AD EDUXIAN JOURNAL

*A Quarterly Multidisciplinary Blind Peer Reviewed & Refereed Online International Journal*

Google Scholar Indexing PIF:1.048(I2OR) & 3.125 (IIFS)

*Vol (2), Issue (3), Oct-Dec 2025* *ISSN: 3048-7951*

# Cyber Safety and Security in Digital World

**Dr. Neeta Sahu**[1]

https://doi.org/10.5281/zenodo.17919036

**Review: 08/11/2025** **Acceptance: 10/12/2025** **Publication:13/12/2025**

**Abstract:** *In the present era we all are living in digital environment, where cyber safety and cyber security is much needed, as the threats of cyber-crimes, cyber-attacks has noticeably increased. Apparently technology is the backbone of present scenario and we can't stay away of the technological gadgets and setup like E- commerce, mobile computing, cloud computing, big data science, artificial intelligence, digital transactions and so on, hence, in these references the knowledge of cyber safety and cyber security is to be considered as a prerequisite for survival in digital world. Cyber security refers to the practice of protecting computer systems, networks, devices and data from theft, damage, disruption or misuse and unauthorized access. Cyber security aims to prevent or mitigate these threats by employing the combination of technical, procedural and administrative help. According to a report, India emerges as a prime target for threat actors. The education sector is a prime target for cyber-attacks due to a combination of exclusive data, lack of cyber risk awareness, lack of technical expertise, financial limitations and widespread vulnerabilities. Hence there is a need of raising awareness of cyber safety and security among common people and netizens.*

***Keywords:*** *Cyber safety, Cybersecurity, Digital footprints, Cyber-attacks.*

**Cyber Safety and Security in Digital World:** Cyber security refers to the practice of protecting computer systems, networks, devices and data from theft, damage, disruption or misuse and unauthorized access. Cyber security aims to prevent or mitigate these threats by employing the combination of technical, procedural and administrative help. It is also known as information technology security. Being a part of highly connected digital era we can't avoid our involvement in online activities. We are sharing and retrieving so much from this ocean of internet which has provoked us to be more conscious regarding cyber safety and security in digital world. It gives birth to the need of safe and secure transaction of information and data over internet. The term cyber security applies in a variety of contexts such as network, information, application etc. In other words cyber safety and security is the safe, intelligent and responsible use of information and communication technologies such as internet, social media, mobile phones, tablets, online games, and online transaction and along with the practice of protecting our computers, networks, programs and data from digital attacks.

**Cyber safety and security: A prominent issue:** National Education Policy 2020 talks about careful attention to the safety and security of the children and especially girl children. Student's safety has been considered on priority and to keep them safe from any form of discrimination and harassment there is need of such a mechanism which is effective and well known to all the students. Cyber bullying, online harassment, student's privacy concerns, digital footprint management, phishing and other issues are among the major issues and challenges regarding safety and security in the digital world. In the last few years the use of technology has been increased at a surprisingly rate. Pandemic Covid-19 has added more to this by switching the system from offline to online mode.

[1] Dr. Neeta Sahu, Assistant Professor, S.S. Khanna Girls' Degree College, A Constituent College of University of Allahabad, Prayagraj, Uttar Pradesh(India) 211003.

Children from preschool stage to higher education are using technology frequently, like wise older people even retired professionals are active in cyber world to accomplish their day to day task, to keep them connected with others and for entertainment as well. They must take care of safety guidelines to be followed in digital world, because they may be well educated but not aware of proper handling of technology. Thus there is need of cyber education, trainings, and workshops to make the personnel well equipped for digital world.

According to the report on 'Cyber Threats Targeting the Global Education Sector on the Rise' which has collected the data from multiple sources across the internet in 2021, reveals that the global education and training market is expected to reach USD 7.3 trillion by 2025 which predicts the increased use of education technology in the future. Hence, educational institutions, educational sites will be an attractive field for cybercriminals. This report says that 5% of total threats identified in 2021, targeted educational institutions. It further reports that the majority of cyber incidents targeted education institutions in Asia & Pacific, followed by Europe, North America, South/ Latin America, and the Middle East. However, India emerges as a prime target for threat actors, out of the total threats detected in Asia & Pacific, 58% of them were targeted at Indian or India-based educational institutions and online platforms. Among the top five targeted countries India is at number one with 28% of the threats.

