STM JOURNALS

International Journal of
Information Security Engineering

Volume 2, Issue 1, 2024
January—June
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Analysis of an Awareness Program of Cyber Security in PIET, Jaipur: A Systematic Survey

Suman Jain[1], Siddharth Joshi[2,*]

Abstract

This paper presents an analysis on what the students and the new generation think aout cyber security after learning about cyber-crimes and security in an awareness program. Our knowledge of technology has dramatically increased in the past five decades, as a result it also gave us a new type of threat, cyber-threats. Through smartphones and computers, life has become easy both for individuals and big organizations. Therefore, we must learn how to be cyber aware. The newer generation certainly knows about the internet risks but according to a survey conducted by Ernst & Young LLP, the newer generation which is born and lives in cyber era is less concerned about cyber security on their work devices than the previous one. Their overconfidence in their ability to avoid deception could be one factor behind this. "Anybody can be scammed" said Ashton Bingham, a cyber security expert from Trilogy Media YouTube channel, on a wired interview. To find the change in vision towards security, firstly, we needed to give students an attention towards cyber-crimes and protections so that they can be aware of all type of scams and threats and how to protect themselves from these. Secondly, we needed to collect data of students about how aware they are. Our research does not include the "fear appeal" of cyber security; instead, it includes cyber awareness as an essential duty of an organization or an individual to protect themselves and their employees or relatives from getting scammed. We are including our survey results here as it shows how an awareness program or campaign makes students more aware towards cyber security. We collected data from 262 students who attended the cyber security campaign. Our article also includes the survey from Arwa A. Al Shamsi for comparison of the campaign impact on the students.

Keywords: Cyber security, awareness, students, threats, cyber frauds

INTRODUCTION

Every person, organization, company, government use information technology because of its convenience and that attracts cyber criminals more [1]. It puts big corporation at a risk of great security threat. They construct security systems to safeguard themselves from such attacks. But sometimes even with security systems, the intense speed of internet innovations outsmarts them. Individual persons cannot build a security system to protect themselves so they have to avoid risking their data. They have to be aware about security threats that they may facing if they are not careful enough. Cyber attackers often choose simple victims who are already vulnerable so that person would be careless about their own internet security. Most of the time, the attackers target humans to breach out in big corporation's system mostly because of human ignorance. Most companies that are facing attacks are facing these because their employees are vulnerable humans [2]. They do careless things such as sharing passwords and emails and opening

*Author for Correspondence
Siddharth Joshi
E-mail: 2022pietcssiddharth162@poornima.org

[1]Librarian, Central Library, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India
[2]Student, Department of Computer Science and Engineering, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India

Received Date: January 29, 2024
Accepted Date: February 17, 2024
Published Date: April 10, 2024

Citation: Suman Jain, Siddharth Joshi. Analysis of an Awareness Program of Cyber Security in PIET, Jaipur: A Systematic Survey. International Journal of Information Security Engineering. 2024; 2(1): 1–9p.

unknown links. A very few numbers of attacks are registered as direct attack that does not include human verifications (5% of all cyber-attacks according to the IBM Cyber Security Intelligence Index report) [4].

As an individual, one has to be more careful about their own security because a normal person cannot spend so much money on antivirus, debugging software, and firewalls. However, by mentioning this precaution we are not saying that they can protect you from cyber harm completely. The threats completely rely on the human behavior towards their security. And because of the laws and regulations about personal information on the internet, the big tech companies like Google, Amazon, and Meta have to invest in improving their security systems. As always, the human aspect of information security remains susceptible to vulnerabilities. We have failed to improve human efforts towards security. If enough efforts are put towards building a cyber aware culture, we are certain that we can build very less vulnerable human society and an organization or company.

In worst-case scenarios, we even see people who have complete zero knowledge about cyber-crimes. These kinds of people often get hacked by a criminal through malicious software, from their computers or from their smartphones. Most of the time fraud call or email arrives on their phone and the criminals convinces them that if they did not give them some amount of money then the government or any other organization will seal their property and then the person who does not know about scams gets scammed. The current psychological system to spread awareness about secure internet is unconventional. We do not have to tell them what should and what should not be done on the internet. Instead, we should make a cyber aware culture from the beginning.

