Cyber-Safety: Concepts, Threats, and Essential Measures

Rejaul Karim Barbhuiya

Assistant Professor, Central Institute of Educational Technology (CIET),

National Council of Educational Research and Training (NCERT), Sri Aurobindo Marg, New Delhi

Email- rejaul.karim@ciet.nic.in

Abstract

The rapid advancement of technology has led to a digital revolution, impacting various aspects of our lives and elevating the importance of cybersecurity. As society increasingly relies on technology for communication and learning, cybersecurity awareness has become crucial. The COVID-19 pandemic accelerated the adoption of digital tools in education, necessitating a comprehensive approach to address cybersecurity challenges for students and teachers. This research article explores the background and significance of cybersecurity, focusing on evolving cyber threats faced by educational institutions and society. It addresses cyberbullying, misinformation, and fake news, advocating for responsible netizenship and media literacy among students. The study comprehensively examines cyber threats, ranging from malware-based attacks to social engineering and denial-of-service incidents. Emphasising cybersecurity as an integral pillar of the digital age, the research stresses the need for robust strategies to safeguard data, ensure privacy, and create a safe online environment for students, teachers, and the broader community.

The study aims to gain insights into the profound impact of cyber threats on individuals and institutions, highlighting the significance of cybersecurity in the digital landscape. Essential measures like user education, device configuration, network security, and identity management are proposed to strengthen defences and secure the digital environment. The paper addresses children's cyber safety concerns, focusing on combating cyberbullying, misinformation, and scams. It presents effective awareness-raising strategies and preventive measures, emphasising the role of education campaigns and parental involvement. This research strives to safeguard education in the digital age by promoting responsible online behaviour and fostering a secure digital environment. The research contributes to the current initiatives towards cyber safety and security by demonstrating the importance and critical role of awareness in the cyber safety and security strategy of the country. The major contribution is the advancement of the theoretical and practical basis for cyber security awareness in proposing a model framework for developing awareness.

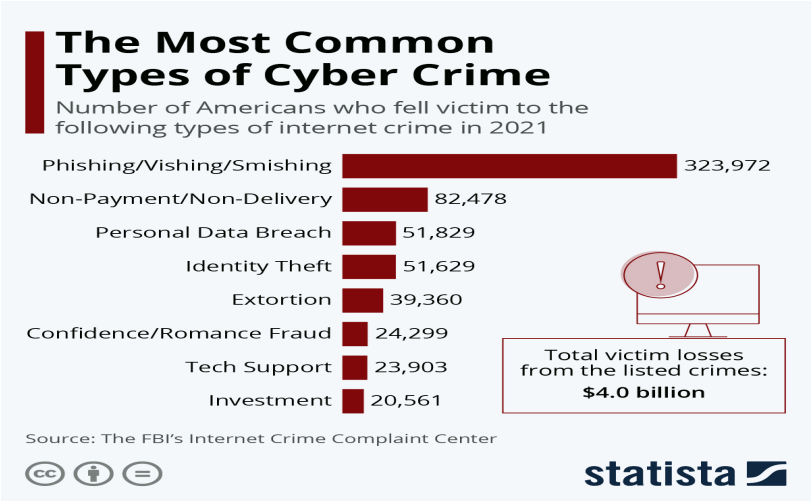
Keywords: Cybersecurity, Cyber safety, Cyber threats, Cyberbullying, Digital Education

Introduction

In recent years, the rapid advancement of technology has ushered in a new era of digital connectivity that permeates every aspect of our lives. As our society increasingly relies on technology for communication, learning, and information dissemination, the significance of cybersecurity has reached unprecedented heights (Clark & Hakim, 2017). The COVID-19

pandemic has further catalysed the adoption of digital technology by teachers, students, and schools, propelling them to embrace these tools at an accelerated pace (Jena, 2020; Kidd & Murray, 2020). The digital landscape offers tremendous opportunities for education, empowering students, schools and educators with innovative learning tools and access to a vast pool of knowledge. However, this digital revolution also comes with inherent risks, as the cyber world presents an ever-expanding frontier for threats and vulnerabilities (Schia, 2018). It exposes educational institutions as well as society as a whole to diverse cyber threats, ranging from malicious attacks, data breaches, misinformation, and cyberbullying. As we embrace the benefits of a digital world, it becomes imperative to have a comprehensive understanding of the intricacies of cybersecurity and to develop robust strategies that safeguard the data and its integrity, preserve privacy, and ensure a safe online environment for students, educators, and the broader community.

