**Dr. Naresh Kumar**

Assistant Professor

D.A.V. College of Education, Hoshiarpur

**e-mail:** drnksharma0181@gmail.com

**Cybersecurity in Education**

**Abstract**

We live in a technologically advanced world that is continually evolving due to advances in digitalization, it is clear that no industry is immune to the threat of a cyber-attack today. With the advancement of technology, we are becoming more vulnerable to larger cyber threats from hackers looking for more polished ways to commit criminality. Regrettably, it now extends to schools, colleges, and universities. The vast amount of data held by educational institutions, as well as the growing number of inter-connected devices, make this sector a target for cyber-attacks. According to [Microsoft](https://www.microsoft.com/en-us/wdsi/threats), education is globally the sector most vulnerable to threats like malware, accounting for more than 6.8 million (over 63%) of total reported encounters in early 2022. Given the complexity of today's networks and the dangers to their security, we can say that standard anti-virus solutions are no longer sufficient. As a result, cybersecurity is an IT issue, but is now tackled holistically across all sectors, and should be treated as a collective effort to reduce. The paper highlights the major cyber threats for educational institutions, teachers, students and parents along with safety measures.

**Keywords:** Cybercrimes, Cybersecurity, Education, Teachers, Students, Parents

**Introduction**

In current scenario, cybersecurity has become one of the greatest concerns for schools/colleges/universities/governments, and industrial institutions around the world. In February 2021, Simon Fraser University in British Columbia, Canada, was the victim of a cyber attack. Hackers had breached servers containing sensitive information such as student and staff ID numbers, admission details, and other academic records. A total of about 200,000 people were affected by this cyber attack. For hackers, educational institutions are a treasure trove of personal information and ideal targets. As per the report of “Threat Research and Information Analytics Division of CloudSEK”, 20% cyber threats are increased at the global education sector in the first three months of 2022, as compared to the corresponding period of 2021. As the threats detected in Asia and Pacific region last year, 58% of them were targeted in Indian educational institutions. This included BYJU’s, IIM-Kozhikode and Tamil Nadu’s Directorate of Technical Education. Recently, between June 2022 and May 2023, there were 190 known ransomware attacks against educational institutions, and many more that went unreported and unrecorded. Between the first and second six months of that period, education experienced an **84% increase in attacks.** As per a report by Checkpoint, in comparison of 2022, each organization in India faced an average of 2108 weekly cyber attacks.

Many institutions also manage large budgets to deal with the problem of cyber attacks. In 2021, organizations spent more than $150 billion on cybercrime protection and by 2025, the cumulative spending could be as high as [$1.75 trillion](https://cybersecurityventures.com/cybersecurity-spending-2021-2025/#:~:text=The%20imperative%20to%20protect%20increasingly,2025%2C%20according%20to%20Cybersecurity%20Ventures). From ransomware to phishing to barbaric pressure tactics, educational institutions are now looking for ways to protect sensitive records online while protecting students and their personal information from hackers. Therefore, cybersecurity must be an integral part of the mission of all educational institutions. Students, teachers, and administrators all need access to the learning tools they need to understand, detect, and prevent cyber threats that they may encounter in their daily activities.

**Cybersecurity**

The act of securing computers, servers, mobile devices, electronic systems, networks, and data from hostile intrusions is known as cybersecurity. It's also known as electronic information security or information technology security. The word can be applied to a wide range of situations, including workplace and mobile computing. A solid cybersecurity plan can give a good security posture against hostile attacks aimed at gaining access to, altering, deleting, destroying, or extorting sensitive data from an organization's or user's systems. Cybersecurity is also important in preventing attacks that try to disable or impair the operation of a system or device.

**Types of Cyber Threats**

The threats countered by cyber-security are three-fold:

1. [**Cyber Crime**](https://www.kaspersky.com/resource-center/threats/cybercrime)**:** It comprises individuals or groups who target systems for monetary gain or to inflict havoc.
2. **Cyber-Attack:** It frequently entails politically driven data collection.
3. **Cyber Terrorism:** Its goal is to generate terror or dread by undermining electronic systems.