**Major challenges and issues of cyber safety and cyber security:**

- **Cyberbullying:** This is one of the major concern of cyber security. Cyberbullying is the repeated hostile aggressive behavior performed by an individual or a group on others aimed to impose harm or discomfort.
- **Cyber stalking/ harassment:** cyber stalking is the use of internet or other electronic communications to harass or frighten someone. It may be in the form of sending threatening emails, making rude, offensive online comments, spreading unwanted messages, defamation etc.
- **Students' privacy concerns:** Educational institutions maintain the personal information of their students in their data base. If proper care is not taken then there is risk of misuse of data and stealing of data. Hackers are mostly interested in the personal details of the students such as their location, interests, loan status, family background, their weaknesses etc.
- **Digital footprint management:** It is also known as digital shadow or electronic footprint, it is traceable data which we leave actively or passively during our online activities. Active digital footprints include social media posts, online comments, sharing of photos and videos on social media, sharing your location, login on several devices, filling online forms, accepting cookies etc. While passive digital footprint include sharing of passwords, account details, tax records, medical records, browsing history, heavily visited websites etc.
- **Phishing or online scams:** Phishing may be called as online scam that targets consumers by sending them an e-mail that appears to be from a well-known source. It may be asking for your personal bank details, or sharing of fraud link, asking to download any application etc. It is actually an attempt to obtain sensitive information of the user by posing as a trustworthy source in email.

- **Cyber grooming:** Cyber grooming is the process of befriending a child online and establishing an emotional connection with future intentions of sexual abuse, sexual exploitation or trafficking. Such people try to gain trust of the children to obtain their intimate and personal data in order to threaten and blackmail for further inappropriate material.

- **Identity theft:** Identity theft is becoming one of the big problems for digital security. When someone uses another's personal identifying information, like their name, their voice, identifying number without their permission, to commit fraud or other crime is known as identity theft. Financial identity theft (to gain financial benefits), tax-related identity theft (files false tax return), medical identity theft these can be forms of identity theft.

- **Copyright infringement:** It is referred as the illegal use or reproduction of someone else work, without his permission. It violates the rules and regulation of copyright. It may include copying, distributing, reusing, performing anyone else’s work/art without prior permission.

- **Hacking (account/ email):** Email hacking refers to unauthorized access to an email account or email correspondence. This access is often obtained by cybercriminals for malicious purposes, such as stealing personal information, executing phishing scams, or spreading malware.

- **Fake websites and apps:** Cybercriminals create fake websites and fake apps which appears same as the legitimate ones through this they capture the login credentials of the users then utilize this information to make monetary transactions and other frauds.

- **Digital arrest:** It is one of the latest cybercrimes where the awareness of cybersecurity is much needed. It is a scam where cybercriminals impersonate law enforcement or legal authorities to extract money from victims by imposing false charges, cases, warrant etc. they demand money to clear victim’s name from the case or to sort out the false case.

**Reasons behind increased cyber threats/Cyber Crimes:** As discussed earlier that education sector and educational institutions are the soft target of the cybercriminals. Let’s have a look on the expected reasons behind the increasing number of threats in educational sector as following-

- Students are young, unaware of the safety and cyber security features and are pretty vulnerable at this age.
- Switching from offline mode to online mode is also a vital reason. It has motivated us to be engaged in digital world but lack of proper handling of technology has led the dangers of cyber threats.
- Hackers are interested in significant database of the students and their families.
- Sometimes due to some constraints educational institutions don’t have technical experts to handle with data, thus also leads opportunity for the attackers.
- Digitalization is the demand of the day this digitalization of data in every field has also increased the probability of cyber-attacks.

- Online games are also one of the reason which give easy access to the attackers. Online games have become popular among each group of people hence there are high risks for cyber safety and cyber security
- Frequently we leave our digital footprints unconsciously on cyber space which poses a danger for cyber security.
- Ignorance of netiquettes also provide an easy platform for threat actors.

**Measures to mitigate these threats:** It has been rightly said that prevention is better than cure hence to enhance cyber safety and security following measures can be opted. The government of India has also launched awareness campaigns across various media to educate the public on common cyber threats like digital arrest scams, investment scams, and phishing etc. Following are the measures to be kept into consideration--

1. **Awareness of cyber safety and security:** For spreading awareness among school children workshops, discussions, display of documentaries, special training and lecture of the experts can be organized. Besides this cyber awareness and hygiene tips have been mentioned for the students, teens, young adults and parents on the website https://cybercrime.gov.in these tips can be shared with the students for making them cyber safe.