Figure-1: Cybercrimes in US for the year 2021 (image source, CC BY-ND)



This research article aims to explore the background and significance of cybersecurity in light of these developments. It seeks to shed light on the multifaceted challenges posed by cyber threats that have evolved into sophisticated and pervasive forms while exploring the strategies to ensure the safety and security of individuals and institutions in the digital domain. The article sheds light on the rising instances of cyberbullying, misinformation, and fake news, emphasising the promotion of responsible netizenship and media literacy among students. The objectives of this study encompass a holistic examination of cyber threats, ranging from malware-based attacks and social engineering schemes to denial-of-service incidents. By gaining a deeper insight into the various facets of cyber threats, this work aims to elucidate their profound impact on individuals, organisations, and society. Moreover, the research aims to highlight the importance of cybersecurity as an integral pillar of the digital age, elucidating the key components of a robust cybersecurity strategy to fortify defences against potential threats. Special attention is devoted to enhancing cybersecurity awareness

and implementing safety measures within educational settings, recognising the pivotal roles of students, teachers, and parents in fostering a secure online environment for future generations.

The rest of the article is organised as follows - Section 2 reviews existing guidelines and mechanisms about cyber safety. Section 3 defines the related key concepts, section 4 explores major categories of cyber threats, and section 5 is about cybersecurity measures and awareness. Section 6 delves into cyber safety concerns and the need for awareness. Section 7 focuses on cyber safety and responsible behaviours. Finally, Section 8 is on discussions and the way forward.

Review of Literature

Given the importance of awareness about cyber safety and security (Rahman et al., 2020, Zwilling et al., 2022), various countries are adopting specific measures for awareness through their education system. Many countries assign cyber-security awareness and education to one or more dedicated government departments or organisations (Kortjan & Von Solms, 2014). The Cybersecurity and Infrastructure Security Agency (CISA) of the USA acknowledged the heightened risks of cybersecurity for the K-12 sector and it has come out with an online toolkit (CISA, 2023) containing guidelines and resources for schools to combat cyber threats and various resources for students and teachers to learn about cyber concepts are available (NICCS, 2022). Recognising limitations at the school level, these guidelines recommend for reporting and collaboration with dedicated expert agencies to combat cyber issues. The United Kingdom (UK) also has national policies for cybersecurity education and skill development, including national curriculum, and cyber security, and online safety content (Knott et al., 2023). In Canada, the organisation Public Safety Canada coordinates across departments and agencies for cyber safety and security. In India, the Indian Computer Emergency Response Team (CERT-In, 2023) is the nodal cyber incident response centre that also works on raising security awareness among citizens., and provides technical assistance and advice to deal with cyber crimes.

The Cyber-security awareness and education framework by Kortjan & Von Solms (2014) for South Africa proposes five layers:

i. Strategic layer for reflecting the overall vision of the government regarding cyber-security awareness and education.

ii. The tactical layer lists the schemes to be employed to realise cybersecurity awareness and education goals.

iii. Preparation layer detailing the schemes identified in the tactical layer.

iv. The delivery layer identifies the target beneficiaries.

v. Monitoring layer for monitoring the progress of the scheme towards fulfilling the goals.

Zwilling et al., (2022) studied the relationships between cyber security awareness, knowledge and behaviour among management students across four countries: Israel, Slovenia, Poland and Turkey. Two broad aspects analysed were the connections between - a) previous cyber knowledge and level of cyber security awareness and b) awareness and safe habits or behaviour.

The arrival of the 5G mobile network is further pushing the emergence of Internet of Things (IoT) where the vulnerabilities are beyond the traditional measures like firewalls, passwords, etc. (Fagen et al., 2021; Hero et al., 2023).

This indicates the need for students as well as teachers to be fairly equipped with cybersecurity knowledge in order to safeguard them in the cyber world.

Key Concepts and Definitions

Cyber Threat

A cyber threat is a potential security risk that might exploit weaknesses or vulnerabilities of a digital system or asset, including its users (Abomhara & Køien, 2015). Cyber threats encompass an array of malicious activities, such as malware, social engineering, data breaches, and more, which could compromise the confidentiality, integrity, or availability of information. Preventative measures can mitigate cyber threats and safeguard information security (Safa et al., 2019). Preventive measures include, among others, putting robust cybersecurity protocols, periodic risk assessments, user education, and advanced security technologies.

