Need of Cyber Security Education in School

Lohote Prathamesh Yashwant
Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Otur, Pune India

Abstract **- Cyber security is a concern for all modern organizations. These organizations cannot achieve their cyber security goals through hardware and information technology (IT) workers alone, so all employees who use computer networks must be trained on the knowledge, skills and policies related to cyber security. This paper reviews what is known about effective cyber security training for end users of computer systems the fact that the Internet has positively impacted people's lives, there are negative issues emerged related to the use of Internet. Cases like cyber-bully, online fraud, racial abuse, pornography and gambling had increased tremendously due to the lack of awareness and self-mechanism among Internet users to protect themselves from being victims to these acts. Young children specifically, need to be educated to operate in a safe manner in cyberspace and to protect themselves in the process. As our nation rapidly building its Cyber-Infrastructure, it is equally important that we educate our population and children to work properly with this infrastructure. Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process beginning at an early age. The valuable aspects for cyber-security are technology, operations and awareness, training and education. This paper focuses issues related to cyber-security in India and presents various methods in bringing awareness in educational system. The objective of this systematic review paper is to explore why it is so critical that modern learners are educated about the risks associated with being active in cyberspace and the strategies that stakeholders can use to promote cyber security education in schools. In this paper, we have discussed importance of cyber security in education sector.**

Index Terms **- Cybersecurity, cyber safety, cyber education, cyber awareness, Cyber-infrastructure, social-networking, cyber-ethics.**

I.INTRODUCTION

The ability to securely connect to virtual systems is an important element within a safe and supportive learning environment. This is particularly the case within institutions of higher education (IHEs), where students are increasingly learning in digital formats; faculty, staff, and visitors are constantly accessing and sharing information online; and more infrastructure and facility functions are being managed online. To maintain their collaborative culture, colleges and universities house robust information technology (IT) networks and multi layered infrastructure systems with varied levels of access and connectivity. Unfortunately, this open environment has made IHEs around the world targets in 2017 cyber-attacks. Social media is being used as medium of expressing the feelings and provoke discussions and to get some attention or to come into the limelight. People are not paying attention to the things such as whether data is authentic and secure or not. Because of this, data becomes more vulnerable. Moreover, use of internet is not limited to adults only Nowadays everyone is using internet. Also, corona. Pandemic has changed the whole picture. Classrooms are now online, and students are learning online platform. In this era of technology and multimedia, knowledge of cybersecurity is also important for children. Although Internet has vast potential and benefits for everybody, the excessive use of the Internet maybe harmful as it may lead to cyber risks for example sextortion, cyber addiction, gaming and gambling addiction, cybersex pornography, and personal information exposure. Cybercrime against children and adolescents is certainly a concern for parents, as they sometimes do not realise their child is a victim of cybercrime. Many parents are unaware of the activities their children perform in cyberspace. Some children are bullied through comments and insults; they may also be intimidated, harassed, abused or sexually exploited. Grooming children and adolescents to become victims of sexual abuse is worsening, as more and more of these sexual predators are using fake identities on the internet when seeking victims.

The objective of cybersecurity education is to educate the users of technology on the potential risks they face when using internet communication tools, such as

social media, chat, online gaming, email and instant messaging. Although there are many past research has been conducted on cyber security, in different areas, f, less articles focused on the steps that need to be done particularly by schools in order to help cultivate cyber security awareness in detail. The objective of this paper is to discuss why it is so critical that modern learners are educated about the risks associated with being active in cyberspace, what factors hamper this education, and the importance of a cybersecurity curriculum that can be used by teachers in junior or primary schools, in the specific context of the Indian education system.

II. CYBERSECURITY

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

In 2020, average cost of a data breach was USD 3.86 million in the United States. These costs include the expenses of discovering and responding to the breach, the cost of downtime and lost revenue, and the long-term reputational damage to a business and its brand. Cybercriminals target customers' personally identifiable information (PII) - names, addresses, national identification numbers (e.g., Social Security numbers in the U.S., fiscal codes in Italy), credit card information - and then sell these records in underground digital marketplaces. Compromised PII often leads to a loss of customer trust, regulatory fines, and even legal action. Security system complexity, created by disparate technologies and a lack of in-house expertise, can amplify these costs. But organizations with a comprehensive cybersecurity strategy, governed by best practices and automated using advanced analytics, artificial intelligence (AI) and machine learning, can fight cyberthreats more effectively and reduce the lifecycle and impact of breaches when they occur.

