International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||04||Pages||1144-1158||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i04.ec05

An Empirical Study on Cybersecurity Awareness, Cybersecurity Concern, and Vulnerability to Cyber-attacks

Chahak Mittal

Eastern Michigan University, United States

Abstract

The research aimed to delve into the landscape of cybersecurity awareness and concern levels within Punjab, India, shedding light on the specific demographic groups most susceptible to cyber-attacks. Through meticulous survey administration and data analysis, the study pinpointed a noteworthy vulnerability: young adult females aged 18 to 29 residing in rural Punjab, particularly those either engaged in student pursuits or currently unemployed. This demographic emerged as disproportionately prone to cyber threats.

Highlighting the gravity of this finding, the research underscores the urgency for tailored interventions to fortify the cyber defenses of this vulnerable population segment. A crucial facet of this approach involves the development of a prototype aimed at augmenting cybersecurity awareness and fostering ethical online conduct among the identified demographic. This prototype seeks to serve as a platform for delivering enhanced training modules tailored to the unique needs and challenges faced by young females in rural Punjab.

Moreover, the paper delineates a comprehensive roadmap for the implementation and evaluation of these recommendations. Central to this plan is the deployment of an application based on the proposed prototype, designed to facilitate the delivery of targeted cybersecurity education and gauge its efficacy in bolstering cyber resilience among the identified demographic.

This research not only illuminates the cybersecurity landscape in Punjab but also charts a proactive course of action aimed at mitigating vulnerabilities and empowering at-risk populations through informed intervention strategies. Through ongoing data collection and evaluation efforts, the efficacy of these interventions will be rigorously assessed, driving iterative refinement and optimization of cybersecurity initiatives tailored to the unique needs of Punjab's populace.

Keywords: Cybersecurity awareness, Cyber-attacks, Cybersecurity concern level, Cybersecurity vulnerability

Introduction

Modern society is progressively driven by cutting-edge innovative technology. However, the ever-increasing reliance on electronic gadgets and Internet-based systems has been challenged by increasing cyberattacks on businesses, organizations, governments, and common people around the world. The convenience of using internet leads to increase of cybercrimes. With ever increasing internet usage, the vulnerabilities among users are also growing (Shah, 2019). While convenient and popular, the online innovation isn't without its problems and challenges that may lead to cybercrime. The nature of cybercrimes in the global scene has evolved significantly with the increased dependence on technological innovations and advancements. Consequently, globally data protection has become a perplexing and rapid security challenge during this time of Information Communication and Technology. In the business world, the consequences of cybercrimes include but not limited to setback to the brand image and reputation or goodwill of the business, loss of intellectual property and sensitive data, service and employment disruptions, cost of countermeasures and insurance, cost of mitigation strategies and recovery from cyber-attacks - all these led to the economic losses. Even with relevant laws and regulations in one form or another, in some advanced nations in the world, the challenge of cybercrimes remains intractable and bewildering. As nations across the globe strive

to curb cybercrimes through the law, so are the cyber criminals devising new sophisticated techniques to further their skill for malicious purposes (Ajoy, 2016).

In the past, significant cyber-crimes included online scamming and phishing schemes. Current cyber-attacks and hacks are more advanced with the capability of disrupting critical operations and infrastructure (Pattnaik & Mishra, 2020). Cybercrime revolves around criminal computer activities as well as the traditional aspects, such as fraud, theft, blackmail through ransomware attacks, etc. The weakest link in the cybersecurity chain is the human as 95% of security breaches are blamed on human error (Roohparvar, 2021). While some people are concerned about cybersecurity; most of them do not comprehend the severity and serious consequences of lack of it, hence do not take precautions to protect themselves from cyberattack. A wide range of factors influence people's online security practices.

In the present innovative and electronic world, shielding from the cyberattacks and finding a right way to anticipate those attacks is a critical need. The carelessness and obliviousness in managing digital data led to cyber security dangers. With simpler access to data these days, sensitive data such as passwords, web-based media profiles are frequently hacked. Data compromise, monetary misfortune, and wholesale fraud possible through Wi-Fi, especially when using public computers. Therefore, having a great awareness of cybersecurity is vital and seriously needed. The most ideal method for defeating digital wrongdoing is through prevention, which can be ensure by cyber security awareness (Kader, 2020).

Literature Review

◆ Define Cybercrime

Cybercrime, a concept which to date has defied a globally accepted definition, describes a very broad category of online offenses. According to Shah (2019), cybercrime is a crime which is performed using computer and internet to extract information from any other computer or device. The experience of cybercrime is universal among individual, corporate, organization, national, multinational or international who are involved in the use of the computer and Internet; especially, with the unavoidable nature of using the cyberspace for social interaction, global trade and commerce are transacted (Ajoy, 2016). Some of the cybercrimes are the similar to the non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Other cybercrimes such as hacking are uniquely related to computers and internet (Kumar & Manhas, 2021).

◆ Cybercrime in India

According to the India's National Crime Records Bureau cyber criminals perform cybercrimes to earn money, to become famous, to just have fun, to sexually exploit, to blackmail, to develop own business, to sell or purchase illegal contents, to take a revenge, or to do a prank, and so on. The main advantage the criminals have is that they are not easily traceable to perform their activities using the internet since it is extended globally. Tracing the location and person behind this criminal activity is a very difficult task because it can be performed from anywhere around the world. In India, these types of crimes are reported and resolved under IT Act 2000 and Indian Penal Code (Shah, 2019).

India saw a significant jump in cybercrimes reported in 2020 from the previous year. Over 50 thousand cybercrime incidents were registered in 2020. India is moving towards a digital era with Internet connection, which allows users to share information using network connected devices. In India, for the last few years, usage has been increasing at a very high rate. Nowadays, every essential task such as shopping, paying bills, transfer of money, business transactions, global communications, etc. are heavily dependent on the Internet. Globally India ranked second in internet users as people in India are having internet connected devices (Shah, 2019). India also ranked 11th worldwide in the number of cyberattacks that were hosted in the country, accounting for 2,299,682 incidents in the first quarter of 2020 as compared to 854,782 incidents detected in the fourth quarter of 2019 (Kumar & Manhas, 2021).

Vimala and Vishalini (2021) in their study on the cyber security threats and challenges in India, emphasized on the significance of network protection in India as government, military, corporate, clinical and financial organizations gather, cycle and store extraordinary measures of information on PC. Sensitive information

transferred across networks and to different gadgets to store it. Discussing about various categories of cybersecurity and what are some of the recent challenges being faced in India, they stated that Indians are utilizing Internet for shopping and banking, putting away their personal sensitive information. Therefore, network safety issue must be tackled unequivocally (Vimala & Vishalini, 2021).