Cyber Attack

A cyber attack involves deliberately exploiting weaknesses or vulnerabilities within an information system, intending to infiltrate, disrupt, or cause damage to a digital system, network, or asset (Li & Liu, 2021). These malicious acts are carried out by cybercriminals, commonly referred to as hackers, who can be individuals, organisations, or even state-sponsored entities. Cyber attacks encompass various forms, such as ransomware, phishing, online fraud, and identity theft, among others (Sabillon et al., 2016). To counter the threat posed by cyber-attacks, implementing preventative measures such as regularly updating software, conducting security audits, and user education is crucial.

Cybersecurity

Cybersecurity safeguards ICT (Information and Communication Technology) systems and their contents from various threats, such as attacks, disruptions, and unauthorised access (Fischer, 2014). It encompasses a range of activities and measures aimed at protecting computers, computer networks, related hardware and devices, software, and the information they store and communicate within cyberspace (Clark & Hakim, 2017). Cybersecurity refers to the state of being protected from these threats and encompasses the broader field of efforts dedicated to implementing and enhancing protective activities and measures.

There is no precise definition of cybersecurity due to its multifaceted nature. However, cybersecurity remains a crucial and constantly evolving area of awareness for every individual and organisation in ensuring the security and integrity of digital systems and information in the modern digital landscape (Dash & Ansari, 2022).

Cyber Safety

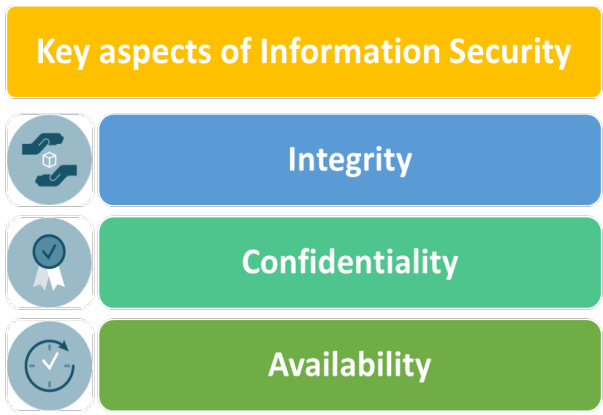
Cyber safety is a subset of cybersecurity that promotes safe and responsible behaviour in the cyber world (Bada et al., 2019; Chang & Coppel, 2020). It involves educating individuals, especially children and young people, about the potential risks of using the internet and how to protect themselves from online dangers, such as cyberbullying, scams, and inappropriate content (Rahman et al., 2020). By teaching safe browsing practices, safeguarding personal information, and recognising online threats, cyber safety helps build a resilient digital community. Cyber safety practices ensure a healthier and more secure online experience for students, parents and teachers.

Information Security

A closely related concept is information security, which safeguards information and information systems from unauthorised access, use, disclosure,

disruption, modification, or destruction (Fischer, 2014). This includes creating a robust and secure environment to safeguard sensitive data and maintain the trust, confidentiality, and reliability of information and the systems that store and manage it (Zissis & Lekkas, 2012). The primary objective of information security is to ensure the protection of information in three key aspects:

Figure-2: Aspects of information security



a. **Integrity:** ensuring that information remains unaltered and protected against improper modification or destruction. This includes measures to ensure that an individual can't falsely deny having performed a particular action and to determine whether a given individual took a specific action, such as creating information, sending a message, approving information, and receiving a message.

b. **Confidentiality:** preserving authorised restrictions on access and disclosure of information. This involves implementing methods to protect personal privacy and proprietary information from being accessed or disclosed by unauthorised entities.

c. **Availability:** ensuring that information is readily and reliably available for access and use by authorised users when needed, avoiding disruptions or downtime that could hinder its access or use.

Cyber Threats: Categories and Impact

There exist diverse types of cyber threats, with cybercriminals and hackers continually striving to devise novel methods to infiltrate digital systems with diverse objectives. Mitigating certain cyber-attacks requires considerable technical intricacy in manipulating program code and software configurations. However, in consideration for the readers' comprehension, this section exclusively addresses commonly encountered cyber threats that exhibit a lesser degree of technical complexity. Starting from this point, the terms cybersecurity, cyber threat, online safety, and cyber attack will be used interchangeably in this article to discuss security issues in the digital world.

Malware-based threats

Malware-based threats arise from malicious software designed to infiltrate, damage, or steal information from computer systems. These malicious software include, among others, viruses, ransomware, and spyware.

