International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1137)
Available online at: https://www.ijariit.com

Study of awareness of cyber security in educational organization

Shruti Sunil Manohar
ssmanohar288@gmail.com
Parul University, Vadodara, Gujarat

Amita Garg
amita.garg@paruluniversity.ac.in
Parul University, Vadodara, Gujarat

Aparna Havaldar
aparna.havaldar21138@paruluniversity.ac.in
Parul University, Vadodara, Gujarat

ABSTRACT

Today we are all living in the era of Internet and Social media. We cannot imagine the world without the Internet. So the Educational organizations are also transforming and trying to use IT tools for various purposes. .The teaching methodologies have also evolved with the technology .During the Covid-19 era technology and the Internet were boon to continue the learning process with the help of several tools . But now Post Covid also many of the tools are still being used as they were found very effective in imparting education. But all of this is resulting in a lot of exposure to the internet or social media. The students even in Kindergarten are busy with some or the other gadgets surfing the internet. But as it is said every coin has two faces ,this cyber world also is also prone to a number of threats and crimes .Therefore it is important for all the stakeholders of any organization to be aware of the challenges in using the Internet .Here we are specially focusing on Educational Organizations to understand whether they are aware of the security measures while using the Internet specially the school kids are more vulnerable to these kinds of threats and even crimes .As the students are not aware of the cyber threats and issues to protect themselves from becoming victims of such activities, cases of cyberbullying, online fraud, racial abuse, pornography, and gambling have significantly grown. Research from the past shows that Internet users still have a very low to moderate level of awareness. Therefore we are undertaking the study regarding the awareness of Cybersecurity in Educational Organizations We will be trying to study how much the young children and young adults are aware regarding cybersecurity and its tools to have safe browsing. The result of this study will be helpful in acquiring knowledge about how much importance do educational organizations give for cyber security .The objective of this systematic review paper is to explore whether modern learners are educated about the risks associated with being active in cyberspace and the strategies that stakeholders are undertaking in the educational industry. In this paper, few strategies are also discussed as to how cyber security education can be implemented in educational Organizations.

Keywords: *Cyber Security, Awareness, Internet, Attacks*

1. INTRODUCTION

In recent years the world has become a cyber world with the increasing use of IT and Internet in all the sectors. The educational institutions are also now using it as a tool for imparting education as well as operations. For any nation, education is the cornerstone of social and economic change. Along with different government initiatives, private institutions play a crucial part in the growth of India's education sector. There are so many online portals also available which are imparting education. Especially, since the COVID pandemic, the use of IT tools has significantly increased in the educational organizations.

The research produced by BitSight (a cyber risk management business), higher education had the second-highest rate of ransomware attacks out of all the industries surveyed. Universities therefore need to create awareness for cyber security and take measures to strengthen their defenses against the significant potential losses caused due to cyber-attacks to the organization as well as the young students.

Universities today therefore needs to strengthen their defenses against these significant potential losses. Second-highest rate of ransomware to stay one step ahead of attacks that are still to come, according to Kim Milford, executive director of the Research and Education Networking Information Sharing and Analysis Center at Indiana University, who made this statement in a 2016 article written by the Center for Digital Education.

India plays an important role in the global education system. India is home to one of the biggest networks of universities in the world. With about 27% of Indians between the ages of 0 and 14 years old, the country's education sector offers several potential for expansion.

The education market in India is expected to be worth US$ 225 billion by FY25, up from an estimated US$ 117 billion in FY20. The Indian edtech market is expected to expand from 700-800 million USD in 2021 to $30 billion USD by 2031.

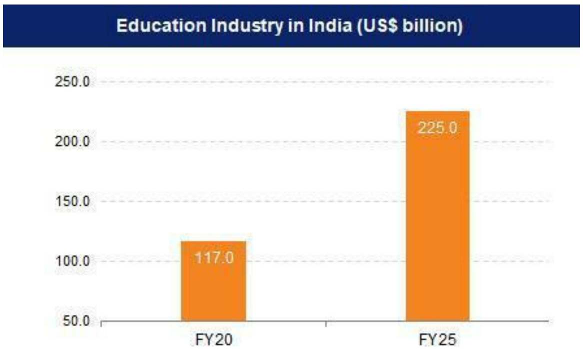


Figure 1: Cyber Security

Cyber security is the process of securing networks, computers, servers, mobile devices, electronic systems, and data from malicious attacks. It is sometimes referred to as IT security or electronic information security. The term is divided into many main categories and is utilized in a variety of applications, including business and mobile computing.