The emergence of the internet allows humans to enjoy two realms: their real life, and the virtual world. With search engines such as Google and Yahoo, and video sharing sites such as YouTube, all information is now available at people's fingertips. However, the growing world of cyberspace may also have negative effects on internet users, such as through cybercrime. Such issues should therefore be contained early so they do not have a major impact. In this context, cybersecurity implementation among internet users is very important. Cybersecurity education is necessary because cybercrime cases can occur anywhere regardless of individuals, organisations and places. The definition of cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. The explosion of Information Communication Technology (ICT) has brought great changes to our lives. With the existence of the World Wide Web, individuals and organisations can easily display any information, but if this is used for damaging purposes it will have a negative effect on people's lives. In addition, the internet makes pornography accessible, which can generate social problems, including crime. The internet can also be an unhealthy channel for crimes and misbehavior, being the main cause of Malay teenagers truanting from school. Cybersecurity can also be defined as the activity, process, ability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation. The internet undoubtedly increases one's knowledge. For example, online computer games require users who are highly skilled in English, in order to understand game settings and procedures. This will indirectly encourage the development of reading, writing and speaking skills in English. However, a computer game will usually be fun, and take the user a long time to complete. This can cause teens to become lazy, or to concentrate on gameplay and gadgets. Adolescents can also become addicted, and productive activities, such as reviewing their lessons, are ignored.

III. NEED FOR CYBER SECURITY EDUCATION

The COVID-19 pandemic has had a profound impact on education, bringing about a sudden boom in remote and online learning. While the transition has forced many schools to implement innovative solutions, it has also revealed stark vulnerabilities in their cybersecurity strategies, which is especially concerning given that schools have become new target for attackers. A big problem is that even before the

pandemic, cybersecurity hasn't been a priority in education. A lack of funding and skilled personnel has meant that schools have basic system set-up errors or leave old issues unpatched. Now, in the mass digital movement, these gaps can be even more damaging, and schools are quickly realizing that they need the knowledge and updated technological infrastructure to continue virtual learning securely in the long-term. Children's use of the internet is changing fast, in response to considerable societal, market and technological innovation. As children's frequent engagement with online videos, music, gaming, messaging and searching implies, their internet use is broadly positive. Parents of three- to four-year-olds report that their child is likely to watch cartoons, mini-movies, animations or songs on YouTube. The content children watch as they grow older differs, as older children watch more music videos, vloggers, YouTube personalities, and funny videos. The role of schools is important in teaching critical digital literacy to students, as well as in guiding and informing parents regarding children's internet use at home.

IV.TYPES OF CYBER ATTACKS

In education system, the children must be made aware of the possible attacks and types of intruders. They should have knowledge about the frauds and scams like phishing, cyber theft and their historic records. They must know about the types of malicious software, their preventive measures etc. Curriculum must also include the advance concepts like the safe use of social networking n mobile devices using GPRS. They must also be aware of the terms like: 1) Hardware/Desktop Security 2) Wi-Fi security, wired security 3) Password Protection/(File/Folder)level security 4) Malicious software: • Phishing, Hoaxes • Scare ware, Malware, Virus, Worm, • Trojans, Zombie and Botnet, Spyware, Adware, 5) Social networking attacks security Students are acquiring information technology skills marks question on the educators' abilities to ensure that positive habits of on-line behavior are being formed. Whereas the teacher giving information about security lacks the knowledge and up-to date information related to Cyber awareness issues, particularly with respect to security. Teacher technology training must be provided for skills development and awareness. A new kind of emerging cybercrime are the Hacktivists. The current record shows least awareness of cyber-crimes at all levels in India. There is an urgent need for introducing courses in various fields. Department of National Security defines cyber security as, "preventing, detecting, and responding to attacks." Indian Education system needs cyber security awareness programs with the increasing use of Indian users in social networking and mobile devices.