In general, there are two types of cybercrimes: *Persistent cybercrimes* and *Emergent cybercrimes*. *Persistent cybercrimes* such as tampering with computer source document, publishing obscene information online, non-compliance with policy, attempting to secure access to a protected system, misinterpretation, breach of confidentiality and privacy, false digital signature certificate publication and fraud digital signature were recorded repetitively in consecutive years under IT Act 2000. Also, crimes such as forgery, criminal breach of trust, counterfeiting and destruction of electronic evidence has been recorded persistently under Indian Penal Code. Although at a relatively less high rate, *Persistent cybercrimes* are occurring repetitively in India; therefore, these crimes are required to be monitored by the government of India to prevent and control the occurrence of it (Shah, 2019). *Emergent cybercrimes*, occurring without any prior indication, are those crimes which are not repetitive but are newly observed. Cybercrimes such as hacking, publishing of threatening information, cheating, receiving stolen communication device or computer, cyberterrorism, publishing of people's private images, obscene information, images containing sexual acts, child pornography, and identity theft have been emerged under IT Act 2000 in India. Also, crimes such as data theft, cheating, and credit/debit card frauds have emerged at a very high rate under Indian Penal Code. Since, the newly emerged crime does not have any previous history, the growth rate of such crime is very high. To handle such incidents, the government of India is required to keep themselves updated and ready to tackle any new emergent crime at any time (Shah, 2019).

Studying the rising trends of internet usage and the vulnerabilities faced by the users in India, Shah (2019) concluded that the growth rate of cybercrime increases with the increase in internet usage in India. Shah also studied the trends of reported cybercrimes in India under IT Act 2000 and Indian Penal Code during 2012-16 and analyzed the persistent as well as emergent types of cybercrimes occurring along with the prevention measures taken by government of India during those years (Shah, 2019).

Singh and Rishi (2015) in their case study on cyber security in India, conducted contextual analysis on a cyber security organization, which has practical experience in computerized wrongdoing, extortion and criminology arrangements and administrations in India. With the versatility, adaptability and monetary benefit offered by distributed computing, an ever-increasing number of associations are moving towards cloud computing that opens up to the threat of advanced computing wrongdoing and security breaks on the cloud stage.

◆ Cybercrime Laws and Policies in India

Reviewing the challenges to enforcement of cybercrimes laws and policy, Ajayi (2016) stated that there are applicable laws across the globe managing digital violations yet the difficulties of implementation of those laws continues. There is the shortfall of a worldwide agreement on exactly what leads to cybercrimes, the absence of consistency between the diverse public procedural laws concerning the examination of cybercrimes, the absence of synchronized law implementation components that would allow global collaboration in cybercrimes prevention (Ajayi, 2016). Evaluating the contrasting cases of the impact of cybersecurity infrastructure on economic development in India and Pakistan, Baker (2013) set up a model to investigate digital laws between two countries. Their research showed various levels in the status to make online safety strategy or NII (National Information Infrastructure) security procedure. Analyzing the causes, consequences and implications of cybercrimes in India, Kshetri (2016) proposed that formative, institutional and global relations issues are important to prevent cybercrimes and ensure network protection in agricultural nations. The study draws together a wide assortment of exploration from various fields like criminal science, global political economy, worldwide relations, institutional hypothesis and formative financial matters to inspect cybercrimes and network protection in India. Discussing the use of a structure regarding cybercrimes and online protection in India, Kshetri (2016) specified how the extraordinary highlights of the Indian double economy are associated with various perspectives of cybercrimes and online protection (Kshetri, 2016).

Focusing on the issues of cyber security and cyber laws in India, Pathak (2017) specified how the ideas of network protection and digital laws are rapidly getting the most significant attention to the government as well as the public in India. In a country like India that increasingly advances towards digitization of its economy, the concern for cyber security is significant (Pathak, 2017). Numerous areas of India's economy would halt assuming any digital attack did indeed occur. In the 21st century, a period of globalization, the internet rules. Exchanges worth billions move of incredibly delicate data and so forth occur consistently. Clarifying the present network safety and digital law system of India, its operations and the issues being looked by it, Pathak (2017) said one may well envision the misfortunes that countries or people will encounter if there is cyber-attack.

Based on an empirical analysis on cybersecurity behavior of smartphone users in India, Shah and Agarwal (2020) mentioned that for many Indians, their cell phone is their first advanced gadget. They have less involvement with managing the Internet-empowered gadget and consequently less involvement with taking care of safety from malware compared to the people in other countries who have gone through the expectation to learn and adapt of taking care of cyber security threats. The unpracticed Indian cell phone users might be powerless against cyber security breaks. Thus, it is fundamental to comprehend the disposition, conduct and security practices of cell phone clients in India (Shah & Agarwal, 2020).

There are many research findings that show people's demographic background play a vital role in their cybersecurity awareness and concern level. Anwar et al. (2017) found that females have lower computer efficacy than males, which may make them vulnerable or prone to cyber-attacks. Also, it is a well-known fact based on much research that senior citizens are quite possibly the target of cyberattacks.

◆ Research Objectives

After reviewing the literature on cyber security, especially in India, we determined to survey how the people in India in different age groups, gender, geographical, educational background, and working history perceive cybersecurity. The objective of this research was to find the segment of population that is most vulnerable based on survey and analysis, study their surroundings and propose an effective cyber security awareness training program. A significant research question to explore was to what extent demographic factors play a role in mediating the factors that affect cybersecurity awareness and online behaviors of individuals.

The survey-based research was conducted in Punjab, a state in north India, where one of the highest cyber-attacks has been recorded in 2019-2020. The specific purpose was to understand how people in Punjab in different age groups, gender, geographical, educational background, and employment history perceive cybersecurity, their cybersecurity awareness and concern level, and which segment is most vulnerable or prone to cybersecurity attacks. The specific research questions that this study attempted to address were: What effect people's age, gender, education, employment, location of residence has on their cybersecurity awareness, cybersecurity concern level, and vulnerability to the cyber-attacks in Punjab, India?

Methodology

◆ Survey Instrument Development

A Web-based survey instrument (Appendix) was developed. The draft instrument was reviewed by an expert panel. The instrument was a set of pre-verified and designed questions, modified per the research goal. The questions in the survey were consisted of demography and the behavioral aspects of the individuals. The survey was intended to be conducted among random people of various age groups, genders, educational background, occupation, locations (urban or rural areas) in Punjab, India. The four independent variable constructs were subcategorized. Educational background factor was sub-categorized into *No Education*, *Undergraduate*, and *Post-Graduate* since the purpose of the analysis is to understand awareness with educational level rather educational program such as engineering, business, etc. Employment status factor was sub-categorized into to *Un-employed* - people with no Job, *Employed*- people currently working, and *Students* - people currently studying. Age factor was break down into 18-25, 26-35, 36-49, and above 50 sub-categories.

