

NEED OF CYBER SECURITY EDUCATION IN MODERN TIMES

Suman Saggu

Assistant Professor
Khalsa College of Education, Amritsar

ABSTRACT

In the digital era, cyber security education is essential due to the widespread use of the internet in daily life. The rise in cyber crimes such as hacking, phishing, and identity theft makes awareness necessary to protect personal and sensitive data. Cyber security education helps individuals use digital platforms safely and responsibly, including social media and online banking. It also plays a vital role in protecting national security and critical infrastructure. Moreover, it prepares students for emerging career opportunities and supports the growth of a secure digital economy. Cyber security education is crucial for ensuring digital safety and sustainable technological development. The aim of this paper is to sightsee why cyber safety education is so critical for modern learners and how they can understand the risks associated with being active in cyberspace. In this paper, few strategies are also discussed as how cyber security education can be implemented in schools.

Keywords : Cyber Security, Cyber Crimes, Hacking, Digital Platforms

Cyber security education is no longer optional in modern times. It is a critical life skill. The revolutionary change with the emergence of vast Internet has brought positive impact on people's lives. We use social media on internet as a platform for self-expression, to incite discussions, or to become known. Side by we cannot ignore the negative impacts too that have emerged related to its use. Due to the lack of awareness among web surfers, cases like cyber-bullying, online frauds, racial abuses, pornography and gambling have increased tremendously. Sometimes people want to be the primary source of information, of sharing a topic, that they overlook the fact stating authentication to the shared information. Today usage of the internet is not just limited to adults, but in this era of technology and multimedia, knowledge of cyber security is also important for children. Still, the level of awareness among Internet users is quite low or moderate. Therefore, if proper measures are taken to cultivate knowledge and awareness among Internet users from their early age, i.e., young children, this issue of cyber safety can be understood in a better way. Since now with covid 19 online education has become the new trend, young children specially need to be educated to operate in a safe manner in cyberspace and to protect themselves in the process.

Technology is deeply intertwined with each aspect of our lives globally. This increases our concern towards cyber security. The present era marked by digital transformation; rural areas are also not safe to the growing threats of cyber-attacks. Like other countries, India faced over 13.9 lakh cyber security incidents in 2022. It includes Phishing, ransom ware attacks, website damage and unauthorized network scanning or probing activities, data violation and many dangerous services happened to all types of users. While out of 759 million active internet users, 399 million users are from rural India, the cyber security awareness among rural citizen plays a major role. Numerous studies emphasize the importance of cyber security awareness in reducing cyber threats. Increased awareness of cyber security can lead to betterinformed decisions and more secure online behavior. According to a report on Cyber Security by Niti Aayog and Saraswat (n.d.), India ranked among the top five countries to be affected by cybercrime. As Whitman and Mattord (2020) clearly defined cyber security is a field encompassing practices, technologies and strategies aimed at safeguarding computers,

networks and data from unauthorized access, attacks and harm. In the advancing world we live in it is crucial to recognize the significance of being aware of cyber security. With our growing dependence, on technology and the internet, for both professional aspects it becomes more essential to grasp and actively participate in cyber security practices. As stated by Disterer (2021), "cyber security awareness is the foundation upon which a strong security posture is built". Cyber security awareness is a broad notion that includes the skills necessary to identify, comprehend, and counteract cyber security threats. The studies highlight the significance of an all-encompassing approach to awareness that includes not only the technical understanding but also a deeper comprehension of the psychological and social dimensions of cyber security (Solms & Niekerk, 2022). This comprehensive viewpoint acknowledges the necessity for people and organizations to have a proactive and watchful mindset in addition to cyber security knowledge (Dumitraş, 2019).

CYBER SECURITY EDUCATION : Cyber security education is the process of acquiring knowledge and skills to protect networks, devices, and data from digital attacks, unauthorized access, and theft. It focuses on teaching threat identification, defensive strategies, and risk mitigation, empowering users to prevent breaches often caused by human error.

FEATURE OF CYBER SECURITY EDUCATION

- Core Principles of CSE are the CIA Triad (confidentiality, integrity, availability), network security, application security, and information security.
- Learners develop practical skills in identifying phishing, creating strong passwords, and understanding data protection, crucial for defending against ransomware and social engineering.
- Education is tailored for various levels, from basic awareness for general users to advanced technical training for IT professionals aiming for roles in fields like ethical hacking or cloud security.
- It utilizes hands-on training, such as simulations in cyber ranges, gamification (e.g., red team vs. blue team exercises), and role-based learning to enhance retention.
- The ultimate goal is to foster a "culture of security" within organizations, ensuring that technology, processes, and people work together to maintain digital resilience.

IMPORTANCE OF CYBER SECURITY EDUCATION:

As cyber threats become more sophisticated, this education is critical to filling the knowledge gap, as many breaches stem from human error rather than technical failures. It ensures that individuals can proactively manage risks and respond to security incidents.

1. **Rapid Digital Transformation :** Almost every aspect of life like banking, education, healthcare, governance, and communication has shifted online. With increased internet usage, the risk of cyber threats has also grown, making cyber security education essential for safe digital participation.
2. **Rising Cyber Crimes :** Cyber crimes such as hacking, phishing, identity theft ransomware attacks, and online fraud are increasing rapidly. Educating individuals helps them recognize threats and protect personal and organizational data
3. **Protection of Personal and Sensitive Data :** People regularly share sensitive information online (Aadhaar details, bank credentials, medical records). Cyber security education teaches safe data handling, strong password practices, and privacy protection.