V. CHALLENGES AND ISSUES FOR CYBER SECURITY EDUCATION

Among the biggest cyber challenges facing the education sector is an increased number of cyberattacks that aim to steal personal information, extort data for money, or disrupt schools' ability to operate. Recently, schools have been regularly targeted with the following three types of cyberattacks to achieve these goals. Cyber security education is an important and pertinent topic as it plays a major role in mitigating the risks caused by a global shortage of cyber security experts. In order to better support this crucial function, a cyber security skills framework needs to be agreed upon by academics in this field, along with an increase in the visibility of cyber security education and training. Without these, there is likely to be a long-term shortfall between the number of skilled cyber security professionals and demand, potentially leaving organizations, institutions, and governments vulnerable.

Education System

1. No separate lesson plans for the cyber security awareness.
2. Teachers are not aware of the current threats in the information technology. Teachers may face problems in developing their knowledge of the latest technology and thus ensuring students are safe.
3. People are not aware of the reason for the educational course and so do not make any effort to understand or learn the course.
4. It is related to the subject matter and non-interactive learning system.
5. People have the tendency to forget what they learnt about information security if there is not practical implementation.
6. The training and education programs don't consider the present knowledge and experience of

their target audience and the problem of "One-size-fits-all" appear.

7. The course material is usually not presented in a memorable manner and therefore makes no impression.
8. The complete and comprehensive education of the users in cyber security involves a continuum of three levels of education.

VI. METHODOLOGY

The research highlights research studies conducted in the field of cybersecurity in education. Multiple databases (Emerald, Google Scholar, Sci, Scopus and EBSCOhost) were explored, using keywords such as Cybersecurity, cyber safety, cyber education, cyber awareness, Cyber-infrastructure, social-networking, cyber-ethics. The literature chosen was in the two languages that can be understood by the researcher, which is English. In addition, the search was limited to studies published between 2011 until 2020. More than 240 studies were found, but only 25 studies were selected.

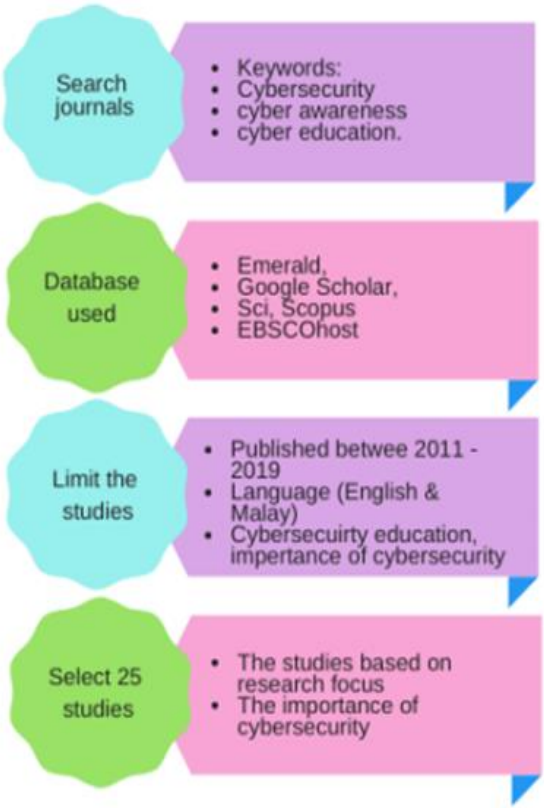

Fig. 1. The selection process of past studies.