The survey questions were divided into three categories based on the three depended variables:

- Cybersecurity awareness
- Cybersecurity concern level
- Prone or vulnerable to cyber-attacks

◆ **Data Collection Process**

After receiving permission from the Institutional Review Board, an invitation to participate in the research was sent via e-mail to the prospective participants in Punjab, India. They were provided a link to the Web-based survey including instructions and study information. They were requested to read the study information before participating in the Web-based survey. The study information informed them of their rights as participant and stated that their participation in the survey was completely voluntary and anonymous. The completion of the Web-based survey was considered as evidence of their willingness to participate in the study. To increase the response rate further, two weeks after the initial e-mail, a follow-up e-mail was sent to all prospective participants as a reminder to participate in the Web-based survey.

Results And Discussion

Survey Data

A total of 61 survey records were received, which is shown below as the breakdown of the survey records.

Table 1: Survey Data

Gender Survey Records		
Categories	**Survey Records**	**% of Total Survey Records**
Male	47	77%
Female	14	23%
Employment Survey Records		
Categories	**Survey Records**	**% of Total Survey Records**
Student	11	18%
Employed	44	72%
Un-employed	6	10%
Geographical Survey Records		
Categories	**Survey Records**	**% of Total Survey Records**
Urban	57	93%
Rural	4	7%
Age Survey Records		
Categories	**Survey Records**	**% of Total Survey Records**
18-25	17	28%
26-35	10	16%
36-50	12	20%
Above 50	22	36%
Education Survey Records		
Categories	**Survey Records**	**% of Total Survey Records**
No Education	0	0%
Undergraduate	35	57%
Post Graduate	26	43%

◆ **Data Analysis**

The 61 surveys records were analyzed to develop a correlation between *Cybersecurity Awareness*, *Cybersecurity Concern Level*, and *Prone or vulnerable to Cyber-attacks* to various demographic criteria such Age, Education, Gender, Employment Status, and Geographical Area. The scores of those three categories were normalized (Score out of 20) to maintain uniformity in the analysis. For normalization, the total score of each person for each of the aforementioned categories was divided by the total scope and then multiplied by 20.

◆ ***Age***

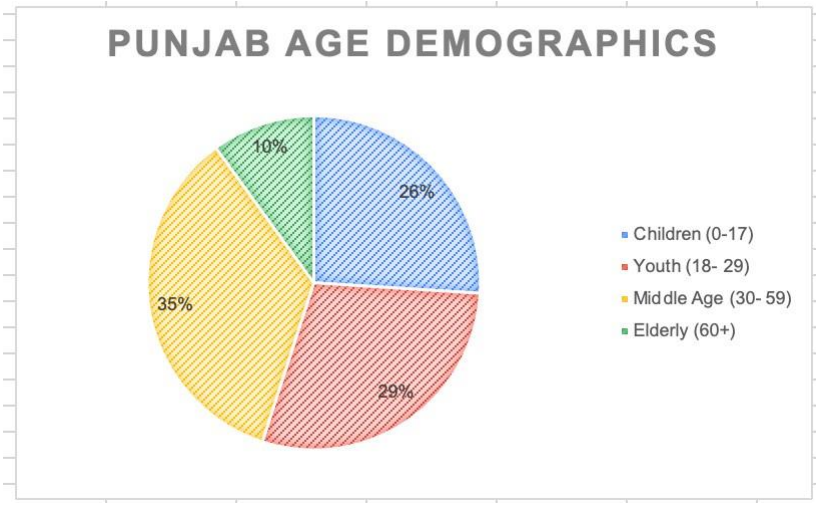

Figure 1: Punjab Age Demographics (Punjab population 2011 - 2022)

On plotting the graph between *Cybersecurity Awareness*, *Cybersecurity Concern Level*, and *Prone or vulnerable to Cyber-attacks* against age, it was observed that with more age people are more aware of cybersecurity and are more interested in learning about cybersecurity. It was also observed that younger people are more prone to cybersecurity attacks. As the result shows that in the age sub-categories people above 50 years are most aware of cyber security (36%), followed by 18-25 (28%), 36-50 (20%), and 26-35 (16%). Therefore, there is a positive correlation between age and *Cybersecurity Awareness*, *Cybersecurity Concern Level* constructs. However, there is negative correlation between age and *Prone or vulnerable to Cyber-attacks* construct.

The results were surprising as one may think the younger people have been using technology for their entire lives, so they should be more aware of cybersecurity challenges. On the contrary, the survey shows that younger people often underestimate the impact of cyberattacks. We believe the cybersecurity problem requires people to implement good security practices which normally takes time to implement and comes in the way of young worker's productivity. Therefore, to make younger people more cyber secure one would have to think of ideas that don't hamper productivity and make them more cyber safe.

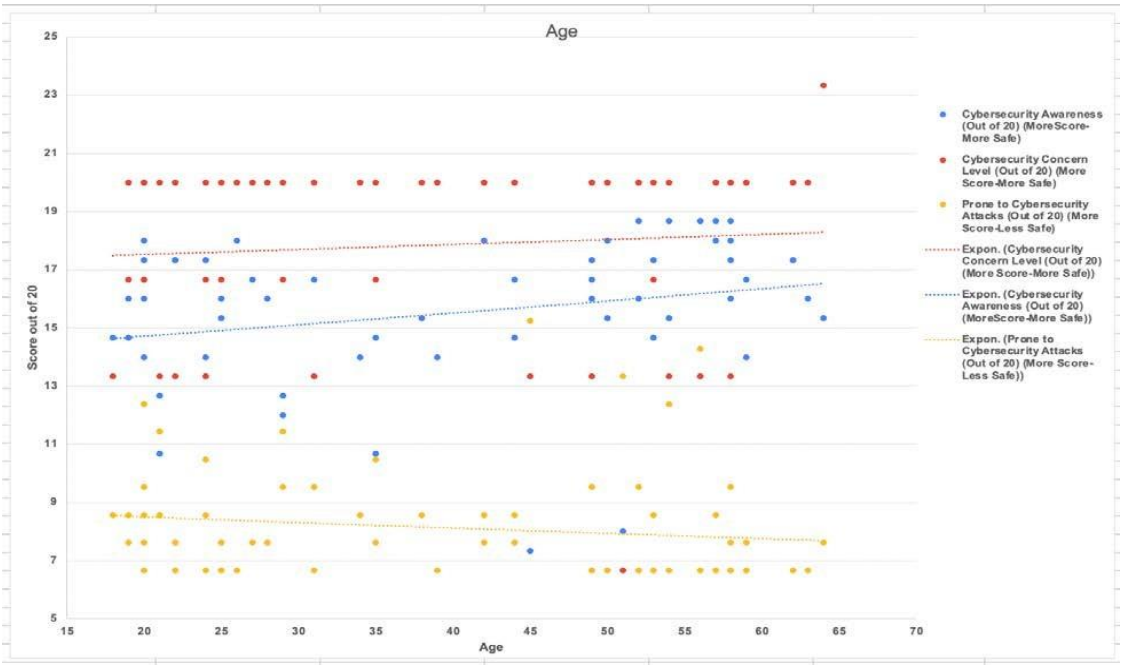

Figure 2: Survey data analysis based on age

◆ ***Education***

Average literacy rate in Punjab is 75.84% with male literacy 80.44% and female literacy 70.73% (Punjab population 2011 - 2022). No surveying data was recorded for people with no education. Therefore, the results of this category are not yielding any conclusions. The cybersecurity awareness, cybersecurity concern level, and prone to cyberattacks are comparable between people with under graduation (57%) and post-graduation (43%). It would be very interesting to have surveys for people with no education and analyze the results with educated. As a next step, we also recommend analyzing, how different education disciplines such as engineering, medical, commerce, business, etc. compare to each other. We believe this will help us identify people in which education program is lagging in cybersecurity awareness and are more prone to cybersecurity attacks. Using this data, we can develop education program-specific awareness programs and target the segments which are at more risk.