**Why Education Sector is a Target for Cyber Crimes?**

Educational institutions vary in size, purpose, and stature, and the motives of hackers can also vary accordingly. Educational institutions need to evaluate their individual risks and understand what data is vulnerable to unauthorized access. There are many reasons that's why education is becoming a prime target for cybercriminals as listed below:

* **Distributed Denial of Service Attack:** It's a regular attack on online users and sites, especially educational institutions. These attacks slow down any online productivity by interfering with one's Internet connection and network.
* **Espionage:** It's also a new way for bad actors to assault you online. Cybercriminals can monitor the activity of students, teachers, and others in a school or institution, and even use the information to abuse or threaten students or teachers. Cybercriminals can steal and/or corrupt educational data over an unprotected network.
* **Data Theft:**  When espionage is employed to obtain sensitive material from institutions such as schools, colleges, and universities, this is known as espionage. Student contact information is a common example of sensitive data (i.e., address, grade level and status, etc.). Personal data on students, teachers, and others (e.g., social security numbers, credit/debit card numbers, and so on). Grading systems, for example.
* **Financial Gain:** When conducting theft and crime in a school or institution's data system, cybercriminals are usually searching for monetary benefit. They have two options: they can either sell sensitive material online or keep the educational institution hostage. They may prevent the school from accessing its own data until a ransom is paid, so turning it into a ransom-ware attack.

**Escalation of Cyber Attacks in the Education Sector**

The following are the main reasons of escalating cyber attacks in the education sector:

* **Limited Budgets:** In the 2021 Security Scorecards report, education was placed last among all industries in terms of cybersecurity. Colleges, particularly public institutions, face budgetary challenges. Security investments often come at the expense of other priorities, and they are frequently put on the back burner.
* **Lack of Technical Staff:** A shortage of technical staff in educational institutions could also be a factor. While most school staff consists of instructors, administration, custodians, and maintenance, having a tech crew to check into cyber threats might be beneficial.
* **Open Networks and Lots of Apps:** Students and employees have access to a wide range of apps and data through college networks, which cover a large area. Every site has the potential to be an opportunity. Institutions are concentrating on making student access simple and providing all of the amenities that make their university competitive. However, this opens the door for hackers.
* **Students Make Easy Targets:** Corporations have the ability to train its personnel as well as their contractors. They put money towards online schooling. Every year, colleges welcome a new class of students, making extensive cyber education impossible with such a huge student body. Because the young are generally unskilled, they are more vulnerable to standard hacking approaches.
* **Many Devices:** BYOD is king on college campuses. Everyone has their own laptops, desktops, phones, and tablets, and they are all connected. Every device represents an opportunity.
* **Big Campuses are Stranger Friendly:** The college campus offers more opportunities for social engineering, tailgating, and man-in-the-middle attacks. Strangers can easily enter and go undetected, planting USBs, intercepting traffic, and entering labs and research centres.

**Security Measures for Educational Institutions from Cyber Attacks**

Here are some great tips to follow:

* **Training of Staff and Students:** Ensure that everyone, including students, teachers, and staff, understands how to recognise questionable internet activity and what to do about it. At least once a year, educational institutions should engage in cyber event planning and response training for their IT employees. This can assist the organisation in developing its own effective cyber event response strategies, which can help safeguard the institution from the financial and reputational harm that cyber-attacks can cause.
* **Appointment of IT Team: Install ransomware, phishing, and DDOS protection with the help of an IT team. Your organisation can choose from a variety of low-cost services and one-time investments to improve overall cyber resilience. Your computer networks and systems will be significantly safer with a few basic security software, and your educational institution will be protected at least from many fundamental cyber dangers.**
* **Encourage Staff and Students to use Two-Step Authentication:** Students, teachers, and other staff members should be required to submit not only a password, but also another level of authentication in the form of a secret answer, completing a riddle, or entering a numeric code when login into school computers (or other devices).
* **Live Fire” Drills: "Live fire" drills involve the administration performing a simulated cyber-attack during regular school hours, similar to traditional fire drills. As they strive to resolve and respond to the problem, students and teachers refer to their training. These drills can also be sent to everyone at school by text messages, emails, and other means. Conducting a full-fledged cyber crisis tabletop simulation would be even better for educational institutions with a larger budget. These are scenario-based exercises that simulate a cyber-attack and force participants to think and behave as if an actual cyber-attack had occurred. These tabletop exercises are also incredibly cost-effective, as they allow the organisation to test its cyber breach readiness while causing minimal disruption to normal operations.**
* **Network Security: The practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware, is known as network security.**
* **Application Security: The goal of application security is to keep software and devices safe against attacks. A hacked application could allow access to the data it was supposed to secure. Security starts throughout the design phase, long before a programme or device is deployed.**
* **Information Security: Data integrity and privacy are protected by information security, both in storage and in transport.**
* **Operational Security: The processes and decisions for handling and securing data assets are included in operational security. The protocols that dictate how and where data may be stored or exchanged, as well as the permissions users have while accessing a network, all fall under this umbrella.**
* **Disaster Recovery: Disaster recovery and business continuity are terms used to describe how a company reacts in the case of a cyber-security breach or any other catastrophe that results in the loss of operations or data. Disaster recovery policies specify how the organisation restores operations and information in order to resume activities at the same level as before the disaster. Business continuity is the plan that an organisation uses when it is unable to operate due to a lack of resources.**
* **End-user Education Addresses:** The most unpredictable cybersecurity component is end-user education. By failing to follow appropriate security standards, anyone can unintentionally introduce a virus into a safe system. It is critical for every organization's security to teach users to delete suspicious email attachments, not plug in unrecognised USB drives, and a variety of other key teachings.

**Cyber Attack Risks for Teachers**

The best first step in cybersecurity for a teacher is to be aware and understand the best practises for protecting yourself and your students. According to a research by the Consortium for School Networking (CoSN), the top five cybersecurity dangers that teachers' encounter are listed below

* **Phishing**: These attacks use social engineering to deceive victims into handing over sensitive information like passwords or credit card numbers. According to CoSN, phishing is the starting point for over 90% of cyber attacks nowadays.
* **Distributed Denial-of-Service**: Multiple systems overload the bandwidth or resources of local servers, resulting in these attacks. These attacks can cost victims up to $40,000 per hour, whereas cyber attackers normally only spend around $40.
* **Data Breach:** A data breach is a security incident in which unauthorised access to private or sensitive information (such as student data) occurs. In fact, one of the most common cyber events in 2019 was the compromise of student and educator data.
* **Ransom-ware:** Hackers are keeping data hostage in return for money or other demands in these threats. Ransomware's potential cost in the United States reached over $7.5 billion in 2019, according to a report by cybersecurity firm Emisof.
* **IoT Vulnerabilities:** Because IoT (Internet of Things) devices like laptops, smart home accessories, and tablets frequently lack security or are not updated on a regular basis, teachers must emphasise security when introducing IoT devices into the classroom.

**Safety Measures for Teachers**

Now that we've learned about the cyber risks that educators face today, we may be wondering what we can do to keep ourselves, our schools, and our kids secure. We can take the following five steps to assist prevent these attacks:

* **Encrypt Your Data:** Hackers can now access data from classrooms by intercepting it while it is in transit. By encrypting your data, you can keep cyber criminals from stealing the information you send and receive.
* **Comply With Your Institution’s Cyber Protocols:** Your school's cybersecurity procedures are almost certainly already in place to protect users. It's critical to adhere to these guidelines and to alert your IT or Cybersecurity department if a problem emerges.
* **Safeguard Your Devices From Physical Attacks:** When you leave your computer, always log out. To keep your passwords safe, avoid writing them down or entering them in front of another person.
* **Back Up Your Data:** If your job or institution necessitates the preservation of student data, you should back it up to avoid attackers from using it in Ransomware-style assaults, in which you could be locked out unless you pay a ransom.
* **Practice Good Password Management:** When it comes to passwords, it's all too simple to take shortcuts. Last Pass, a password management application, can assist in creating unique passwords for all of your accounts.