Here are a few of the most widespread categories of cyber-attacks:

Ransomware attacks
IoT attacks
Cloud attacks
Phishing attacks
Blockchain and cryptocurrency attacks
Software vulnerabilities
Machine learning and AI attacks

2. RESEARCH METHODOLOGY

It is concerned with the systematic techniques that a researcher takes while planning a study to ensure accurate results that satisfy the investigation's aims and objectives.

Primary data

Data that is gathered for the first time. The data was Collected by means of an online survey and questionnaire.

Secondary data

It is information that has previously been gathered or is publicly accessible. This information was gathered through websites, online journals, and other sources.

Design Sampling

Sampling is the process of choosing observations to offer a sufficient population description and inferences. Sample size The number of individuals or observations included in a research is referred to as the sample size. We have considered a sample size of 150 of different age groups.

Objectives

To study the awareness about Cyber security in educational Institutes
To create awareness regarding importance of cyber security for all the stakeholders in the educational institutions.
To discuss regarding various cyber-Threats

3. PROBLEM STATEMENT

- ➢ As the edu tech companies are growing and the educational institutions are also now using IT as a tool for imparting education as well as operations.
- ➢ We should therefore understand the importance of cybersecurity for educational institutions.
- ➢ All the stakeholders, especially the students should be educated about the cyber-Threats as well as the tools of protection.

4. LITERATURE REVIEW

The following studies conducted by researchers was referred during this research paper

Cyber Security Behaviour among Higher Education Students in Malaysia (3 February 2017)

Lalitha Muniandy, Balakrishnan Muniandy and Zarina Samsudin are the authors.

Cyber security education is as essential as "the three R's" (December 2019)

M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter are the authors.

Conclusion

This study assessed smartphone cyber security knowledge amongst students at a South African institution. In this regard, they were able to affirm the value of a CS education—an encouraging but disappointing result. First, because it shows how well the university is doing its part to raise awareness of CS instruction. The latter, as anyone who is not registered for a computer science degree at a university is not receiving the necessary information to be able to increase their personal cyber resilience. This indicates that, in terms of building a populace that is cyber-resilient, the South African approach to cyber security awareness is failing.

Digital Badges and E-Portfolios in Cybersecurity Education (October 2020)

Ronald E. Pike, Brandon Brown, Tobi West , Aeron Zentner are the authors.
Conclusion
In the classroom, group projects can be a useful experience for applying knowledge, resolving issues, and strengthening teamwork abilities. Employers require these competencies. The professors of this course believe that despite having attended two semesters of English classes and participating in other group projects in other subjects, a portion of College of Business students still lack the skills necessary to communicate effectively in groups. Many pupils lack the skills necessary to interact with others in teams in the workplace. Students list the most frequent issues they encounter in group work as a lack of interaction, accountability, participation, and teamwork.

Cyber security: Threats, Vulnerabilities and Countermeasures - A Perspective on the State of Affairs in Mauritius (2018)

Tikshnayah Nelliah Maistry, Nomesh Ramkurrun, Mageshwaree Cootignan, and Pierre Clarel Catherine are the authors.
Conclusion
The confidentiality, dependability, and accessibility of computing systems and their components are all goals of computer security. Hardware, software, and data are the three key components that are vulnerable to attacks in computing systems. These three, as well as the interactions between them, are susceptible to computer security flaws. The need for better cyber security infrastructures is becoming increasingly crucial as Mauritius aims to make the information technology sector its key economic pillar by integrating innovative technologies like Smart Cities, the Internet of Things, and cloud computing are just a few examples. Although cyber-attacks are typically the work of lone hackers, challenge groups, or criminals seeking illegal financial gain, some also pose a threat to national security.

A Systematic Review of Cybersecurity Risks in Higher Education (2 February 2021)

Georgios Kambourakis is the author.
Conclusion
Although the information was obtained from sources of differing repute, it was generally acknowledged that HE: The most valuable assets controlled in academia include financial information, research data, intellectual property, student grades, and administrative information. Threat occurrences involving incursion, malware, and other types of compromise were the most frequent. Scanning and vulnerable assets were two additional frequent sources of events. In HE, social engineering attacks and accidental disclosures happen frequently as well. The main threats to higher education were organized crime, state-sponsored espionage, and human mistake. These dangers can take advantage of holes in the administrative, technical, and physical defenses of the HEI, such as a lack of information security awareness or best practices, or a lack of best practice security measures.

