ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2023; 9(6): 12-15
www.allresearchjournal.com
Received: 10-04-2023
Accepted: 15-05-2023

Dr. Bhuvneshwar Prasad Gaur
Associate Professor,
Department of Education,
Forte Institute of Technology,
Meerut, Uttar Pradesh, India

Corresponding Author:
Dr. Bhuvneshwar Prasad Gaur
Associate Professor,
Department of Education,
Forte Institute of Technology,
Meerut, Uttar Pradesh, India

Cybersecurity awareness education in schools: A review

Dr. Bhuvneshwar Prasad Gaur

Abstract
Internet has become the lifeline of our life today. Internet, all of us have also become a part of a cyber world wherein we share and access resources, connect and interact with many people. Just like real world we need to be cautious and alert while working in this cyber world as well. Cases like cyber-bully, Online Grooming, Phishing, Juice Jacking, Threats due to Keyloggers, Threats due to spam mails, 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. However, past studies revealed that the level of awareness among Internet users is still low or moderate. One of the vital measures to be taken is to cultivate knowledge and awareness among Internet users from their early age, i.e., young children. Young children specifically, need to be educated to operate in a safe manner in cyberspace and to protect themselves in the process. Today it is necessary for our students as well as teachers and parents of children to know about the safe use of the Internet. In this review paper, some strategies related to awareness education related to cyber security in schools have been discussed.

Keywords: Internet, cybersecurity, cyber safety, cyber crime, cyber education, cyber awareness

Introduction
Today it is necessary for our students as well as teachers and parents of children to know about the safe use of the Internet. Cybersecurity is crucial in any business setting, but especially in education. Cyberattacks not only compromise the safety and security of teachers and school administrations, but also the privacy of students particularly minors in schools. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cybersecurity should not be limited to the classroom- virtual or otherwise. Since most home networks do not provide the same increased firewalls or protections offered by institutions, teachers and students become more susceptible to hacking attempts as they spend more tine online. It is Important to practice safe online behaviour everywhere. Use of the internet is not limited to adults, but 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.

Cybersecurity means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today's world, cybersecurity is very important because of some security threats and cyber-attacks. For data protection, many companies develop software. Cybersecurity is important because not only it helps to secure information but also our system from virus attack. After the USA and China, India has the highest number of internet users.

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.

Cybersecurity education is necessary because cybercrime cases can occur anywhere regardless of individuals, organisations and places.

Cyber security

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information.

Cyber Crime

Cybercrime is defined as any unauthorized activity involving a computer, a digital device, or network. Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them.

The Need for Cybersecurity Education

Schools need enterprise-class security measures and hardware-enabled security to help protect their students, faculty, and data from cyberattacks. Cybersecurity refers to the protection of networks, devices, and data from unauthorized or unintended access or illegal use. Cybersecurity education is also needed to control addiction to computer games. This addiction certainly has a negative impact. Teenagers spend a lot of time on computers and socialise through their gadgets. Over time, an addiction to online games cannot be avoided, and teenagers' precious time is taken up by addiction to their gadgets.

Challenges of Cyber Security Education

The carious challenges schools face in implementing cybersecurity education include lack of expertise, funding and resources. Lack of knowledge in Teachers and expertise regarding cyberspace. Schools and government ministries may lack resources and facilities to implement cybersecurity education. The speed of technological change results in new risks, requiring new solutions. Teachers may face problems in developing their knowledge of the latest technology and thus ensuring students are safe.

Methodology

This paper has two research questions.

What is the importance of cybersecurity education in schools?

According to the literature review, there are many benefits if a school is able to fully apply cybersecurity education. A survey on adults and cybersecurity states that participants are less willing to spend money or time on seminars or programmes about cybersecurity. It is therefore crucial for schools to become knowledge centres to expose issues around cybersecurity to the community. School administrators and teachers can discuss together and organise school programmes or activities about cybersecurity. Moreover, cybersecurity education is beneficial for changing the mindset of individuals. Every person who lacks cybersecurity awareness is a result of not being informed of the importance and effects of cybersecurity itself.

What are the strategies that stakeholders can use to promote cybersecurity education in schools?

Video cartoons were identified as resources for teachers to use when discussing cybersecurity principles with primary school learners, for example, using the U-PIN and I-PIN stories to raise awareness of cybersecurity. The primary school subjects of Information and Communication Technology need to be improved to include cybersecurity topics. In addition, the safety aspects of cybersecurity can be taught through other subjects. Teacher education programmes must also prepare their pre-service & n-service teachers to model and teach cybersecurity topics and safe computing practices so that future generations will know how to behave ethically, as well as to keep themselves safe and secure online. Moreover, security awareness programmes are one of the strategies that can promote cybersecurity education in school. Even though students develop a high level of awareness on some cybersecurity issues such as cyberbullying, sharing personal information and internet banking, little information is given to them regarding cyber-sex and self-protection.