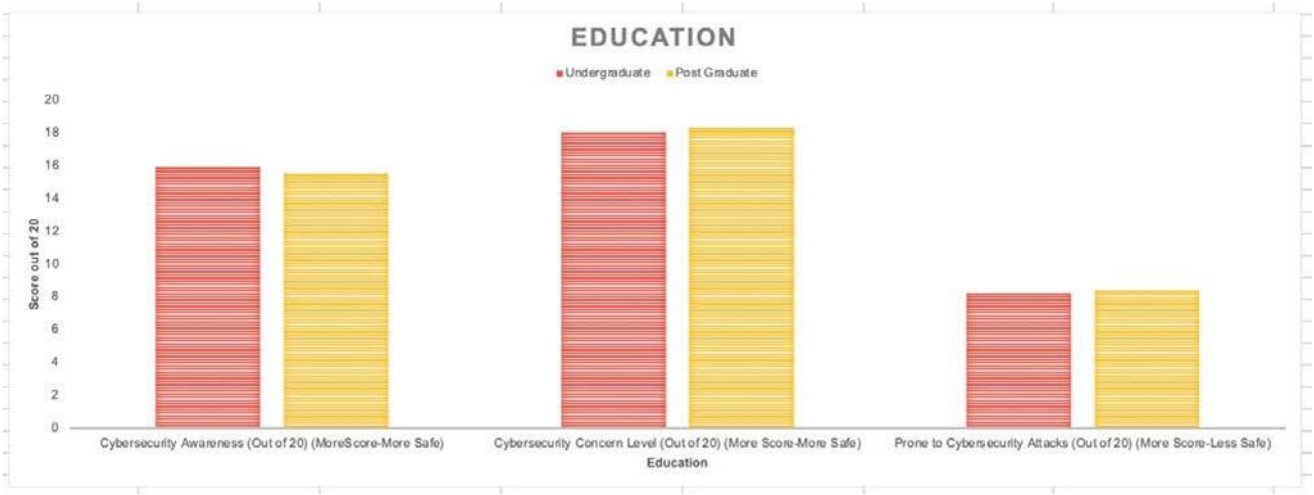

Figure 3: Survey data analysis based on education

◆ ***Gender***

According to the India demographics department, Punjab had 47.2% Females and 52.8% males (Punjab population 2011 - 2022).

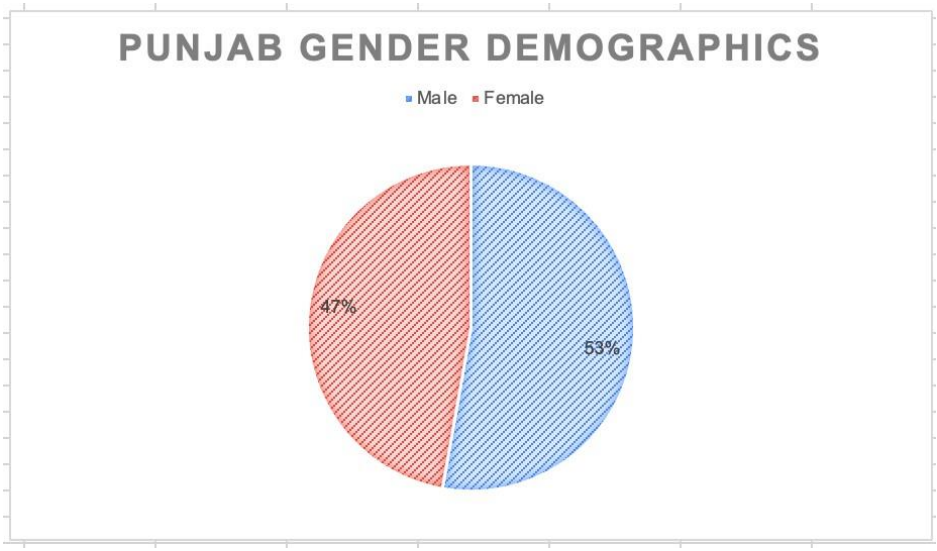

Figure 4: Punjab Gender Demographics. Source: Punjab population 2011 – 2022.

Per our survey data, males are more aware of cybersecurity and have higher concerns (77%) than females (23%). The survey analysis also shows, females are significantly more prone or vulnerable to cybersecurity attacks. It is believed that the gender-based difference might be related to gender gaps in computer skills, prior experience, and computer self-efficacy. Self-efficacy refers to an individual's belief in their capacity to

execute behaviors necessary to produce specific performance attainments. Rhee et al. (2009) found that individuals with higher self- efficacy in information security use more security protection software and that individuals with higher self-efficacy in information security demonstrate more security-conscious care behavior. The female's computer self-efficacy was observed significantly lower than men's (Anwar, 2016).

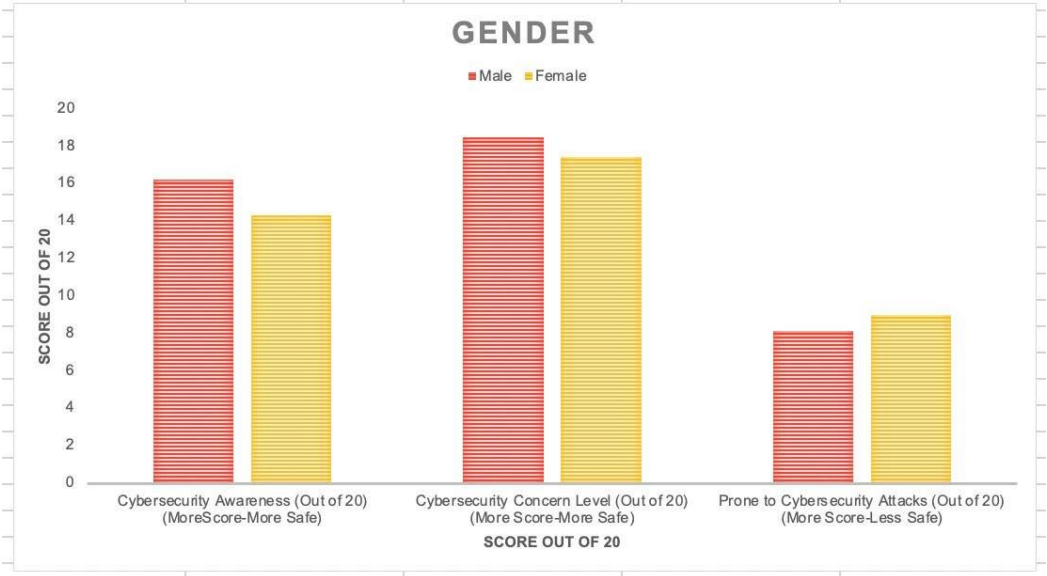

Figure 5: Survey data analysis based on gender

◆ ***Employment Status***

Out of Punjab's population as shows below in graph, 36% is employed, 31% is unemployed and 33% is currently studying (Official website of employment generation, Punjab 2021).