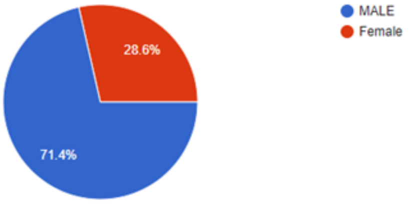
Cyber security: Study on Attack, Threat, Vulnerability (June, 2017)

TUSHAR P. PARIKH, DR. ASHOK R. PATEL are the authors
Conclusion
Research suggests that the best defense in cyber security issues involving assaults is a computer knowledgeable user. The most vulnerable individuals within a company, identified in this research as new hires, should be taken into account since the attacker is specifically looking for personally identifiable information from those involved. The psychological factors that affect user and network vulnerability are also supported by this research. This study comes to the conclusion that, even while technology can help lessen the effects of cyberattacks, human behaviour, human desires, and psychological predispositions still pose a hazard and vulnerability and can be changed via education.

Research Paper on Cyber Security (APRIL, 2021)
Mrs. Ashwini Sheth , Mr. Sachin Bhosale , Mr. Farish Kurupkar are the authors
Conclusion
We built this project on the premise that the "cyber" and "security" mechanisms of the concept of "cybersecurity" will coexist in a rapid state during the latter half of the 2010s. Although the manner it is used varies greatly depending on our circumstances, that gesture is more likely to quicken than to slow. That is not a part of our inquiry process; rather, it is the focal point of the work. We anticipate that cybersecurity will be widely acknowledged as the "master challenge" of the internet era at some time in the not-too-distant future (assuming it is not already true at the present).

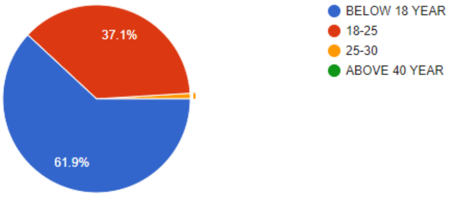
5. DATA ANALYSIS AND INTERPRETATION

A total of 150 responses were collected and on that data the analysis and interpretation has been done.
Gender-Wise



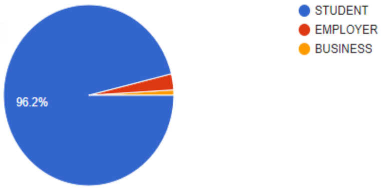
Interpretation
The above pie chart shows that 71.4% of respondents are male and 28.6% are females who are aware of the cyber threats and its solution

Age



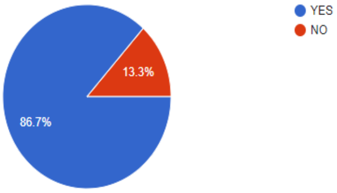
Interpretation
The above pie chart shows that 37.1% of respondents are between 18 to 25 years, majority of the responses are in the age between below 18 years and some of the students responded are in between 25 to 30.

Occupation



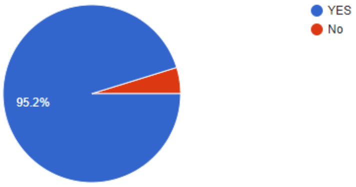
Interpretation
The above pie chart shows that majority of respondents are students i.e 96.2%, moderate respondents are employers and least respondents' business.

Are You Aware About Cyber Security?



Interpretation
The above pie chart shows that the maximum number of respondents (86.7%) are aware of cyber security and the minimum respondents (13.3%) are aware of cyber security.

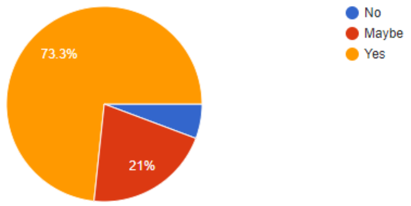
Do You Think Cyber Security Is Important for Educational Industry?



Interpretation

The above pie chart shows that the maximum number of respondents (86.7%) are aware of cyber security and the minimum respondents (13.3%) are aware of cyber security.