2. **Change in passwords at regular intervals:** It is always advised that we should keep changing the passwords at regular intervals and create a strong and unique passwords which could not be easily guessed.

3. **Don't open email attachment from unknown sender:** To avoid phishing and online scam it is advised that one should open only authentic and secure websites by checking the URL and should not forward spam and suspicious email to others. One should avoid opening any link shared by unknown source and sharing any personal details on online platform.

4. **Don't use unsecure WiFi networks at public place:** Public WiFi and network connection may lead to cyber threats rather it should be avoided to use any public network without ensuring its authenticity. Antivirus and anti-malware software should be installed and be regularly updated to keep the gadgets safe.

5. **Keep software updated:** System updation for cybersecurity refers to the regular updating of software and operating system to avoid cyber threats. To fix security vulnerabilities and protection against treats we should enable automatic updates in all the gadgets and updates should be from trusted sources like official app stores and manufacturers only.

6. **Data backup:** Data backup is needed for computer security as it works like a safety feature which helps in quick recovery from a wide range of threats including ransomware, viruses, human error and hardware failure.

7. **National cybercrime reporting portal (https://cybercrime.gov.in/):** On this portal anyone can register a complaint against women/ children related crime, any financial fraud or any other cybercrime. Through the 'Report Suspect' facility at NCRP, citizens can report various types of suspect identifiers as websites, URLs, WhatsApp numbers, Email-ids, social media etc.

8. **Cyber safe portal (www.cybersafe.gov.in):** Cyber safe is an application which has been developed with an objective of making the digital payment ecosystem safe and secure.

9. **Sanchar Saathi portal** (**www.sanchasaathi.gov.in**): Sanchar Saathi is a citizen centric initiative of Department of Telecommunication (DoT) to strengthen mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. It is available in the form Mobile App.

**Conclusion:** Being a part of digital era we can not keep ourselves isolated from digital world. Directly or indirectly we all are involved in digital activities, digital transactions etc. and leaving our digital footprints behind in the digital world which leads to many kinds of digital crime. Keeping in view the current and future scenario awareness of digital safety and security must be our priority. Government has taken several initiatives and has shared awareness tips on cybercrime.gov.in for students, teens and parents. It's our responsibility to come forward and follow all the digital safety tips and also spread awareness among young and old generations as well to make cyber world safe to all.

**References:**

- Clare Stouffer, (2023). What is a digital footprint how can you protect it. Retrieved from: https://us.norton.com/blog/privacy/digital-footprint
- Cyber grooming. Retrieved from: https://www.csa.gov.gh/cyber_grooming.php#:~:text=Cyber%20grooming%20is%20when%20someone,abuse%2C%20sexual%20exploitation%20or%20trafficking.
- Cyber safety and security guidelines for schools. Retrieved from: https://ciet.ncert.gov.in/storage/app/public/files/14/cyber-safety/Cyber_safety_for_schools_Eng.pdf
- Cyber safety guides for schools. Retrieved from: https://www.brainstormproductions.edu.au/student-cyber-safety-guide-for-schools/#:~:text=Cyber%20safety%20is%20the%20safe,stay%20safe%20in%20online%20environments.
- **https://cybercrime.gov.in/**
- **https://www.ncrb.gov.in/crime-in-india.html**
- https://www.staysafeonline.in/concept/digital-footprints/managing-for-data-protection-and-online-security
- Safety and security in the cyber world. Retrieved from https://ncert.nic.in/textbook/pdf/iict107.pdf
- Saxena, H.(2022) Cyber Threats Targeting the Global Education Sector on the Rise https://assets-global.website-files.com/635e632477408d12d1811a64/63d6d0decdfd66befc1bc36e_Cyber-Threats-Targeting-the-Global-Education-Sector.pdf
- What is cyber safety? https://www.brainstormproductions.edu.au/student-cyber-safety-guide-for-schools/#:~:text=Cyber%20safety%20is%20the%20safe,stay%20safe%20in%20online%20environments
- What is cyber security? Types, threats and cyber safety tips. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security