4. **National Security and Critical Infrastructure:** Cyber attacks can target power grids, defense systems, financial institutions, and government databases. Trained cyber security professionals are vital for protecting national assets and ensuring digital sovereignty.
5. **Safe Use of Social Media and Digital Platforms:** Students and citizens are vulnerable to cyberbullying, misinformation, fake news, and online exploitation. Cyber awareness promotes responsible digital behavior and ethical internet use.
6. **Workforce Readiness and Career Opportunities:** Cyber security is one of the fastest-growing career fields globally. Education in this domain equips students with in-demand skills and improves employability in IT, defence, finance, and corporate sectors.
7. **Supporting Digital Economy and E-Governance:** India's push toward Digital India, online payments, and e-governance requires a cyber-aware population to ensure trust, safety, and smooth functioning of digital services.
8. **Preventing Financial Losses :** Organizations and individuals suffer huge financial losses due to cyber attacks. Cyber security education helps in early threat detection, risk management, and incident response.
9. **Promoting Ethical and Responsible Technology Use :** Education instils values such as digital ethics, legal awareness (IT Act, cyber laws), and responsible use of technology.
10. **Lifelong Digital Safety :** Cyber threats evolve continuously. Cyber security education builds adaptability, critical thinking, and lifelong awareness to stay safe in an ever-changing digital world.

TECHNIQUES OF CYBER SECURITY EDUCATION

In the schools, colleges, and other professional fields, following are some effective techniques which are used for providing cyber security Education.

1. **Experiential / Hands-On Learning:** Cyber security is best learned by doing. While using virtual Labs & simulation tools students make to learn practice ethical hacking, network defence, malware analysis in safe environments. Further Lab-based practical sessions e.g. Firewall configuration, penetration testing, encryption setup helps to students to tackle cyber crimes. By capturing the Flag (CTF) competitions, students develop problem-solving skill through real-world security challenges .
2. **Problem-Based Learning (PBL)** Students learn by solving real security problems. Case studies of real cyber attacks (e.g., ransomware, phishing scams), Incident response simulations. Risk assessment and security audit projects and threat modeling exercises enhance analytical thinking and decision-making skills.
3. **Gamification Techniques :** Gamified learning improves engagement. Like Cybersecurity escape rooms, Points, badges, and leaderboards, Scenario-based challenges, Interactive security quizzes.
4. **Project-Based Learning :** Students work on practical cyber security projects such as: Designing secure networks, Developing secure web applications, Creating awareness campaigns, Building encryption tools.

5. **Industry Collaboration & Certifications** : Guest lectures from cyber security professionals, Internship opportunities, Workshops and boot camps and Certification-oriented training like CEH, CompTIA Security+, CISSP and more advanced level.
6. **Blended & Online Learning Approaches** : MOOCs and online cybersecurity courses, Recorded demonstrations, Interactive webinars or Flipped classroom models.
7. **Role-Playing & Scenario-Based Training** : Red Team vs Blue Team exercises., Ethical hacker vs system administrator simulations, Crisis management drills are some of games.
8. **Interdisciplinary Approach** : Cyber security education should integrate: Law (cyber laws, IT Act), Ethics (data privacy, digital responsibility), Psychology (social engineering) and Management (risk governance).
9. **Continuous Assessment & Feedback** : Continuous Assessment & Feedback can be done through Real-time skill evaluation, Practical-based exams, Peer review of security projects and Reflective learning journals.
10. **Awareness & Community Engagement**: Awareness regarding cyber security can be spread in community by Cyber hygiene workshops, School/college awareness drives, Phishing simulation campaigns, Digital citizenship programs.

CONCLUSION

Cyber security education has emerged as an essential life skill in the contemporary digital era. As technology becomes deeply integrated into everyday activities such as banking, education, healthcare, governance, and communication, the risks associated with cyber threats have increased significantly. The widespread use of the internet and social media platforms has created opportunities for innovation, connectivity, and economic growth. However, it has also exposed individuals and institutions to cyberbullying, phishing, ransomware attacks, identity theft, misinformation, data breaches, and financial fraud. These threats are no longer limited to urban or technologically advanced regions; they affect rural populations as well. In countries like India, where digital expansion has accelerated rapidly under initiatives such as Digital India, the need for widespread cyber awareness has become even more urgent. A major concern in cyber security is that many breaches occur due to human error rather than technical system failures. Lack of awareness, weak password practices, careless sharing of personal information, and inability to identify fraudulent activities make users vulnerable. Therefore, cyber security education must focus not only on technical knowledge but also on behavioral change, ethical responsibility, and critical thinking. It should cultivate an understanding of fundamental principles such as confidentiality, integrity, and availability, while also equipping individuals with practical skills to recognize and respond to cyber threats effectively.

REFERENCES

1. Disterer, G. (2018). Cyber security – Its Importance in the World of Technology. In Cyber security – Its Importance in the World of Technology ,45-53. Springer.
2. Dumitraş, (2019). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 27(4), 4729– 4752. <https://doi.org/10.1007/s10639-021-10806-7>
3. Solms, R. & Niekerk, J. (2022). From information security to cyber security, Computers & Security. (2).97-102.
4. Whitman, M. E., & Mattord, H. J. (2020). Principles of Information Security. Cengage Learning.