Viruses

Computer viruses are malicious programs that can infect regular files on a computer and get transferred from one computer to another through a pen drive, as email attachments, and in various other ways. Viruses can attach themselves to other documents, executable files or multimedia contents, and when those infected files are opened, the virus starts doing bad things to your computer. Viruses may also propagate through email attachments, whereby, upon opening or downloading such attachments, the virus program becomes operational and initiates its malicious activities (Serazzi & Zanero, 2003). Viruses have the capacity to remain concealed within various types of files, including videos, software, documents, and images. Obtaining such content from unreliable or unfamiliar persons or websites may lead to the inadvertent downloading of viruses into a system. Viruses can corrupt data, steal information, or disrupt the normal functioning of the infected device.

Ransomware

Ransomware is a malware that infects crucial data and files within a user's computer system. It encrypts the victim's files and data, or locks the system's screen, and then demands a ransom payment for getting the key required to decrypt those files or unlock the computer and regain access (Beaman et al., 2021). The infamous WannaCry ransomware attack in 2017 (Mohurle & Patil, 2017) was a large-scale global assault, resulting in significant financial repercussions across numerous sectors worldwide, including hospitals, companies, universities, and government organisations in over 150 countries. Ransomware is typically disseminated through unsolicited email attachments or embedded web links within email communications.

Spyware and Keyloggers

Spyware is a type of malicious software that scammers try to install on users' computers secretly. It is intended to spy on the user's activities and gather sensitive data such as browsing habits, websites they visit, passwords, login credentials, and documents stored on the targeted computer (Talukder & Talukder, 2020). It allows the cybercriminal to spy on what users are doing on their computers: the websites they visit, the files they create/use and other details they store on PC.

Keyloggers is a particular type of spyware that secretly records every keystroke a user makes on their keyboard and sends this data back to the scammer over the internet (Talukder & Talukder, 2020). Cybercriminals exploit this captured keystroke information to access sensitive information, such as usernames, passwords, credit card details, and other confidential data.

Attackers use a wide range of tricks to get their spyware and keyloggers installed onto the user's computer. This involves luring users into clicking on spam email links or visiting specially designed websites intended to infect their computers. Other sources of spyware and keyloggers are free games or music that one can download online.

Social engineering attacks

Social engineering refers to the art of influencing individuals or organisations to disclose sensitive information, and the process of doing so is known as a social engineering attack. It involves leveraging social interactions to persuade a target to comply with a specific request from an attacker, wherein the social interaction, persuasion, or request involves a computer or related entity. This form of attack relies on exploiting human psychology, trust, and vulnerability to gain unauthorised access to confidential data, systems, or resources. Social engineering attacks do not directly

target technological vulnerabilities but instead exploit the inherent weaknesses in human behaviour to achieve their malicious objectives.

Figure-3: Major types of social engineering attacks

Phishing attacks

Phishing attacks are the most common form of fraudulently obtaining private and confidential information through deceptive phone calls or emails. These attacks often involve using fake websites, emails, advertisements, and various false offers or advertisements (Salahdine & Kaabouch, 2019; Quayyum et al., 2021). For instance, calls, messages, or emails from a fake lottery department about winning prize money, and requesting the target to click on a malicious link and provide credit card details, insurance information, personal details, or asking for a transfer of some processing fee. Other types of social engineering attacks include:

- *Baiting* - offering free software or media downloads that contain malware.
- *Pretexting* - impersonating someone with authority and obtaining information from individuals or organisations.
- *Quid pro quo*: promising service or benefit in exchange for sensitive information.

Denial-of-service (DoS)

It involves overwhelming the target system with excessive illegitimate traffic or data, causing it to fail to respond to legitimate users (Dong et al., 2019). A Distributed Denial-of-Service (DDoS) attack aims to disrupt the normal functioning of a target website, server, or network resource, and thereby denying service to legitimate users. DDoS attacks use multiple compromised computers, known as "botnets," to carry out the attack. The objectives of DDoS attacks include causing financial losses due to downtime and damaging the organisation's reputation.

Essential Measures to Ensure Cybersecurity

Need for Cybersecurity Measures

The digital economy is expected to constitute approximately 24.3 per cent of the global GDP (Xuetong, 2020) by 2025. Additionally, e-Conomy India (2023) projections indicate that India's internet economy will likely represent 12-13 per cent of its GDP by 2030. The dynamic growth of the digital economy,

fuelled by Internet-based digital technology innovation, leads to fierce international competition while also drawing the attention of cybercriminals.

In the digital age, schools increasingly use technology for various purposes, such as online classes, student records management, examination processing, and administrative tasks. Given their handling of vital personal data, schools are vulnerable to cyber threats. As a result, cybersecurity becomes indispensable for schools and students as well to protect their sensitive information.