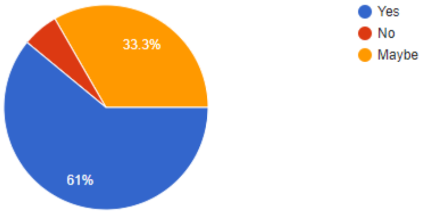
Cyber Security Can Provide Protection for Cyber Attack?



Interpretation

The above pie chart shows that the maximum number of respondents (73.3%) are yes that cyber security provides the protection over data and 21% of students are not sure about that. Many less students believe that cyber security cannot provide the protection over cyber-attack.

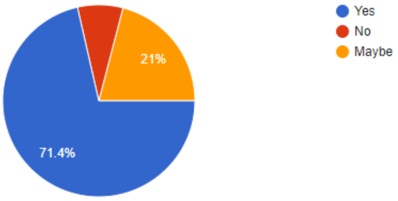
Do You Think Cyber Security Provides More Safe Use of The Internet?



Interpretation

The above pie chart shows that the maximum number of respondents (61%) are yes that cyber security provides the protection over data and 33.3% of students are not sure about that. Many fewer students believe that cyber security provides more security than others.

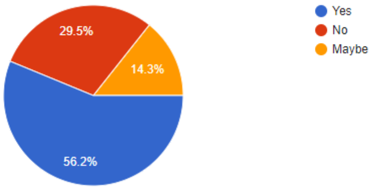
Do You Think That We Can Reduce Risk Using Cyber Security?



Interpretation

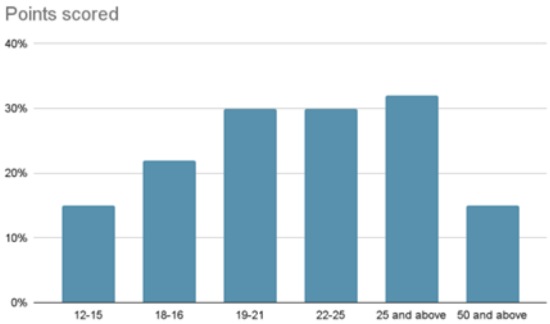
The above pie chart shows that the maximum number of respondents (71.4%) are that cyber security reduces the risk over data and 21% of students are not sure about that . Many fewer students believe that cyber security reduces the risk over data.

Do You Know About Cryptography?



The data was collected from respondents of various age group. The awareness regarding cybersecurity in different age groups.

AGE GROUP	AWARENESS
12-15	15%
18-16	22%
19-21	30%
22-25	30%
25 AND ABOVE	32%
50 AND ABOVE	15%



Interpretation
The above pie chart shows that the maximum number of respondents (56.2%) are yes that they know about cryptography and 29.5% of students are not aware about it

6. SUGGESTIONS

The educational institutions should organize programmes to create cyber awareness among the students and teachers of the institution. Following are some of the techniques used for security.

Cyber Security Techniques

Anti-Virus Software & Updates
Firewalls
Backups
Passwords
Multi-Factor Authentication
VPN
Employee Security Training

7. Conclusion

In the era of online education and increased use of the internet, it is observed that only a small percentage of people are aware of the threats and cyber security. After analyzing the secondary data, it has already been seen how cyber-attacks are increasing in Educational Organization
So, there is the necessity of educating all the stakeholders regarding the threats and the security measures -The wise and safe use of the cyber world is to be communicated.

8. REFERENCES

[1] Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety (December 6, 2021), Yamin, M.M., Katt B. and Gioulos
[2] Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety (December 6, 2021),Tam, K., Forshaw, K. and Jones
[3] Cyber security education is as essential as "the three R's" (December 2019),I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter
[4] Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study (April 2022) , Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke
[5] Cyber Security Behaviour among Higher Education Students in Malaysia (3 February 2017) , Lalitha Muniandy, Balakrishnan Muniandy and Zarina Samsudin
[6] Exploring Cybersecurity Threats in Digital Marketing (17 June 2020),Susan Konyeha.
[7] Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective (September 2019), Sagar Samtani, Maggie Abate, Victor

Benjamin, and Weifeng Li

[8] Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Pro cesses at a Crossroads(February 2020),Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer

[9] Cyber Security Behaviour among Higher Education Students in Malaysia (3 February 2017) , Lalitha Muniandy, Balakrishnan Muniandy and Zarina Samsudin.