**Cyber Attack Risks for Students**

Before we can prevent an assault, we need to have a good grasp of the threats that today's student confront. The following are five different sorts of attacks to be cautious of:

* **Data Theft:** Cyber attackers are aware, according to CNBC, that students often have insufficient grasp of how to properly protect personal and financial data when entering it online for the first time. Hackers could use this information for identity theft, credit fraud, and other crimes, according to experts.
* **Mobile Malware:** Attacks on mobile devices have increased by 50% during 2018, according to Check Point researchers. With more students switching from a desktop or laptop to a smartphone, mobile security is more crucial than ever.
* **Malicious Social Media Messaging:** Hackers are using platforms like Facebook and WhatsApp to attract victims to phishing websites, which can compromise personal information, according to a study on cybersecurity concerns during the COVID-19 epidemic.
* **Confession:** Many students' phones, tablets, and laptops now include a desktop webcam or camera. Unfortunately, this could lead to confession, in which hackers gain remote access to and control of a webcam.
* **Social Engineering:** According to Education Dive, social engineering schemes are among the top cybersecurity dangers facing higher education students. These attacks rely on users being duped into divulging sensitive information**.**

**Safety Measures for Students**

Cyber criminals are always coming up with new exploits and tactics to breach users. To defend the students from them, here are five cybersecurity recommended practises:

* **Avoid Sharing Personal Information:** Be cautious about the information you share on the internet, such as your school's name, email address, home address, and phone number.
* **Invest in Virus Protection:** Ensure that all of your devices are protected with antivirus and anti-phishing software (desktops, laptops, tablets, etc.). Set it to automatically update and scan for viruses at least once a week.
* **Keep Software Up-to-Date**: Make sure your operating system, browser software, and apps are all patched up to date. Even new machines may contain out-of-date software, putting you at risk.
* **Be on Guard for Phishing:** Untrustworthy email attachments should not be opened. You may be expecting emails from group members or teachers, but open any attachments with caution.
* **Be Careful What You Click:** Avoid going to unfamiliar websites or downloading software from untrustworthy sources. These websites may include malware that will secretly install and corrupt your computer.

**Cyber Attack Risks for Parents and Children**

According to a PCMag research, seventy six percent of parents are concerned about their children's online safety and have serious concerns about the internet hazards they encounter. The following are the common cyber attacks aimed at young web users:

* **Cyber Predators:** Adults who use the internet to harm children and/or teenagers (whether emotional, financial etc.) are known as internet predators. As per the report of Cybertip, a Canadian tip line, online child exploitation, has had an increase of 81% in reports.
* **Malware:** Today's cyber criminals frequently use deception to get victims to download malware that allows them to take control of their device. Some cybercriminals disguise their software as games or apps, which can be particularly appealing to children.
* **Malicious Ads:** These advertisements are used to disseminate a wide range of unwanted messages or spam. Researchers from the University of Michigan and the C.S. Mott Children's Hospital recently examined one hundred thirty five applications aimed for children under the age of eight and discovered that several of them used questionable advertising techniques such as manipulation and shaming.
* **Identity Theft:** Cyber criminals are increasingly targeting children online in order to steal their identities and credit records. In fact, according to a Javelin Strategy & Research study, over one million children were victims of identity fraud in 2017, resulting in $2.6 billion in damages and $540 million in out-of-pocket costs for families.
* **Online Gaming:** According to Entertainment Software Association study, seventy percent of homes have at least one child who plays video games. According to Webroot, phishing schemes, malware, and harassment have grown routine in gaming groups as a result of so many children actively gaming.