In a nutshell, cybersecurity is essential and indispensable in the digital age to protect individuals, organisations, and nation, due to the following reasons:

i. **Protecting Sensitive Data**: personal data, financial records, personal communication, and other information are stored and exchanged online. Likewise, schools collect and store vast amounts of sensitive student data, including personal information and academic records. Robust Hence, cybersecurity measures are necessary to safeguard this data from unauthorised access or use.

ii. **Preserving Privacy**: As individuals and organisations carry out more online activities, ensuring their privacy protection is essential. In the context of education, schools rely heavily on online learning platforms and communication tools. Security and privacy of online learning environments are crucial for students. Cybersecurity helps prevent unauthorised surveillance, identity theft, and other privacy violations.

iii. **Ensuring Business Continuity**: As organisations rely heavily on digital systems and networks for their operations, strong cybersecurity can safeguard against attack and ensure business continuity.

iv. **Protecting Critical Infrastructure**: Cybersecurity is vital to protect critical infrastructures such as power grids, transportation networks, and healthcare systems, as they can severely paralyse cities and challenge national security.

v. **Protecting National Interests**: Today, cybersecurity is closely linked to national security. Protecting critical infrastructure, government systems, and sensitive information is essential to safeguard a nation's interests and sovereignty.

Basic Cybersecurity Measures

A comprehensive cybersecurity plan for organisations to defend against cyberattacks is built upon its three key pillars:

a. **People**: Users must be educated about and adhere to fundamental data security principles, such as using strong passwords, being cautious about email attachments, and regularly backing up data.

b. **Processes**: The plan should include a well-defined framework to handle attempted and successful cyber-attacks. It should cover various aspects, such as identifying attacks, safeguarding systems, detecting and responding to threats, and recovering from successful attacks.

c. **Technology**: Utilising computer security tools like firewalls, DNS filtering, antivirus software, and email security solutions is essential to protect devices such as computers, smartphones, routers, and cloud services.

The essential cybersecurity measures for all organisations, regardless of their size, include the following:

a. **Device configuration**: Ensure systems have unnecessary functionalities removed or disabled. Set higher system security configurations and regularly update the operating system and other application software.

b. **Identity and access management**: Grant users system privileges and rights based on their specific roles. For example, it is necessary to define roles and access privileges for technical administrators, teachers, and students in a school setting. Implement multifactor authentication, requiring both passwords and OTP through mobile networks to log in to the school portal/LMS. Practice lifecycle management of users, like removing student credentials when they leave the school or when a teacher resigns.

c. **Network security**: Establish robust security settings in firewalls and routers. Employ authentication-based access for both incoming and outgoing network connections. Implement password-based access for your devices, such as printers, scanners, etc., linked to Wi-Fi or other networks.

d. **Removable media controls**: Discourage using pen drives, hard drives, or other portable storage devices on systems and disable such ports. Prefer cloud-based data transfer methods instead. If necessary to use removable media, scan all devices for malware before their use.

By implementing these basic cybersecurity measures, organisations can have the first level of readiness against cyber threats while maintaining a safer and more secure digital environment.

Cyber Safety Concerns and Awareness for Children

Cyber Safety Concerns for Children

Cybersecurity awareness is an approach to educating users about the diverse cyber threats and the vulnerability of computers and data to such threats (Rahim et al., 2015). Children nowadays spend a considerable amount of time on online activities, either for education or for entertainment. While the Internet provides numerous opportunities, it also presents various risks. Because of their young age, children frequently overlook safety and security concerns. They get lured with malicious offers and prompts, putting their privacy and safety at risk and often realising the consequences only after it's too late (Quayyum et al., 2021).

- In the context of **social networks**, raising awareness among young individuals regarding the potential privacy-related risks they may encounter is crucial. Children frequently tend to divulge their real-time locations online to a broad audience. Moreover, they often engage in geo-tagging photographs taken with smartphones and share them on online platforms. Regrettably, such geo-tagging practices can risk their online privacy, making them vulnerable to potential threats.
- The use of **smart toys** by young children introduces another dimension of risk, as inadvertent disclosure of sensitive information can occur during interactions with these devices. Particularly concerning are voice-based smart toys, which may inadvertently expose children's voice content to eavesdroppers, consequently exposing them to the possibility of audio injection attacks facilitated through these devices.

- **Online games** are becoming more interactive and immersive in nature. As children engage in virtual worlds and multiplayer environments, they may encounter various risks and threats, such as,
    - communication with strangers, disclosing their personal information,
    - getting lured through fake websites promising free in-game currency, rewards, or cheats,
    - in-game purchases, financial loss and conflicts with parents
    - addiction and excessive screen time negatively impact children's physical health, mental well-being, and academic performance, including social isolation, addiction, aggression, and even self-harm and suicide in extreme cases (Dahabiyeh et al., 2021).