The main objective of this paper and survey is to find that any kind of cyber security campaign can give students a motivation to be more aware towards their internet and their personal data. We have asked 10 questions to 262 students of Poornima Institute of Engineering and Technology (PIET). Each related to some kind of awareness towards their personal data on the internet. We have included questions related to their knowledge of state law, and views about whether a crime is punishable or not.

The paper's sections are as follows. The second section follows what we did in our institute to spread awareness among the students. The third section is about our survey and its result and analysis on it. The fourth section is about the laws and what we can do if we get scammed. The fifth and last section is the conclusion and what we understand about the views and awareness of younger generation towards cyber-crime.

THE CYBER AWARENESS CAMPAIGN OF PIET

A cyber awareness program has to be very powerful, strong, and clear. It is very crucial for students who are not aware of this. We did not want to go with so-called "fear-appeal", we rather wanted to integrate it as their hobby to be alert on the internet. But before we move to our campaign program, first we need to define what is awareness.

In the book *The Conscious Mind,* David Chalmers [5] defines awareness as a condition in which an individual possesses the ability to utilize certain information directly for a diverse range of behavioral responses. If someone does not know the information that is being transferred that means he is not aware.

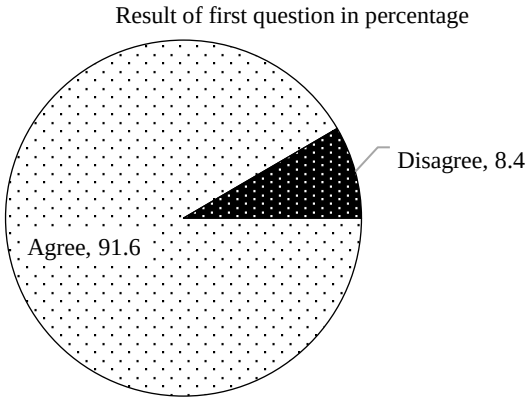
Our chief guest in PIET was Mr. Manoj Raman, cyber forensics consultant in Rajasthan Police Academy, Jaipur. In that session he interacted with students and taught them how to handle this kind of situation [3]. What can we do if we become victim of a cyber-crime; how to track your or other personal device; how to stay safe from many kinds of viruses; what kind of tricks that criminals can use; how to distinguish if a site is genuine or not; how to make strong passwords; and how to distinguish between secure mail and phishing mail, etc. In his 2-hour session, he interacted with many students to provide

them engagement with the subject. He taught about the career in cyber security. The session gave students a brief idea towards cyber awareness.

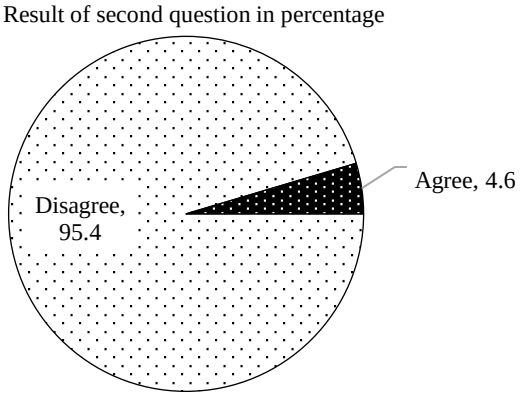
THE SURVEY AND ITS RESULTS

The survey that we have conducted in PIET has 10 different questions about whether the crime is punishable or not. A total of 262 PIET students participated in it. The following survey was conducted after few days of cyber security campaign to see if the awareness is retained in the students' minds or not. The average age of survey taking contestants is 19 years. The questions and results are as follows.

