academic staff, researchers, undergraduate students and employee within educational environments in the Middle East in an attempt to understand the level of awareness of information security, the associated risks and overall impact on the institutions. The results reveal that the participants do not have the requisite knowledge and understanding of

the importance of information security principles and their practical application in their day-to-day work. This situation can however be corrected through comprehensive awareness and training programs as well as adopting all the necessary safety measures at all levels of the institution to ensure that the students, academic staff and employees are trustworthy, technology savvy and keep their data safe. The above findings of the study were supported by Ms. Minal S. Chaudhari (2021) conducted a study to assess the Awareness regarding Cybercrime and cyber safety among undergraduate students from selected Nursing Institute of Nashik City. A descriptive study design was used on 60 students of undergraduate Nursing Institute. A student nurse researcher conducted a structured interview schedule for 30-45 minutes to collect data. The result revealed that undergraduate nursing students have significant score (15.68) of cybercrime and having poor knowledge that is "poor knowledge" of cyber safety. There was a no significance association found between cybercrime and cyber safety with their selected socio-demographic characteristics like age, gender, father occupation, mother occupation, monthly family income, Time spends on Internet, Internet use as, Awareness about cybercrime, feel safe while using Internet, knowledge about Hacking, known victims of cybercrime, cybercrime investigation cell.

CONCLUSION

The cyber security awareness program regarding cyber security was effective in improving the knowledge and perception of the selected group of people. Hence, with an increase in knowledge, there is a gradual increase in perception. Post-test mean of knowledge score, perception score was higher than pre-test mean knowledge score, perception score, which showed that the cyber security awareness program has a significant effect in improving knowledge and perception regarding cyber security & safety among students. There was no significant association between post-test knowledge & perception regarding cyber security with selected demographic variables. The investigator concluded that the majority of the students were not much aware of cyber crime and this study showed the effectiveness of the cyber security awareness program on cyber security. Hence, training program in a regular period will help in gaining knowledge & improving perception regarding cyber security among students.

REFERENCES

- Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, https://www.academia.edu/4613831/Computer_security_and_ethics_awareness_among_IIUM_students_An_empirical_study
- Chakraborty, S. (2019). Malware attack and malware analysis: A research. International Journal of Scientific Research in Computer Science, 5(3), 268-272. doi:10.32628/CSEIT195379
- Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 20(2), 96-121. DOI:10.1080/02681102.2013.836699