Cyber Bullying

Cyberbullying is the act of harassing, intimidating, or causing harm to others through online or digital communication channels. Among school students, cyberbullying is a significant issue on social media, instant messaging, email, as well as online gaming platforms. The victims of cyberbullying are often peers, teachers, or anyone else within the school community. While online, students often perceive a sense of unchecked autonomy, believing they have the liberty to engage in any activities of their choosing while remaining unnoticed. Cyberbullying encompasses several harmful actions, including:

- **Sending Hurtful, Offensive, or Threatening Messages**: Cyberbullies use social media platforms, messaging apps, or email to send messages that are hurtful, offensive, or threatening. They may use derogatory language, insults, or name-calling to humiliate the victim.
- **Social Exclusion**: Cyberbullies spread rumours or gossip about the victim while deliberately excluding them from online groups, isolating them from their peers.
- **Creating Fake Profiles or Impersonation:** Cyberbullies create fake profiles or accounts in the victim's name and use them to post offensive content online or engage in harmful interactions with others, causing harm to the victim's reputation.
- **Publicly Sharing Embarrassing or Private Information:** Cyberbullies publicly share embarrassing or private information, photos, or videos of the victim without their consent. This humiliation can cause significant emotional distress and even instigate the victim to consider drastic measures.
- **Online Polls and Surveys for Public Shaming:** Cyberbullies create online polls or surveys targeting the victim, posing hurtful or offensive questions to shame or embarrass them publicly. This further contributes to their emotional distress and humiliation.

Combating Cyber Bullying

Cyberbullying can have severe and long-lasting effects on the victim's mental, emotional, and even physical well-being. Understanding the different forms of cyberbullying is essential to effectively recognise and address this harmful behaviour. Preventing and combating cyberbullying among school students requires a comprehensive approach involving preventive measures and intervention strategies, such as:

a. **Educating about Responsible Online Behaviour**: Students should be educated on responsible online behaviour, including understanding digital footprints, cyber ethics, and the potential consequences of cyberbullying. Additionally, they should be made aware of the importance of responsible social media use and safeguarding personal information.

b. **Implementing Anti-Cyberbullying Policies**: Schools should develop and enforce anti-cyberbullying policies, ensuring that students are well-informed about the repercussions of engaging in cyberbullying behaviour. If needed, schools can employ trained counsellors to resolve conflicts between the victim and the cyberbully,

c. **Fostering a Positive and Inclusive School Culture**: To cultivate a positive and inclusive school environment, promoting respect, kindness, and empathy among students can reduce cyberbullying incidents.

d. **Establishing an Anonymous Reporting System**: Schools should establish a confidential reporting system, allowing students to report cyberbullying incidents without fear of retaliation. If cyberbullying incidents get noticed, schools must immediately investigate the incidents, identify the perpetrators, and protect the victim. Schools should involve law enforcement agencies in severe cases of criminal cyberbullying incidents.

e. **Involving Parents in Monitoring Digital Activities**: Encouraging parents to become role models for their children by adhering to a structured schedule for digital gadget usage, maintaining open communication, and monitoring their children's online experiences and behaviours.

Misinformation and Fake News

In recent years, fake news and misinformation have gained significant traction through social media and other online platforms. Fake news refers to intentionally fabricated or distorted news items presented as factual information, while misinformation consists of factually incorrect information presented as news to deceive consumers. The prevalence of social media has exacerbated the problem, enabling rapid dissemination and a broader reach of false information (Sharma et al., 2019).

Deceptive communication through the Internet can have far-reaching consequences, affecting financial, political, and societal aspects. Fake news has been linked to influencing national elections, damaging reputations, and inciting violence and chaos. Photographs or videos of past events are often misrepresented as something else on social media. False and provoking captions accompanying these images or videos lead to the rapid spread of rumours or fake stories and, at times, escalate into physical violence, riots, and social chaos. Misinformation about health tips, home remedies, etc., spread through social media and instant messaging groups can also harm public health.

Research suggests that people tend to believe in information aligned with their ideologies, leading to the sharing of false information within like-minded communities. Given the vast amount of information available online and the speed at which it can spread, combating misinformation and fake news in the age of the internet is a complex and ongoing challenge. Dealing with Misinformation and Fake News requires a multifaceted approach, including media literacy

education, fact-checking initiatives, responsible sharing, technological solutions, and global cooperation.