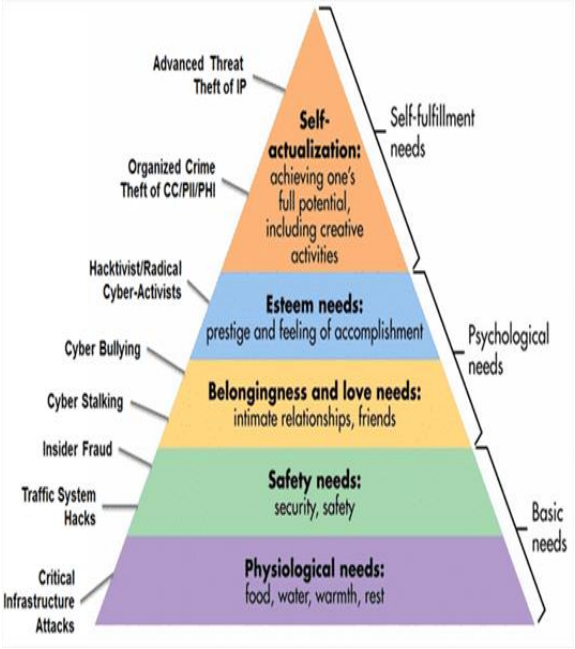

Fig2. cyber world and human emotions

Malicious actors use emotions in human hacking with a high success rate. Indeed, even the most experienced IT professional can be a victim of this type of attack. Hackers use emotions as a social engineering tool, to persuade their victims to take an action they normally would not. The best way to protect yourself from these attacks is by becoming familiar with the techniques used. Bad actors manipulate the following four emotions the most in social engineering attacks. Cybercrooks play with human emotions such as fear, sympathy, curiosity, and greed to trick people into clicking on malware-ridden bogus links, malicious pop-up advertisements or using physical media such as flash drives to gain access to confidential information.

VII. MEASURES TO BE TAKEN TO ENSURE CYBER SECURITY

1. Use an Internet Security Suite
2. Install a firewall
3. Use Strong Passwords
4. Keep Your Software Up-to-Date
5. Take appropriate actions if you have been a Victim
6. Learning safe chatting and messaging skills
7. Installing and updating anti-virus software and regularly downloading security protection updates

8. Preventing stranger access to private computer files
9. Individual awareness about all the laws and rights before using any new software
10. Government must participate in funding cyber education and create strong partnerships with local state and regional governments industry and educational institution
11. Government should provide proper laws for cyber-crime and prosecute people who steal digital property or harm others on-line

VIII. CONCLUSION

Based on a synthesis of the literature selected, The IT industry has been playing catch-up with hackers and cybercriminals for decades. Thus there is a need of cyber –security curriculum in the near future which will in-build the cyber-security understanding in the current youth and finally the IT sector will get more profound, securely skilled professionals it was found that it is very important to protect children through cybersecurity education so that they can become aware of the potential risks they face when using internet communication tools, such as the social media, chatting and online gaming. However, there are several challenges to cybersecurity education. These include the level of teachers' knowledge, and the lack of expertise, funding and resources. It is very important for all relevant parties, including teachers, parents, peers and the government, to work together to find the best solution to protecting children from cybercrime and cyberbullying through school-based cybersecurity education. The media, such as television and radio, must also play an important role in educating children through cybersecurity campaigns because such campaigns are more interactive and interesting for children to understand. Hence Effective cyber-security policies, best practices must be planned and most-important must be implemented at all levels. In the future the Government role and education systems participation in the cyber security awareness approach will lead to a strongly secured nation.

REFERENCES

[1] F. Khalid, ―Understanding university students' use of Facebook for collaborative learning,‖ International Journal of Information and Education Technology, vol. 7, no. 8, pp. 595-600, August 2017.

[2] F. Annasingh and T. Veli, ―An investigation into risks awareness and e-safety needs of children on the internet, ‖ Interactive Technology and Smart Education, vol. 13, no. 2, pp. 147-165, 2016.

[3] L. Muniandy and B. Muniandy, ―The impact of social media in social and political aspects in Malaysia: An overview, ‖ International Journal of Humanities and Social Science, vol. 3, no. 11, pp. 71-76, 2013.

[4] V. Ratten, ―A cross-cultural comparison of online behavioral advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory, ‖ Journal of Science & Technology Policy Management, vol. 6, no. 1, pp. 2536,2015.

[5] M. D. Griffiths and D. Kuss, ―Online addictions, gambling, video gaming and social networking, ‖ The Handbook of the Psychology of Communication Technology, Chichester: John Wiley, pp. 384-406, 2015.

[6] L. Mosalanejas, A. Dehghani, and K. Abdolahofard, ―The students' experiences of ethics in online systems: A phenomenological study,‖ Turkish Online Journal of Distance Education, vol. 15, no. 4, pp. 205-216, 2014.

[7] D. Krotidou, N. Teokleous, and A. Zahariadou, ―Exploring parents' and children's awareness on internet threats in relation to internet safety, ‖ Campus-Wide Information Systems, vol. 29, no. 3, pp. 133-143, 2012.

[8] N. Ahmad, U. A. Mokhtar, Z. Hood et al., ―Cyber security situational awareness among parents, ‖ presented at the Cyber Resilience Conference, Putrajaya Malaysia, pp. 7-8, November 13-15, 2019.

[9] Monika D. Rokade, Yogesh Kumar Sharma ―Identification of Malicious Activity for network packet using deep learning. International Journal of advanced Science and technology.