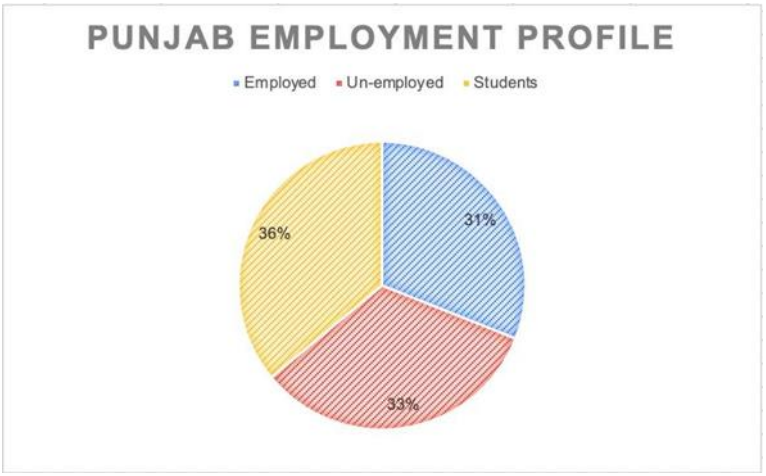

Figure 6: Punjab Employment Demographics. Source: Official website of employment generation, Punjab 2021.

From the surveys in our research, it was observed that employed people are most cybersecurity aware (72%), followed by students (18%), and unemployed (10%). This might be because the companies have employed cybersecurity awareness programs expecting good online behavior from employees. It is evident that students and unemployed people are significantly less aware of cybersecurity and are more prone to cybersecurity attacks.

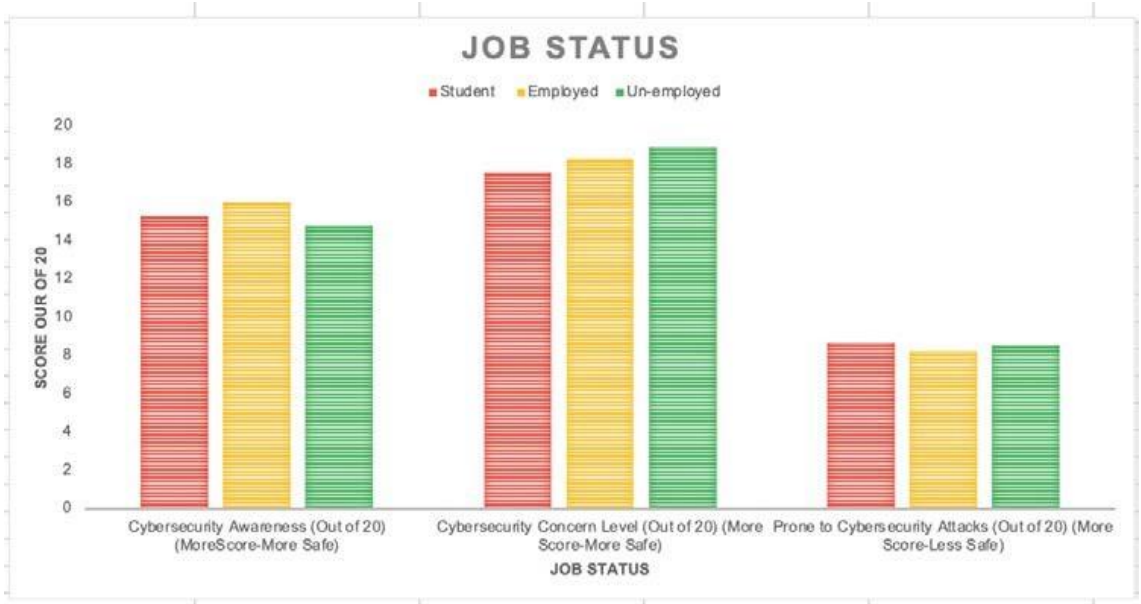

Figure 7: Survey data analysis based on employment status

On further analyzing the inference from above with Punjab's employment profile by gender, where only 14% of the total employed population is women. This leads to the majority of the population of students and unemployed women. Hence, women are at greater cybersecurity risk.

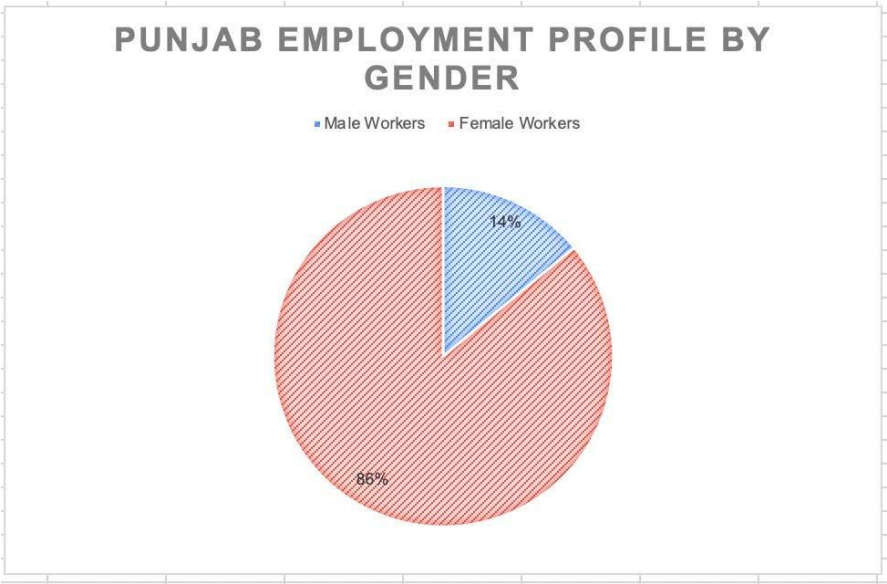

Figure 8: Punjab Employment Profile by Gender. Source: Department of Planning Punjab.