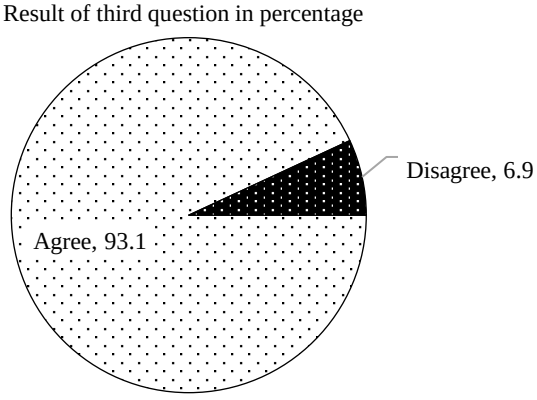
Q1. Manipulate or tamper with a computer database or introduce a virus into a computer without permission that it is unlawful?



Q2. Stealing, hiding, destroying or altering computer source code used for any computer resources with the intent to cause harm should result is punishable?

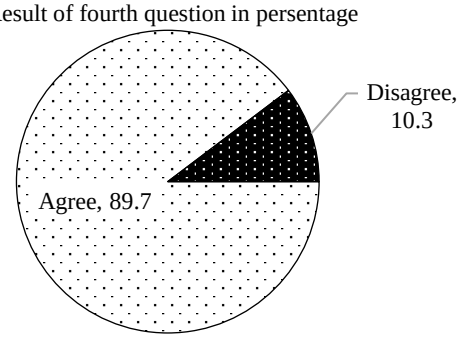


Q3. The unauthorized access, download data, copy data, or remove data from any computer is illegal?



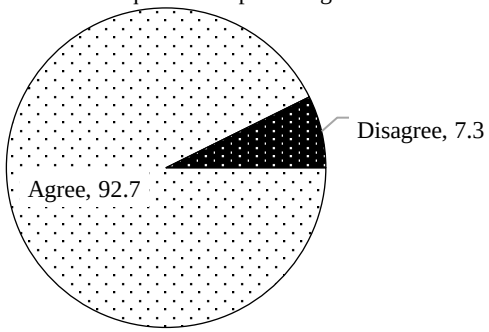
Q4. The denial-of-service assaults should be punishable?

Result of fourth question in persentage



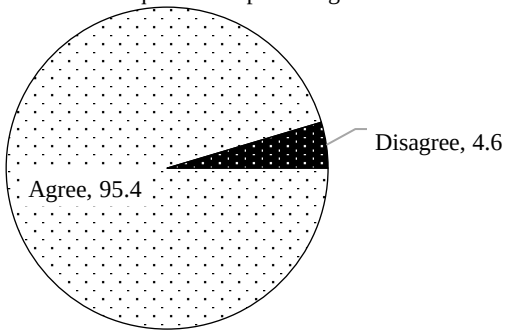
Q5. Anyone who interrupts a computer without the owner's permission or refuses to grant access to anyone who has been granted authorization is punishable?

Result of fifth question in percentage



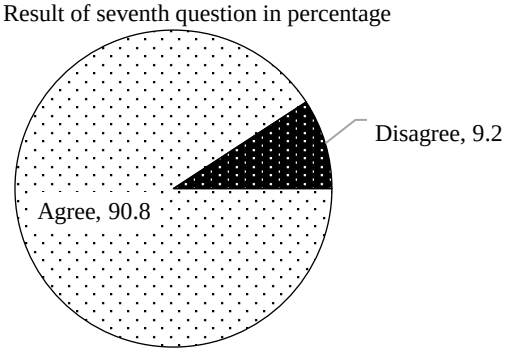
Q6. Under state law, for someone to use another person's electronic signature, passwords, or other unique identifier in a fraudulent manner is punishable?

Result of sixth question in percentage



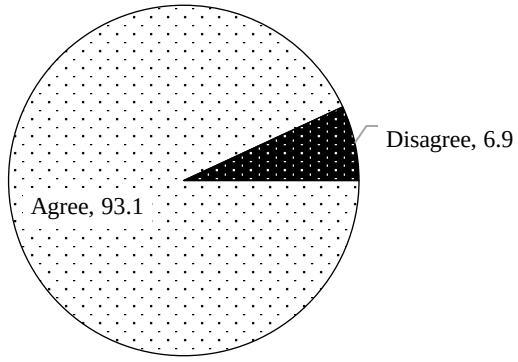
Q7. Using a communication device or computer resource fraudulently should be a maximum sentence of three years in prison.