**Safety Measures for Parents and Children**

Being a parents, here are five steps that we should start following with our child today:

* **Teach Passwords and Privacy:** Assist the child in creating strong passwords for all of their gadgets and online accounts. Teach children why strong passwords are vital, how to develop them, and why they should never be shared.
* **Monitor and Communicate:** Communicate what constitutes an acceptable, respectable (to themselves and others) online post, and spend as much time as possible in monitoring child's online behaviour.
* **Protect Identity and Location:** Disable photo geo-tagging on Android or i-Phone, and tell the child not to disclose any personal information online, such as his or her age, school, address, phone number, last name, or any other personally identifying information.
* **Use Secure Wi-Fi:** To limit outside access, make sure our home's wi-fi has encryption and a strong password, and only share the password with people we know and trust.
* **Utilize Parental Controls:** Many children receive their first tablet or internet-connected device before fully comprehending the potential they hold. To begin taking safeguards and monitoring their usage as soon as possible, use the built-in parental control options.

**Conclusion**

Cyber-attacks can affect anyone, including schools, colleges, universities, and other institutions. The reason behind, the education industry need to consider solid cybersecurity procedures in order to protect students, professors, and everyone else involved with the institution from hostile behaviour, as well as the school's bottom line and painstakingly-built brand name. Staff and students must be informed about cyber-attacks, online frauds, and phishing campaigns, and must be instructed on how to create strong password rules and enable multi-factor authentication (MFA). Institutions should also keep their software and networks up to date on a regular basis and keep numerous backups in different and secure locations, both online and offline.

It's also a good idea to keep an eye on logs for odd traffic and activity on websites and other applications on a regular basis. Using network firewalls, the institutions should block unauthorised IP addresses and disable port forwarding. They should monitor the internet in real time to discover and neutralise low-hanging dangers like misconfigured programmes, unsecured data, and leaked credentials, which cybercriminals use to launch large-scale attacks. Students, parents, instructors, and staff should use secure passwords and avoid clicking on questionable emails, messages, and links. They should also not download or install unverified apps.

**References**

Caulkins, B. D. (2016). [Cyber workforce development using a behavioural cybersecurity paradigm.](https://ieeexplore.ieee.org/document/7836614) *International Conference on Cyber Conflict* *1*(6). [doi](https://en.wikipedia.org/wiki/Doi_(identifier)):[10.1109/CYCONUS.2016.7836614](https://doi.org/10.1109%2FCYCONUS.2016.7836614).

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security, 73*, 519-544.

Janicke, H. (2019). Heart-is: A novel technique for evaluating human error-related information security incidents. *Computers & Security, 80*, 74- 89.

Katzan, J.H. (2016). Contemporary issues in cybersecurity. *Journal of Cybersecurity Research, 1*(1), 1-6.

Lestch, C. (2015). Cybersecurity in K-12 education: Schools face increased risk of cyber-attacks. Retrieved from http://fedscoop. com/cybersecurity-in-k-12-educationschoolsaround-the-country-face-risk-of-cyber-attacks on June 15, 2022.

Reeder, E. (2018). Three reasons for improving cybersecurity instruction and practice in schools. In Society for Information Technology & Teacher Education International Conference (pp. 1020-1025). Washington, DC. Association for the Advancement of Computing in Education (AACE).

Thomas, J. (2018). Individual cybersecurity: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management, 12*(3), 1-23.

Whitman, M. E., & Mattord, H. J. (2016). Principles of information security. (5th Ed). Boston, MA: Cengage Learning.

**Web References**

https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/

https://en.wikipedia.org/wiki/National\_Initiative\_for\_Cybersecurity\_Education

https://www.cybersecurityeducation.org/

https://www.indiatoday.in/education-today/featurephilia/story/importance-of-cybersecurity-in-the-education-sector-1770586-2021-02-18

https://terranovasecurity.com/cyber-security-and-going-back-to-school/