Cyber Safety Awareness

The importance of cyber safety and cybersecurity awareness for everyone is significant, especially with the added complexity of cyber threats during the COVID-19 pandemic (Bada et al., 2019; Chang & Coppel, 2020; Dash & Ansari, 2022;). Education and awareness campaigns are crucial in promoting cybersecurity awareness among individuals, organisations, and society (Jena, 2020; Khan et al., 2020; Rahim et al., 2015). These campaigns teach people about online threats in the forms of malware, phishing, ransomware, and social engineering, making them more cautious online. They also educate about essential security measures, like strong passwords, two-factor authentication, and safe browsing habits. Moreover, these programs are vital in educating children and teenagers about data privacy, cyberbullying, responsible social media use, and avoiding financial fraud through phishing and other tactics. Raising awareness through such campaigns is essential for inculcating secure and vigilant online behaviour.

Cyber Safety and Responsible Behaviour

This section enlists some of the good practices for safeguarding against cyber threats. It also talks about the practice of cyber hygiene in a digital environment and the online behaviours can save us from the ethical and legal concerns related to the cyber world.

Strategies for Safeguarding Against Online Scams

a. **Be vigilant and think critically** - on receiving a message claiming to be from authority and asking for urgent action, take a moment to pause and question its legitimacy. Consider whether a genuine authority figure would demand such quick action.

b. **Search on the Internet** - if a message or news appears suspicious, perform a quick Internet search with a brief description of the matter along with the term "scam".

    a. **Second level verification** - even while you receive an email from a supposedly trusted organisation, verify its authenticity by calling it. Ensure not to use the phone number provided in the email footer.

    b. **Caution during online payment** - Use known and trusted platforms for handling credit card transactions and other online payments

    c. **Report suspicious incidents** - don't feel embarrassment or reluctance in reporting scams. File a police report or notify relevant authorities such as the National cybercrime portal (https://cybercrime.gov.in/) or cybercrime helpline number 1930 about any cybercrime.

Safety Measures to Prevent Cyber Attacks

This subsection summarises the cybersecurity best practices that can mitigate the chances of cyberattacks. It recapitulates a list of best practices related to social media usage, password management, software updates, hardware updates, and other cybersecurity measures.

Social Media Usage

i. Be cautious on social media platforms and avoid accepting friend requests from strangers. Trust online users only if you know them in real life.

ii. Refrain from sharing sensitive personal information on social

media, such as address, phone number, and date of birth, etc., to prevent identity theft.

iii. Share personal photos and videos only with trusted friends using appropriate privacy settings on social media platforms.

iv. Immediately notify the social media service provider if you come across a fake account created with your personal information.

v. Verify each message, photo or video before posting or sharing on social media, as they may contain fake news, misinformation, or sensitive information.

Password Management

i. Never use easy-to-guess passwords such as your mobile number, email address, home address, PIN code, date of birth, etc.

ii. Always set strong passwords containing a mix of alphabets - both uppercase and lowercase, numbers, and special characters (e.g., @ # $ % ^ & * ( ) _ + | ~ - - = Thank you for reaching out ' { } [ ] : " ; < > / , etc.) for social media accounts and all other websites requiring username and password to access.

iii. Regularly change passwords (usually once every 3 months) to enhance security and prevent malicious activities. Never reuse the same password for multiple accounts or websites.

iv. Use two-factor or multi-factor authentication (e.g., requiring both password and mobile OTP to log in to your banking portal) to add an extra layer of security to your accounts.

Software and Network Management

i. Regularly update your operating system, antivirus software, and other installed software applications to remove vulnerabilities that hackers may exploit.

ii. Download software from the original website only, and never go for websites that promise software for free.

iii. install mobile apps only from legitimate and trusted sources or app stores and keep your mobile device updated with the latest Android/iOS version.

iv. Install trusted and legitimate anti-virus protection software.

v. Keep the firewall in the operating system always on.

vi. Secure your Wi-Fi networks by setting a password to access them. Avoid using public Wi-Fi without a VPN to prevent unauthorised access to your data.

Email and Data Protection

i. Avoid opening emails from unknown senders and carefully scrutinise email attachments or the links given for potential threats and phishing links.

ii. While forwarding an email from a chain of emails to a new user, check whether that email chain contains any sensitive or confidential information. Before forwarding an email that is part of an email chain with a new user, ensure that it does not contain any sensitive or confidential information

iii. Regularly backup your important data on different devices or cloud storage to ensure data availability and recovery during a cyber-attack.

