SECURING THE ONLINE LEARNING ENVIRONMENT: CYBERSECURITY CHALLENGES AND SOLUTIONS FOR THE EDUCATION SECTOR

by:
MELBOURNE L. SALONGA
Special Science Teacher I Limay Senior High School

Cybersecurity is the protection of networks, devices, and data from unauthorized or illegal access or use. It is especially important in the education sector, where sensitive information such as student and faculty data, academic records, and research findings are stored and transmitted online. Cybersecurity helps safeguard the privacy, integrity, and availability of these valuable assets, as well as the reputation and trust of educational institutions.

The education sector faces various cyber threats, such as phishing, ransomware, data breaches, and distributed denial-of-service (DDoS) attacks. These threats can have serious consequences, such as compromising personal information, disrupting online learning, extorting money, or damaging infrastructure. According to a Consortium for School Networking (CoSN) report, over 90% of cyberattacks today start with phishing, which exploits human emotion to trick victims into giving up sensitive information. Ransomware attacks, which encrypt data and demand payment for its release, cost victims up to $40,000 per hour, while data breaches can expose confidential information to malicious actors or the public.

The education sector needs to review its cybersecurity risks and improve its cyber resilience. This requires a proactive and methodical approach that involves assessing the current state of security, identifying vulnerabilities and gaps, implementing best practices and standards, and monitoring and evaluating the effectiveness of security measures. The Board Toolkit, developed by the Global Tech Council, is a useful resource that helps organizations adopt such an approach. It provides guidance on establishing a cybersecurity governance framework, developing a cybersecurity strategy and policy, managing cybersecurity incidents, and promoting a culture of cybersecurity awareness and education.

Cybersecurity is a shared responsibility that involves not only technical solutions but also human actions. All members of the education community, such as administrators, teachers, students, parents, and IT professionals, need to collaborate and cooperate to enhance cybersecurity. They can do this by following best practices, such as using strong passwords, updating software, and avoiding phishing emails. They can also raise awareness of cybersecurity risks and threats among their peers and colleagues. They can report any suspicious or malicious activities to the relevant authorities and seek help when needed. They can provide feedback and suggestions to improve the cybersecurity policies and procedures of their institutions. By doing so, they can create a safe and secure online learning environment for everyone.

References:

Global Tech Council. (n.d.). Why is cybersecurity important in the education sector? Retrieved from https://www.globaltechcouncil.org/cyber-security/why-is-cybersecurity-important-in-the-education-sector/

Berkeley Boot Camps. (2020, September 9). Cybersecurity in education: What teachers, parents and students should know. Retrieved from https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/

Hina, A., & Bashir, M. (2018). The importance of cybersecurity education in school. International Journal of Academic Research in Progressive Education and Development, 8(2), 205-212. Retrieved from https://www.researchgate.net/publication/340714158_The_Importance_of_Cybersecurity_Education_in_School