







# Online Education and Increasing Cyber Security Concerns During Covid-19 Pandemic

Shazia Shaikh , Nafisa Khan , Ayesha Sultana , and Nazneen Akhter<sup>(✉)</sup> 

Maulana Azad College of Arts, Science and Commerce, Aurangabad, Maharashtra, India  
shaziazshaikh20@gmail.com, getnazneen@gmail.com

**Abstract.** COVID-19 pandemic has hard hit not only global economy but also the education sector. The sudden shift to online education not only threw technological challenges but posed some serious privacy and security concerns as well. When online classes became the new normal for not only universities and high schools but even the primary schools, it turned out that most of them were not prepared for the new fully digital format. The students and institutions both lacked in technical resources in some cases while in most of the cases the educational institutions were not at all prepared for cyber-attacks, putting cyber security of all stake holders at increased risk.

In this study, we surveyed the cyber-attacks on the educational institutions during the covid-19 pandemic. Our study revealed that over 95% of IT infrastructures of the educational institutions were not able to protect themselves and the students from the cyber-attacks that crippled the education system in its entirety in some cases. We present a brief review of the cyber-attacks made on the education sector during covid-19 and the tools and technologies adopted and the types of attacks each tool faced. We also present the cyber security tools being utilized and we also propose some preventive suggestions as a primary safe guard.

**Keywords:** Cyber security in education · Types of cyber security attacks · Thermo graphic cameras · Physiological identification · Encryption · Multifactor Authentication

## 1 Introduction

The current pandemic has completely changed the perspective of education sector, with educational institutions remaining physically closed for more than a year up-till now. Online education came to the forefront globally and online classes became the new normal for not only universities and high schools but even the primary schools. This called for a complete paradigm shift forcing schools and colleges to entirely adapt to online meeting platforms like zoom and Microsoft teams in addition to already in use blended e-learning platforms like WebCT, Moodle and Blackboard [1]. Online learning has grown dramatically in recent years. They are large and dynamic with a variety of resource users. The data must then be protected in order to preserve its confidentiality, integrity and availability. Protection against data manipulation, fraudulent user authentication and privacy breaches are important security concerns in e-learning [2]. Due to

current global pandemic educational institutions across the globe closed their doors to physical live learning and shifting to online learning in their efforts to continue teaching and learning. It is essential to take into account cyber security and confidentiality before implementing alternatives to learning in the classroom [3]. Neglecting to consider cyber security and confidentiality until the end of the planning process and implementation or completely forgetting poses significant risks to the security and privacy of students and teachers [4].

## 2 Online Education and Cyber Security

Subsequently after the current pandemic forced the whole world into lockdown and the educational institutions in the urge to provide continuity in learning shifted to online mode, as expected most of them started experiencing rise in cyber security threats [5]. And institutions started to contemplate how they can enable all stakeholders with security and privacy along with undisrupted online experience. Recent report by Barracuda Networks [6] states that more than 1000 educational institutions were attacked just during the initial three months of lockdown. The researcher at the center said this after reviewing almost 3.5 million cyber-attacks on various sectors. Over the years, educational institutions have been lethargic to respond to cyber threats, thus leading them into key targets of cyber-attacks [7]. Educational institutions possess sensitive personal data of students, teachers and staff and which keeps growing with every academic year. And in some cases institutions also stores the payment details of parents as well. In most of the cases the IT department of the institutions cannot afford the highly- rated secure data centers and thus become vulnerable [8].

It was found that around 60% of the institutions faced phishing attacks [9] and around 33% faced account compromised just in 2020. Ransomware and other malware attacks contributed to 27% [10] while 49% of institutions were unaware of the infections for days. Hackers breached a server containing student and staff ID numbers, admissions details, and other academic records. In all, about 200,000 people were affected by the cyber-attack in February 2021 [11]. Simon Fraser University in British was one of the victims. In February 2020, Quebec's Minister of Education confirmed that hackers stole the personal information of 360,000 teachers and ex-teachers in Quebec [12]. According to a July 2020 report that states 54% of U.K. universities reported a data breach to a regulator, 46% of university staff didn't receive security training in the 12 months report says [5]. The Blackbaud hack [13] was first reported in the summer of 2020. It's an example of a massive data breach that crosses international lines. Nearly a dozen universities were affected by the attack, including the University of London and the Rhode Island School of Design. The university says it paid the ransom and released the stolen data in exchange for some of its donors' information.

## 3 Types of Attacks

Analyzing the most prevalent cyber-attack vectors offers insight into how educational institutions can effectively emphasize data security and safeguard their networks. Ransomware assaults, DDoS attacks, and phishing attacks are three of the main cyber-attacks against educational institutions.