◆ ***Geographical Data***

The majority of Punjab's population lives in rural areas with 63% and only 37% in urban areas (State Profile – Government of Punjab, India)

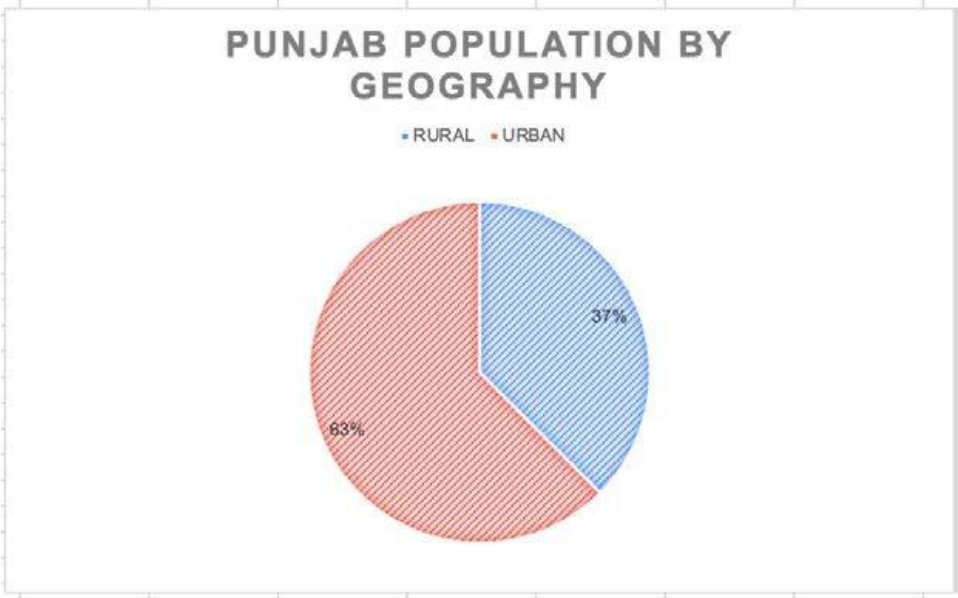

Figure 9: Punjab Population by Geography. Source: State Profile – Government of Punjab, India.

The research survey records showed that rural people are significantly less aware and concerned about cybersecurity (7%) compared to urban people (93%). The rural people are prone to cyberattacks and hence at higher risk. The same cyber-attacks in rural cities can have as many significant consequences. The large cities in Punjab may have a significantly higher financial and operational impact on awareness and concern about cybersecurity.

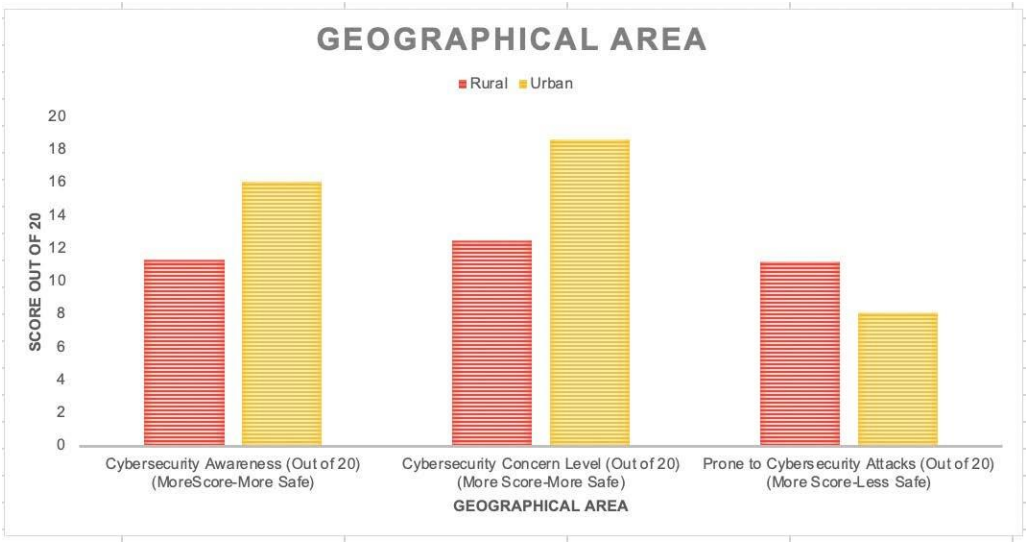

Figure 10: Survey data analysis based on geographical area

Conclusion And Recommendation

The prevalence of cybercrimes is on the rise, prompting proactive measures by the Indian government to enhance public awareness and prevention. These initiatives include dissemination of cyber awareness through various channels such as newspaper articles, radio and television advertisements, as well as email and text message campaigns aimed at promoting safe online practices. Additionally, the government has facilitated the accessibility of reporting mechanisms by developing mobile applications and websites dedicated to reporting cybercrimes. Despite these efforts, a significant portion of the population in Punjab, India harbors concerns regarding cybersecurity, yet only a minority actively seeks to educate themselves and adopt preventive measures.

The efficacy of current awareness and training programs is questioned, with a perceived lack of interactive engagement hindering their impact. Many existing programs are critiqued for their technical complexity,

rendering them inaccessible to the general audience without requisite educational backgrounds. It is observed that these programs often fail to resonate with their intended recipients, as they lack contextual relevance and fail to address the diverse needs of the target audience. Moreover, a one-size-fits-all approach to cybersecurity education is deemed inefficient, necessitating tailored programs that cater to the specific requirements and comprehension levels of the audience.

Addressing these concerns requires a paradigm shift in the development and delivery of cybersecurity training programs. A focus on audience-centric curriculum design, coupled with the integration of practical, relatable examples, is essential to fostering meaningful engagement and comprehension among participants. By aligning training initiatives with the knowledge and learning preferences of the target demographic, the effectiveness of cybersecurity awareness programs can be significantly enhanced, thereby mitigating the risks posed by cyber threats.

◆ **Recommend Realistic Training**

To encourage secure online behavior, we recommend training people using entertaining games that are similar to their real-life experience that they can relate to. Per the survey data and analysis of our research, we found that young adult females from the age group 18 to 29 living in rural Punjab who are students or unemployed are more prone to cyberattacks.

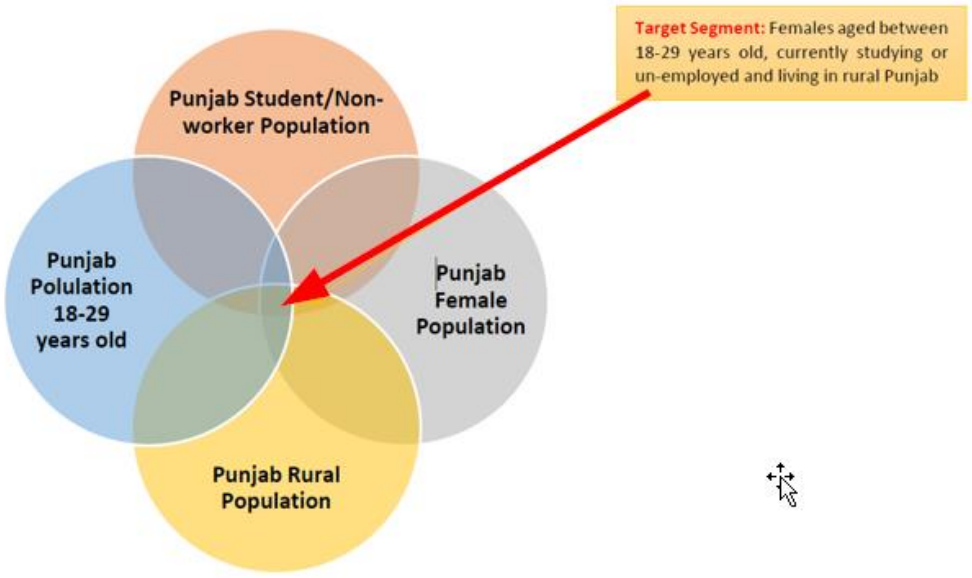

Figure 11: Venn Diagram - most vulnerable segment of population in Punjab, India.