Cyber Safety Tips for Teachers, Students & Parents

Cyber security should not be limited to the classroom – virtual or otherwise. Since most home networks do not provide the same increased firewalls or protections offered by institutions, teachers and students become more susceptible to hacking attempts as they spend more time online. It is important to practice safe online behaviour everywhere.

Online Transaction/Financial Frauds

Always be sure about the correct web address of the bank website and look for the "lock" icon on the browser's status bar while visiting bank's website or conducting any online transaction. Secure way of swiping credit/debit cards. Do not share your Net Banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. to any person even, if he is claiming to be employee or representative of bank and report such instances to your bank. Beware of KYC/Remote App Frauds. Enhance your protection by deploying additional layer of security to access your online accounts or doing online financial transactions by enabling two factor authentication (2FA) - username with password and OTP on your mobile. Do not respond to any message assuring credit of money into your bank account with request to share personal details. It may be an attempt to defraud you. Secure password practice. Public networks might not be secured. Avoid financial transactions on these networks. Alternatively, use personal mobile data or VPN (Virtual Private Network). Security against fake banking E-mails.

Online Job Fraud

Many organisations conduct interviews through telephone, chat services, Skype calls or Google hangouts. Please check credentials of organisation and its representative before the online interview. Make sure to ask detailed questions related to job and organisation from interviewer. Beware of the emails, which offer jobs in exchange for money, such emails are spam. No organization/ company ever asks for money to

work for them. Many job portals offer paid services for resume writing, resume promotion, and job alerts. Before paying to these portals, check authenticity and reviews of the website. Consult your family and friends to know about reliable websites. Always look for the spelling errors in the e-mail address and job descriptions. If an email has spelling, grammatical and punctuation errors, it could be a scam. Always check the website of the Government organisations for details about the job openings in a government department. All government websites have "[dot]gov[dot]in" or [dot]nic[dot]in as part of their website address (e.g. mha.gov.in).

Unauthorized Access/data breach

Do not leave your phone unattended in public places and refrain from sharing your phone password / pattern lock with anybody. Always enable a password on the home screen to restrict unauthorized access to your mobile phone. Configure your device to automatically lock beyond certain duration. Many mobile apps ask for many permissions to access data and functions regardless of the necessity for functioning of the app. Identify nature of app, assess the necessity of permissions asked while installing app and avoid giving unwanted permissions. Enable mobile device access to third-party applications selectively. Do you know some malicious apps, if given SMS access, may read OTP and other sensitive information from your messages. Always lock your computer before leaving workplace to prevent unauthorized access. A user can lock computer by pressing 'ctrl +alt+del' and choosing 'lock this computer' or "window button+ L". Be aware while using public charging points.

Wireless / Bluetooth security awareness

Secure all the wireless access points (Wi-Fi, Routers) with a strong password. Hackers usually scan for open access points, a method called as war-driving to anonymize their identity. Be careful while using public Wi-Fi at Airports, Railway Stations, Bus Stops etc. Public Wi-Fi is an easy target for any hacker to steal your information. Use secure VPN or proxy to avoid unauthorised access to your personal information.

Virus, Worms and Trojans

Do not use public computer/ cybercafé to access social networking websites, it may be infected/ installed with a key logger application to capture your keystrokes including the login credentials. Be careful of what you plug in to your computer. Malware can spread through infected USB drives, external hard drives, and even smart phones. Computers should be protected from virus/worms using an Antivirus software. It is advisable to keep Auto run / Auto play feature disabled for all removable media. Never download any content like Images, Videos, Apps, Games, System Software, Software Drivers, Operating Systems etc. from unknown sources. They might contain malware.

Phishing and Spamming

Heard a lot about Phishing, but how to identify it? Hackers generally use link manipulation as a method to create illegitimate URLs. E.g. For a legitimate link like yourbank.com, a phished link would look like y0urbnk.com. Use caution while clicking on links received as a message from your friends, posts on social networking websites, e-mails, etc. It can be a malicious link that may compromise your personal information. Beware of "Smishing", where hacker uses cell phone text to trick the users. Attackers use URL link or number in text messages, make sure you don't click on the link. Never click on any UNKNOWN messages with links and do not reply to text messages. Never open spam emails unless the source is authentic as such emails may download malware silently in the background and may lead to personal data loss.