Discussion and Way Forward

Cybercriminal gangs are continuously innovating ways to exploit vulnerabilities and enhance the efficiency of their attacks. As time progresses, the

complexity of these attacks is on the rise. For instance, the Ransomware report (2023) from the Indian Computer Emergency Response Team (CERT-In) highlights a notable 53 per cent increase in reported Ransomware incidents in 2022 compared to the previous year. The report also draws attention to a worrying skill gap in managing Ransomware attacks, assessing the scope of infections, inadequate IT inventory lists, and improper computer network configurations, identified as critical areas of concern while combating cyber threats.

Promoting digital literacy among common citizens, especially in rural areas, is a challenging but crucial task to empower them with the knowledge and skills for safe internet navigation. The National Education Policy (NEP, 2020) has advocated the integration of digital technology across education, encompassing enrollment, transfer, assessment, and providing access to interactive learning resources utilising AR, VR, 3D, and other emerging technologies. Consequently, it becomes imperative to incorporate age-appropriate cybersecurity education programs into schools (Pencheva et al., 2020) and teacher education curriculums, equipping students and teachers to address the intricacies of cyber safety and security effectively.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490.

CERT-In | *Indian - Computer Emergency Response Team*. (accessed on 29 August 2023). https://www.cert-in.org.in/

CISA | Protecting our Future: Cybersecurity for K-12 (2023). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*, 101959.

Clark, R. M., & Hakim, S. (2017). Protecting critical infrastructure at the state, provincial, and local level: issues in cyber-physical security. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 1-17.

Dahabiyeh, L., Najjar, M. S., & Agrawal, D. (2021). When ignorance is bliss: The role of curiosity in online games adoption. *Entertainment Computing*, *37*, 100398.

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, *7*, 80813-80828.

e-Conomy India 2023. (2023, June 6). By Google, Temasek, and Bain & Company. Retrieved July 1, 2023, from https://services.google.com/fh/files/blogs/india_economy_report_2023.pdf

Fagen, M., Maronn, J., Brady, K., Cuthill, B., Megas, K., Herold, R., Lamire, D., & Hoen, B. (2021). IoT device cybersecurity guidance for the federal government. National Institute of Standards

and Technology (NIST) Special Publication 800-213. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-213

Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief.

Hero, A., Kar, S., Moura, J., Neil, J., Poor, H. V., Turcotte, M., & Xi, B. (2023). Statistics and Data Science for Cybersecurity. Harvard Data Science Review, 5(1). https://doi.org/10.1162/99608f92.a42024d0

Jena, P. K. (2020). Impact of pandemic COVID-19 on education in India. *International journal of current research (IJCR)*, *12*.

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*, *7*(421), 11-14.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Kidd, W., & Murray, J. (2020). The Covid-19 pandemic and its effects on teacher education in England: how teacher educators moved practicum learning online. *European Journal of Teacher Education*, *43*(4), 542-558.

Knott, J., Yuan, H., Boakes, M., & Li, S. (2023, March). Cyber Security and Online Safety Education for Schools in the UK: Looking through the Lens of Twitter Data. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (pp. 1603-1606).

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), 29-41.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International journal of advanced research in computer science*, *8*(5), 1938-1940.

NEP. (2020). National Education Policy. Ministry of Education, Government of India. Retrieved June 10, 2023, from https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf

NICCS | *Cybersecurity for teachers*. (2022). National Initiative for Cybersecurity Careers and Studies. https://niccs.cisa.gov/education-training/cybersecurity-teachers

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68-74.

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382.

Rahim, A., Hayani, N., Suraya, H., Kiah, M. L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*.

Ransomware Report. (2023, April 13). The Indian Computer Emergency Response Team. Retrieved May 18, 2023, from https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016, June). Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, *97*, 587-597.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, *11*(4), 89.

Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly*, *39*(5), 821-837.

Serazzi, G., & Zanero, S. (2003, October). Computer virus propagation models. In *International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems* (pp. 26-50). Berlin, Heidelberg: Springer Berlin Heidelberg.

Sharma, K., Qian, F., Jiang, H., Ruchansky, N., Zhang, M., & Liu, Y. (2019). Combating fake news: A survey on identification and mitigation techniques. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *10*(3), 1-42.

Talukder, S., & Talukder, Z. (2020). A survey on malware detection and analysis tools. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *12*.

Xuetong, Y. (2020). Bipolar rivalry in the early digital age. *The Chinese Journal of International Politics*, *13*(3), 313-341.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97.