Result of seventh question in percentage



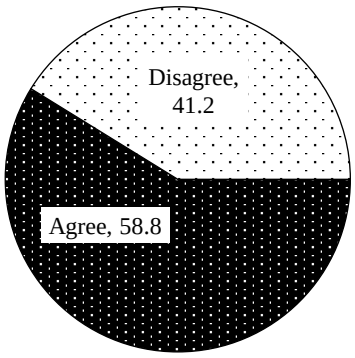
Q8. Introducing or causing to introduce any computer contaminant or computer virus into a computer without the owner's consonant is illegal.

Result of eighth question in percentage



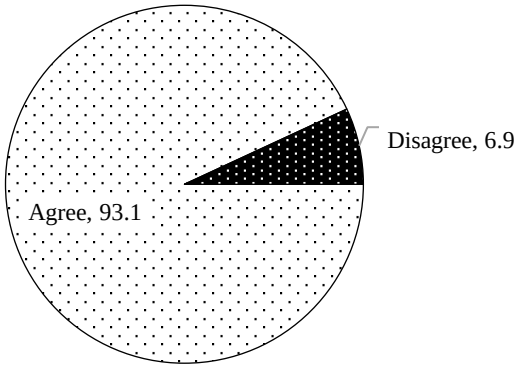
Q9. Altering, deleting, or transmitting computer resident data or programs is acceptable.

Result of ninth question in percentage



Q10. The computer virus refers to "any computer instruction, information, data or program that destroys, damages or degrades".

Result of tenth question in percentage



By analyzing the above results, we can say that a cyber awareness campaign certainly put positive impacts on the newer generation's mind. About 10% of students disagreed on punishing the crime activities, especially in the ninth question. Mostly because people or students think that altering friend's smartphone or computer is not a crime. The second and sixth questions which are most critical among them got over 95% agree votes, which shows that in serious crime students do think about their privacy and about their harm to them. In the third, fourth, and fifth questions about interruption without owner's permission, unauthorized access or denial of access get almost 8% disagreement rating, which means some students do not think that unauthorized access is forgivable or not a crime. The seventh question

gets almost 10% disagreement, which means that certain students think that 3 years' punishment is too much for using someone's personal computer which shows the students do not take cyber-crime as seriously as a theft of physical items. The 10th question about the definition of virus gets 93% agreement rating, meaning that students still do not know what virus really is. The first and eighth questions also got an unusual amount of disagreement rating almost 8% students think that inserting a virus in someone's computer is not unlawful.

According to the research by Digital Education Services firm Jisc [6], only 77% of students who are pursuing their higher education think cyber-crime is a growing threat and 35% thinks that it is their responsibility to learn about cyber security and fewer than 20% say that they are concerned about it. So as a result, our findings about the topic do show some positive results. The cyber security campaign certainly had an impact on the students' minds temporarily if not permanently.

Comparing the Results with a Similar Survey

A survey conducted by Arwa A. al Shamsi in the British University in Dubai [3] found similar results. The researchers found that while the students who participated in the cyber security awareness program and the program's educators both recognized potential online hazards that kids might encounter when using the internet, the majority of the prevalent threats were unanimously indicated by the interviewees. The instructors in the program held the view that the primary online threats for children aged 8 to 10 years are cyberbullying, and students also shared the concern that they might encounter such incidents. Both trainers and students identified additional online risks, including identity theft, phishing, and breaches of privacy.

The result in their published paper "If we compare the online risks that were identified earlier and considered as common, these online risks were covered in the content of the cyber security awareness program and children trained about them. This can be considered as a positive strong indicator of the efficiency of the cyber security awareness program."

The effectiveness of the cybersecurity awareness program was acknowledged by both the design and technology teachers, who served as trainers, as well as by the students. They both stated that the awareness program was very effective and beneficial. Many students express the effectiveness of awareness without providing detailed reasons, likely attributed to their youthful age hindering comprehensive explanations. Conversely, program trainers, who are teachers intimately familiar with the students and engage with them daily, elucidate the tangible benefits observed from the awareness program. Upon completion of the program, students exhibit increased online vigilance, actively safeguarding their personal information and adopting robust password practices. A notable change is observed as students refrain from agreeing to meet strangers encountered online. Additionally, students engage in discussions with teachers about their responses to various online incidents and share insights on how they communicate with parents to keep them informed about any discomforting online experiences.