The low computer self-efficacy may be very well the reason for making these girls in India vulnerable to cyber-attacks (Rhee et al., 2009). It makes us think if the current highly technical cybersecurity training program is not helping the cause but rather further lowering the self-efficacy in the many end users. The games that target the improvement of computer self-efficacy can encourage good and secure online behavior (Chen et al., 2019). In this context, our proposal would provide a decision-making tree that will form the basis of a television/streaming show and animated game that would target the females in the most vulnerable segment discussed above. This decision tree is the first step to develop transformative television/streaming shows and cybersecurity game apps that will be effective and well-received by different audiences who are vulnerable to cyber-attacks.

◆ ***Cyber Safe Meena***

'Meena' is a fictional girl character that was created by UNICEF in India to educate children on issues of gender, health, and social inequality through her stories in comic books, animated films (Meena Cartoon), and radio series (affiliated with the BBC). We propose to use the popular Meena character to teach

especially these vulnerable girls about cybersecurity because of the trust Meena has developed with rural girls for over the decades. Consequently, using this popular character, we have proposed a cyber security prototype called “Cyber Safe Meena”.

Figure 12: Meena Cartoon by UNICEF

◆ ***Proposed Cyber Security Prototype***

As a first step towards this great initiative, we created a prototype decision-making tree for “How to Avoid a Scam Call?” The decision tree takes Meena through series of questions to help her make the right decision in online interaction.

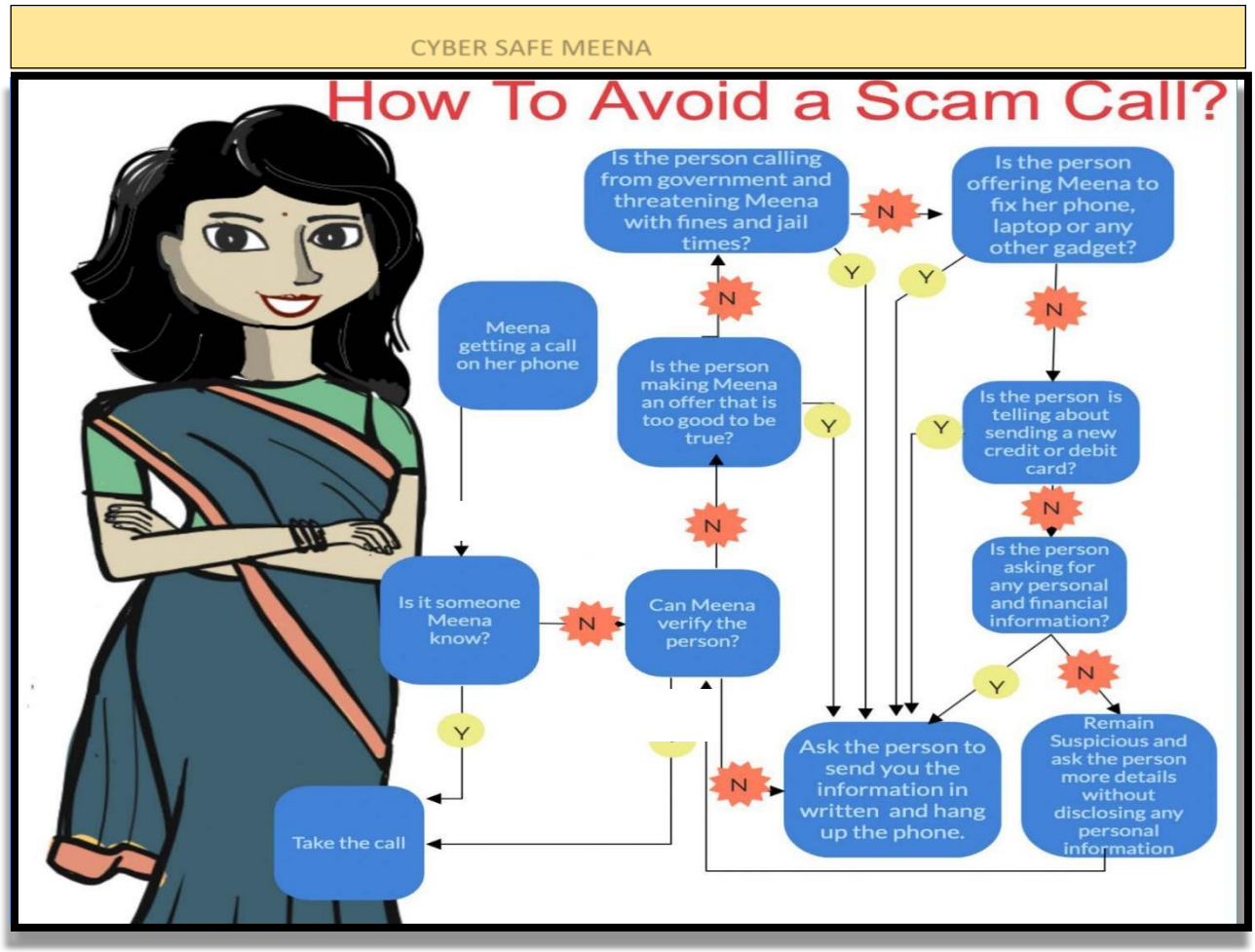

Figure 13: Cyber safe Meena Prototype

Implications for Research and Practice

This recommended cybersecurity awareness approach expected to be more effective than the traditional cybersecurity awareness training programs as it is:

1. More Immersive - gives training to the audience in the realistic environment
2. Persistent - allow users to actively learn from success and failure
3. Higher Retention - Improved retention of cybersecurity lessons
4. Not Generic - Specific to the target audience's surroundings and environment
5. On-demand - It can be integrated into the daily workflow

Proposed Future Work

Mindfulness through better prevention is consistently a need at this crossroads. Education pace of women isn't equivalent to that of men in India. Especially, cyber education or awareness is substantially less among women compared to men although regardless of gender identity all online users are inclined to cyber-attacks with same serious consequences. In fact, women are more misled by schemers or hackers than men are. Therefore, appropriate measures ought to be there to provide information regarding cyber security risks and how to handle those challenges.