Phishing and Spamming Cyber Bullying / Stalking / Grooming / Sexting

If you are victim of cyber stalking, consult your parents, friends or relatives and file complaint against the cyber stalker on National Cyber Crime Reporting Portal/ Police. Also save all communications with the stalker as evidence. Cyber Stalking means, using internet or any electronic means to harass or stalk any individual/ group or an organization. Two dangers that can haunt social media users are stalking and cyberbullying. To deter stalkers, disable auto location update services of social media sites/Apps and refrain from tagging your location on your posts. Be careful to upload your photos on social media which show your location or places you frequent visit as cyber stalker may keep tab on your daily life. Do not accept friend requests from strangers on social networking sites. Teachers and parents should regularly discuss about cyber threats with children and encourage them to inform in case they are a victim. Act against Cyberbullying. Delete any unwanted messages or friends who continuously leave inappropriate comments. Children must share such incidents with their parents. Such inappropriate comments can be flagged and reported to the networking site for action.

Online Matrimonial Frauds

Always choose to meet the prospective match in a public place as you don't know what kind of person he or she might be. Also, keep your family and friends informed about the meeting. This will help avoid matrimony frauds. While chatting on matrimonial website, avoid talking to a person, if he/ she pressurizes you to reveal your personal information. Always refrain from sharing your personal information until you are completely sure and have done a thorough background check. Always be careful while dealing with 'NRI' profiles on matrimonial websites. Commit to marriage only after face-to-face meetings, especially the prospective match's parents/ relatives and validating any documents related to their address and employment abroad.

Ransomware

Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files. Do not pay the ransom. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files. Lookout for the latest scams! Currently, "ransomware" is on the rise. Make sure you do not click or download links from unknown sources. Hackers can steal your credentials and encrypt your data and demand ransom to decrypt it.

Logic bombs

These are event dependent programs. These programs are activated after the trigger of specific even. Chernobyl virus

isa specific example which acts as logic bomb and can sleep of the particular date.

Web Jacking
Web jacking is the forceful control of a web server through gaining access and control over the web site of another. Hackers might be manipulating the information on the site.

Stealing cards
Information Stealing of credit or debit card information by stealing into the ecommerce server and misuse these information.

Cyber Terrorism
Deliberately, usually politically motivated violence committed against civilians through the use of, or with the help of internet.

Child Pornography
The use of computer networks to create, distribute, or access materials that sexually exploit underage children pornography in shared drives of community networks.

Cyber Contraband
Transferring of illegal items or information through internet that is banned in some locations, like

Malware scanners
This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls
A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Anti-virus Software
Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

Role of Social Media in Cyber Security
As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

Conclusion
Today due to high internet penetration, cybersecurity is one of the biggest need of the world as cybersecurity threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free. Based on a synthesis of the literature selected, 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, Mobile awareness van must also play an important role in educating children through cybersecurity campaigns because such campaigns are more interactive and interesting for children to understand.

References

1. Cyber Dost, Cyber Safety, Indian Cyber Crime Care Centre, Ministry of Home Affairs, Government of India; c2023.
2. Gaur, Bhuvneshwar Prasad. The importance of educational technology in teacher education, Legal Journal of Royal College of Law. 2022;9:25-27. ISSN: 3454 5910.
3. Ahmad N, Mokhtar UA, Hood Z, *et al*. Cyber security situational awareness among parents,‖ presented at the Cyber Resilience Conference, Putrajaya Malaysia. 2019 Nov 13-15:7-8, 2020.
4. Lokman HF, Nasri N, Khalid F. The effectiveness of using twitter application in teaching pedagogy: A meta-synthesis study, International Journal of Academic Research in Progressive Education and Development. 2019;8(2):205-212.
5. Rahim NHA, *et al*. A systematic review of approaches to assessing cybersecurity awareness, Kybernetes; c2015.
6. Dong P, *et al*. A systematic review of studies on cyber physical system security, International Journal of Security and Its Applications. 2015;9(1):155-164.
7. Kim EB. Recommendations for information security awareness training for college students. Information Management & Computer Security. 2014;22(1):115-126. DOI: 10.1108/ IMCS-01-2013-0005.
8. Gaur, Bhuvneshwar Prasad, Rani Sharma. Multimedia is the best instructional package than audio-visual instructional package & conventional instructional package on the achievement of information technology in school education, The Journal of Business & Economic Studies, ISSN: 2320 110X. 2013;6-2&7-1: 67-78.