Students typically use strong passwords and take precautions to secure their personal information. Students respond properly to different incidents online and they become more cautious while playing online games. The positive impact observed in students' online behavior serves as a strong indicator of the success of the cyber security awareness program implemented for children.

The trainers of the awareness program emphasize the significance of their crucial role in enhancing children's awareness levels. It is imperative for the community to actively participate in cyber security awareness training to foster a culture of cyber security within society. Parents should receive cyber security awareness training because their children will benefit greatly from their understanding of various online risks and best practices, as well as increased online protection. The involvement of all media outlets in promoting cyber security awareness would significantly enhance knowledge within society. Awareness posters in public places are recommended as well as awareness messages for all citizens. So, as we can see that the results are very similar.

LAWS AND REGULATIONS

Governments from around the world have their own laws and regulations about cyber-crimes and how to report them. In India we also have many cyber security laws and regulations. Most common of them are being mentioned here. For more details, you can visit their website in Reference [7].

- Section 43 of the Information Technology Act, 2000 (IT Act) defines hacking as a criminal offence in India. It prohibits the following actions with regard to computers, computer systems, computer networks, or computer resources: Unauthorized access includes any of the following: downloading data, information, or computer databases without authorization; introducing viruses or "computer contaminants"; helping someone else gain access by breaking the IT Act; and tampering or manipulating data so that services received by one person are charged to another.
- *Phishing:* There is no direct reference of phishing in statute. However, the Delhi High Court described phishing as "...a form of internet fraud...that involves a deliberate misrepresentation or theft of identity in order to perpetrate data theft" in the National Association of Software and Services Companies v. Ajay Sood 2005 (30) PTC 437 (Del) case [9]. As mentioned in earlier responses, Section 43 of the IT Act broadly encompasses activities falling under this criterion and could be classified as phishing assaults. The penalties for violating Section 43 have also been mentioned previously.
- *Security measures of organizations:* The IT Act mandates that all entities involved in processing, controlling, and handling data must comply with obligations related to transparency, possess a legal basis for data processing, and adhere to restrictions on the purposes of data usage as well as requirements for data retention. The law lacks specificity regarding the required measures for monitoring, identifying, preventing, or mitigating occurrences [10]. In contrast, Section 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules articulate specific guidelines in this regard.
    1. To be considered as having followed reasonable security practices and procedures, a corporate entity or an individual representing it should have incorporated security practices and standards. Additionally, they must have established a thorough information security program and policies encompassing operational, technical, managerial, and physical security controls suitable for the specific business and the protected information assets. In the event of an information security breach, the corporate entity or its representative is required to furnish evidence of compliance.
    2. The standard referenced in sub-rule (1) is IS/ISO/IEC 27001, which pertains to "Information Technology Security Techniques – Information Security Management System – Requirements" in the realm of international standards for information security.
    3. The central government is required to officially endorse and communicate the approval of any industry association or its affiliated entity, established by such an association, if its members engage in self-regulation through adherence to data protection codes of best practices that deviate from those outlined in IS/ISO/IEC, as stated in sub-rule (1). This will enable the codes of best practices to be implemented effectively.
    4. The entity or an authorized representative acting on its behalf, which has adopted either the IS/ISO/IEC 27001 standard or the approved and notified codes of best practices for data protection as specified in sub-rule, shall be considered the body corporate [8].
- A Helpdesk for Incident Response, available 24/7, should adhere to Rule 12 outlined in the CERT-In Rules. Any individual, organization, or corporate entity affected by cybersecurity incidents can report them to CERT-In.

  The Annexure to the Rules specifies certain incidents that must be reported to CERT-In without delay. These are as follows targeted scanning/probing of critical networks/systems:
    1. Compromise of critical systems/information;
    2. Unauthorized access of IT systems/data;
    3. Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.:
    4. Malicious code attacks such as spreading viruses/worms/Trojans/botnets/spyware,

5. Attacks on servers such as databases, mail, and DNS (domain name server), and network devices such as routers;
6. Identity theft, spoofing and phishing attacks; etc.