### 3.1 Ransomware

According to a recent research, the education sector has just eclipsed healthcare and government as the field that suffers the most ransomware assaults, with 13% of educational institutions experiencing the infection [14]. In comparison, 5.9% of government organizations and 3.5 percent of healthcare providers fall under this category. Ransomware is a form of virus that encrypts the owner's files and demands a ransom in exchange for the decryption key once it has infected the system. As ransomware as a service acquire acceptance, these assaults are likely to gain much more traction. Ransomware attacks cause downtime and unforeseen expenditures that schools cannot afford, with the cost of ransomware mitigation estimated to surpass \$5 billion [15]. Schools, in particular, are frequently obliged to pay up since they cannot justify postponing the teaching of hundreds or thousands of children while they work to repair the system meticulously. Malicious files or URLs provided via emails are commonly used to spread ransomware.

### 3.2 Phishing

With 91 percent of cyber-attacks beginning with a phishing email, phishing scams are a common attack vector across business industries and have now expanded to education [16]. Phishing scams are most commonly sent by email, but they may also be sent over social media or SMS. Attackers will send an email that looks to come from a trusted source or from someone the victim knows, requesting them to provide sensitive information or enter their login credentials on a counterfeit website. Targets open 30% of phishing texts and twelve percent clicks on malicious attachments of phishing emails. After obtaining the desired information, hackers can exploit it for a variety of objectives, including credential stuffing on other websites, selling it on the dark web, and more. Scams using phishing can have a variety of outcomes and objectives. According to reports, hackers planned to exploit school districts as entry points into other government networks, including state voting systems, in addition to targeting personal data, showing the necessity of internal segmentation. In addition, the IRS recently issued a warning about a phishing fraud targeting school employees [17].

### 3.3 DDoS

At both K-12 and university levels, distributed denial of service (DDoS) assaults have grown commonplace [18]. DDoS attacks overburden network servers by flooding them with requests from tens of thousands of workstations, generally via a botnet. Eventually, the increased traffic brings the institution to a halt. DDoS is most commonly used by hackers to profit from. Therefore they attack businesses or organizations with which they compete or have a disagreement. As a result, DDoS attacks against schools are common, with numerous examples occurring at the K-12 and university levels. Since a DDoS as a service assaults can cost as low as \$5, this is a trend that will certainly continue [19].

## **4 Solutions that May be Adopted by Educational Institutions**

### **4.1 Auditing User Activity**

This is actually a regular practice of network monitoring team to audit the network traffic for strange and odd user behaviors. The educational institutions can adapt machine algorithms to classify legitimate network traffic from illegal one based on their activities. Audits can help locate unusual behavior in the network.

### **4.2 Encryption**

The logins and the authentications can be provided with high level of encryptions to prevent hijacking of username and password during transmissions. AES 256 is considered to be the hardest encryption so far, but theoretically even AES 128-bit has not been broken up till now [20].

### **4.3 Review of Access Rights (Attestation)**

Access rights are to be reviewed frequently to see if any unauthorized users have not gained access to sensitive data. Even authorized users need to be watched for unusual activity.

### **4.4 Multifactor Authentication**

This should be a very robust approach [21], if can be combined by multifactor authentication based on biometrics and/or on mobile device OTP to get access to the network. And in case of extremely sensitive data, physiological biometrics like HRV [22] or multispectral face recognition using thermo graphics camera can also be used [23].

### **4.5 User Training**

Human error was one of the major factors in compromising the network securities. Most of the phishing attacks are carried out on the untrained unaware users of the networks. Educational institutions should arrange for user training and make all the stakeholders aware of the cyber security corners and best practices while using the resources. Teachers and other employees at schools need to be regularly briefed on the latest security risks to know how to respond intelligently to data breaches, ransomware, and phishing attacks.

### **4.6 Data Classification**

This is the most essential part which the educational institutions should be very vigilant about. Institutions should be able to identify and classify their most sensitive data so that security and privacy of that data becomes priority of the institution and necessary security and privacy measures can be applied to the same.

#### **4.7 Cloud Backups**

To be safe from ransom ware attacks this is the most reliable policy, to keep the backups of the cloud data in premises. Though it can be cumbersome and may be redundant to maintain the duplicate copies of the data but very helpful at the time of attack.

#### **4.8 Remove Sensitive Data from the Cloud**

This policy can be adapted if the data classification has identified the sensitive data. And restricting access to such data should provide the necessary security against cyber-attacks.

#### **4.9 Enhanced Cloud Access Security**

The sensitive data on the cloud should not be accessible to unauthorized users, hence cloud access should be provided with enhanced security measures either multifactor authentication or encryption.

### **5 Conclusion**

Security awareness training is the key to addressing the fast-moving threat landscape of cyber-attacks, says security expert. Security awareness training will give the participants the heads-up on the methods that cyber criminals are using now and educate them on best practices to protect their information and systems. To protect your data, security awareness training needs to be at the forefront of your defense strategy. To prevent ransom ware secure email gateways should be in place for school districts and institutions to detect and block messages from fraudulent accounts. Firewalls should also be installed on the network's perimeter as well as within it. Malware such as ransomware may be detected and blocked by network perimeter defenses such as next-generation firewalls, while internal segmentation firewalls keep any breaches isolated. This is especially essential as ransomware distributed through worms, which do not require human input, is becoming increasingly common. Breach will occur as these attacks become increasingly prevalent. Schools must ensure that they have robust SIEM processes in place to detect intrusions immediately and mitigate the repercussions. These examples of cyber-attacks aimed at colleges and universities highlight the need of email security, internal network segmentation, and speedier incident detection and reaction times. DDoS assaults must be detected early in order to be mitigated. Next-generation firewalls and web application firewalls, particularly those with anti-botnet protection, can help fight against DDoS assaults that persist at the web application or network layer.