As a next step, in our future research will focus on understanding what specific cyber-attacks rural females are exposed to and further develop these decision trees effective for those various high-frequency cyber-attacks. To create mass awareness, this research proposes to check the scalability of this program to other states in India too. Also encourages partnering with UNICEF to develop television shows, apps, etc. to penetrate into rural Punjab audience and educate them about cyber-attacks.

In this research, educational background factor was sub-categorized into *No Education*, *Undergraduate*, and *Post-Graduate* since the purpose of the analysis was to understand cyber security awareness based on educational level rather educational program such as engineering, computer, business, etc. However, it would be an interesting analysis of cybersecurity awareness with different educational programs or disciplines, which will help us to identify specific fields that are more prone to cybersecurity attacks.

Additionally, the employment status factor was sub-categorized into to *Un-employed* - people with no Job, *Employed*- people currently working, and *Students* - people currently studying. The respective fields of work/employment were not analyzed as part of this study. It is however recommended to study the level of awareness among people employed in different departments within the organization assuming this will help companies to develop the training programs by the departments and the type of cyber-attacks they are prone to. Organizations need to come up with new ways to increase cybersecurity awareness among their employees. While technology can filter out most attacks, it cannot eliminate every threat. Employees represent the last line of defense and they should be educated on cybersecurity, how to deal with potential threats, and how to report them (Roohparvar, 2021).

References

1. Anwar, M., He, W., Ash, I., Yuan, X., Li, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Information Technology & Decision Sciences Faculty Publications*. 13.
2. Ajayi, E. F. G. (2016). The challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems, 6*(1), 1-12.
3. Baker, E. W. (2013). A model for the impact of cybersecurity infrastructure on economic development in emerging economies: Evaluating the contrasting cases of India and Pakistan. *Information Technology for Development, 20*(2), 122-139. https://doi.org/10.1080/02681102.2013.832131
4. Chen, T., Hammer, J., & Dabbish, L. (2019). Self-efficacy-based game design to encourage security behavior online. Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3290607.3312935
5. Department of Planning Punjab. (n.d.). Retrieved on January 28, 2022 from: https://pbplanning.gov.in/reports.htm
6. Demographics of population ageing in India. (n.d.). Retrieved on November 22, 2021 from: http://isec.ac.in/BKPAI%20Working%20paper%201.pdf.

7. Kader, A. N. (2020). Cyber security awareness- a necessity for more productive digital experience. *IJRAR- International Journal of Research and Analytical Reviews, 7*(2). https://doi.org/E ISSN 2348 –1269, print ISSN 2349-5138.
8. Kshetri, N. (2016). Cybersecurity in India. *The Quest to Cyber Superiority*, 145-157. https://doi.org/10.1007/978-3-319-40554-4_8
9. Kumar, S. & Manhas, A. (May 2021). Cyber crimes in India: Trends and prevention. *Galaxy International Interdisciplinary Research Journal* (GIIRJ) ISSN (E*): 2347-6915. 9*(5).
10. Official Website of Employment Generation, Skill Development and Training Government of Punjab, India. (n.d.). Retrieved on March 28, 2021 from: https://pbemployment.punjab.gov.in/
11. State Profile – Government of Punjab, India. (n.d.). Retrieved on January 28, 2022 from: https://punjab.gov.in/state-profile/
12. Pathak, U. (2017). Cyber security and cyber laws in India: Focus areas and issue areas. *The Clarion-International Multidisciplinary Journal, 6*(1), 51-56. https://doi.org/10.5958/2277-937x.2017.00008.9
13. Pattnaik, P. K., & Mishra, I. (2020). Cybercrimes in India and related laws. *Psychology and Education, 57*(9), 757-760.
14. Punjab population 2011 - 2022. Punjab Population Sex Ratio in Punjab Literacy rate data 2011-2022. (n.d.). Retrieved on January 28, 2022 from: https://www.census2011.co.in/census/state/punjab.html
15. Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008
16. Roohparvar, R. (May 23, 2021). People – the weakest link in cybersecurity. Infogurd – Cyber Security. Retrieved from: https://www.infoguardsecurity.com/people-the-weakest-link-in-cybersecurity/
17. Shah, P., & Agarwal, A. (2020). Cybersecurity behavior of smartphone users in India: An empirical analysis. *Information & Computer Security, 28*(2), 293–318. https://doi.org/10.1108/ics-04-2019-0041
18. Shah, R. (2019). Cyber crimes in India: Trends and prevention. *International Journal of Research and Analytical Reviews (IJRAR), 6*(1). www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138)
19. Singh, N., & Rishi, A. (2015). Pyramid: A case study of cyber security in India. *South Asian Journal of Business and Management Cases, 4*(1), 135–142. https://doi.org/10.4135/9781526405470
20. Vimala, S. C., & Vishalini, S. P. (2021). Cyber security: Threats and challenges in India. *International Journal of Advanced Research in Science, Communication and Technology, 2*(3), 128-131. https://doi.org/10.48175/ijarsct-v2-i3-322.
21. Wikimedia Foundation. (2021, November 4). Meena (character). Wikipedia. Retrieved November 22, 2021. Retrieved from: https://en.wikipedia.org/wiki/Meena_ (character).

APPENDIX
Survey Questions

Questions under the three categories comprise of:

- ✓ ***Cybersecurity Awareness***
- ✓ Do I apply privacy settings to my profiles, photographs, and other information on the Internet or social media?
- ✓ Do I read the terms and conditions when installing any application on my smartphone or any other electronic gadget?
- ✓ Do I read or comply with the government guidelines and policies on how to be secure online?
- ✓ Do I verify the name, email address, phone number, and other information before responding to an unknown email?
- ✓ Do I regularly update my mobile applications?
- ✓ Do I validate the background check of a person who asks for my information on a phone call/message/email?
- ✓ Do I log out of online applications when I am not using them?
- ✓ Do I know what cybersecurity is?

- ✓ If I am suspicious about someone I am communicating with via email or online, do I discuss it with my friends/parents/siblings/teacher?
- ✓ Do I share my passwords with anyone?

I. Cybersecurity Concern Level

- ✓ Does it bother me if my information is used by anyone without my permission?
- ✓ Does learning about how to be secure online, interests me?

II. Prone to Cybersecurity Attacks

- ✓ Do I click on any link or attachment in an email or message sent by unknown people?
- ✓ Do messages or emails like' gift-card, 'sale' or 'free coupon' lure me to click on any link on the internet?
- ✓ Do I share my personally identifiable or sensitive information on Social Networking Sites?
- ✓ Have I ever been a victim of online banking fraud?
- ✓ Have I encountered that my sensitive information or photograph being used somewhere without my knowledge?
- ✓ Has my credit card ever been used to conduct a transaction by someone without my knowledge/permission?
- ✓ Do I take information security and privacy casually?