- Any additional actions that have a negative impact on or pose a risk to the availability, confidentiality, integrity, or security of any IT system, infrastructure, communications network, device, or data Section 66F of the IT Amendment Act defines and penalizes cyber terrorism. The provision states as follows:
  Whoever:
  1. With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by
  2. Denying or cause the denial of access to any person authorized to access computer resource; or
  3. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
  4. Introducing or causing to introduce any computer contaminant, and by engaging in such behavior, damages or is likely to damage property, results in death or injury to people, interrupts or knows that it will disrupt essential services or supplies for community life, or negatively impacts the vital information infrastructure listed in Section 70; Furthermore, the India cybercrime report helpline number is 1930.

CONCLUSION

In this paper, we tried to understand a student's mindset towards cyber security after attending a cyber awareness program. We can say that simply telling students to be aware on the internet is better than terrifying them from the risk of internet. We need them to learn how to benefit from internet with safety. By analyzing the results, we can conclude that presenting a cyber awareness campaign in right direction does have a significant impact on a student's mind. Just Because many people do not know how serious a cyber crime is, they do not take action on it and another reason behind this kind of mindset would be because they do not know about the state laws. Our chief guest in PIET tried to fill that gap between information and misinformation and it certainly had a positive impact on the student's minds. We need to build a culture around cyber security and talk about it with our parents, friends, and other relatives.

In conclusion, the research findings indicate that about 90% of students are serious about their cyber security. It is encouraging that students understand the value of safeguarding their private and sensitive information when using the internet. In the contemporary digital era, it is crucial for individuals to prioritize their cybersecurity, given the potential severe consequences of a cyberattack. Therefore, it is encouraging to see that the majority of students are taking the necessary precautions to ensure their online safety. It is important for all individuals, not just students, to continue to educate themselves on the latest cyber security practices and to take the necessary steps to protect their online presence.

REFERENCES

1. Hemmerdinger J. (2022). Gen Z and millennials less serious about cybersecurity on work-issued devices than personal. [online]. Ernst & Young. Available from: https://www.ey.com/en_us/newsroom/2022/10/gen-z-and-millennials-less-serious-about-cybersecurity-on-work-issued-devices-than-personal-according-to-new-ey-consulting-survey
2. Bingham A, Kulik A. (2022). Scam Fighters Answer Scam Questions from Twitter (ft. Trilogy Media), Tech Support. [online]. WIRED. Available from: https://www.youtube.com/watch?v=GrZi2pHnoQg
3. Al Shamsi AA. Effectiveness of cyber security awareness program for young children: a case study in UAE. Int J Inform Technol Lang Stud. 2019; 3 (2): 8–29.
4. Khudyntsev M, Davydiuk A, Lebid O, Trofymchuck O, Zhylin A. Cybersecurity Indices: Review and Classification. In: CEUR Workshop Proceedings. CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, Ukraine, October 26, 2021. Pp. 117–126.

5. Chalmers DJ. The Conscious Mind. Oxford, UK: Oxford University Press; 1996.
6. McDonald C. (2016). Most students say cyber security is a growing threat. [online]. ComputerWeekly.com. Available from: https://www.computerweekly.com/news/4500278781/Most-students-say-cyber-security-is-a-growing-threat
7. Tiwari P, Banerjee S. Cybersecurity Laws and Regulations India 2024. International Comparative Legal Guides and International Business Reports. Luxembourg: Global Legal Group; 2023.
8. Zhamburbayeva S. Improvement of legal acts regulating representation on someone's behalf in civil proceedings. Bull Karaganda Univ Law Series. 2022; 107 (3): 109–117.
9. Maneela. Cyber crimes: the Indian legal scenario. US-China Law Rev. 2014; 11: 570–584.
10. Reddy GN, Reddy GJ. A study of cyber security challenges and its emerging trends on latest technologies. Int J Eng Technol. 2014;4(1). DOI: 10.48550/arXiv.1402.1842.