### **References**

1. Morze, Nataliia, and Eugenia Smyrnova-Trybulska. "Web-based community-supported online education during the COVID-19 pandemic." *International Journal of Web Based Communities* 17(1) (2021): 9–34.

2. Ball, Albert L., Michelle M. Ramim, and Yair Levy. "Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems." *Online Journal of Applied Knowledge Management* 3(1) (2015): 180–207.
3. Sarker, Iqbal H., et al. "Cybersecurity data science: an overview from machine learning perspective." *Journal of Big data* 7(1) (2020): 1–29.
4. Olsen, Rune Vålandsmyr, and SimenTokerud. Teachers' awareness, knowledge and practice of information security in school. MS thesis. University of Agder, 2020.
5. Lallie, Harjinder Singh, et al. "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & Security* 105 (2021): 102248.
6. Wickline, Ty. The Capabilities of Antivirus Software to Detect and Prevent Emerging Cyberthreats. Diss. Utica College, 2021.
7. Steingartner, William, DarkoGalinec, and AndrijaKozina. "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model." *Symmetry* 13(4) (2021): 597.
8. Ngwacho, Areba George. "COVID-19 pandemic impact on Kenyan education sector: Learner challenges and mitigations." *Journal of Research Innovation and Implications in Education* 4(2) (2020): 128–139.
9. Alkhalil, Zainab, et al. "Phishing Attacks: Recent Comprehensive Study and a New Anatomy." *Frontiers in Computer Science* 3 (2021): 6.
10. Ramesh, Gowtham, and Anjali Menen. "Automated dynamic approach for detecting ransomware using finite-state machine." *Decision Support Systems* 138 (2020): 113400.
11. Chatterjee, Dave. *Cybersecurity Readiness: A Holistic and High-Performance Approach*. SAGE Publications, 2021.
12. <https://montreal.ctvnews.ca/major-data-breach-personal-information-of-360-000-teachers-and-former-teachers-in-quebec-exposed-1.4822449>
13. Feng, Xiaohua, YunzhongFeng, and Edward SwarlatDawam. "Artificial Intelligence Cyber Security Strategy." 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCoM/CyberSciTech). IEEE, 2020.
14. Prasad, Ramjee, and VandanaRohokale. *Cyber Security: The Lifeline of Information and Communication Technology*. Springer International Publishing, 2020.
15. McLilly, Landon, and Yanzhen Qu. "Quantitatively Examining Service Requests of a Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses." 2020 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2020.
16. Alabdan, Rana. "Phishing attacks survey: types, vectors, and technical approaches." *Future Internet* 12(10) (2020): 168.
17. Farrell, Casie. *Phishing in the Financial Sector*. Diss. Utica College, 2020.
18. Robbins, Michael S. *Exploring the Impact of Information Security Awareness Training on Knowledge, Attitude, and Behavior: A K-12 Study*. Diss. Northcentral University, 2020.
19. Singh, Jagdeep, and Sunny Behal. "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions." *Computer Science Review* 37 (2020): 100279.
20. Smart, Nigel P., and Emmanuel Thomé. "History of Cryptographic Key Sizes★."
21. Fauzi, Muhammad Ali, and Bian Yang. "Audiouth: Multi-factor Authentication Based on Audio Signal." *Proceedings of the Future Technologies Conference*. Springer, Cham, 2020.

22. Akhter N., Tharewal S., Kale V., Bhalerao A., Kale K.V. (2016) Heart-Based Biometrics and Possible Use of Heart Rate Variability in Biometric Recognition Systems. In: Chaki R., Cortesi A., Saeed K., Chaki N. (eds) *Advanced Computing and Systems for Security. Advances in Intelligent Systems and Computing*, vol 395. Springer, New Delhi. [https://doi.org/10.1007/978-81-322-2650-5\\_2](https://doi.org/10.1007/978-81-322-2650-5_2)
23. Shaikh S., Gite H., Manza R.R., Kale K.V., Akhter N. (2016) Segmentation of Thermal Images Using Thresholding-Based Methods for Detection of Malignant Tumours. In: Corchado Rodriguez J., Mitra S., Thampi S., El-Alfy ES. (eds) *Intelligent Systems Technologies and Applications 2016. ISTA 2016. Advances in Intelligent Systems and Computing*, vol 530. Springer, Cham. [https://doi.org/10.1007/978-3-319-47952-1\\_11](https://doi.org/10.1007/978-3-319-47952-1_11)

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

