IMPORTANT PROBLEMS OF THE CONCEPT OF CYBER SECURITY IN THE EDUCATIONAL PROCESS

Abdusamatova Shahodat Khojiakbar's daughter
Informatics and information technology teacher at the academic lyceum named after Islam Karimov at the Almalyk branch of TDTU
phone: +998(93) 375 – 42 - 15 e-mail: abdusamatovashahodat@gmail.com,
Mannonov Asliddin Akbar's son
student of cyber security faculty of TATU named after Al Khorazimi, phone: +998(97) 960-03-02, e-mail: asliddinmannonov0980@gmail.com.

Abstract: *This article presents an analysis of the importance of the concept of cyber security in education and its current problems*

Keywords: *spam, cybercrime, phishing, malware, ransomware, social engineering, denial of service*

The accumulation of digital information has given rise to the cyber world and has penetrated into every sphere of our life, especially the sphere of education. The development of technologies has created the basis for increased efficiency and the creation of many new opportunities, but the deliberate use of these opportunities has also created some serious risks. Educational institutions can be exposed to cyber security threats mainly because of the number of devices they manage, the variety of operating systems and more. Currently, it is difficult to imagine the educational process without modern information technologies, therefore, safe access to the Internet and the safe storage of students, employees, teachers and other important information is an important issue, therefore, the role of cyber technologies in education is important.

The main types of cyber security threats in educational institutions include phishing, malware, ransomware, spam, social engineering and denial of service attacks. Cybercriminals are using these tools to target educational institutions for financial gain.

Phishing is the most common form of cyberattack used by cybercriminals to break into educational institutions' systems.

Phishing is a fraudulent email or website that aims to collect sensitive information such as passwords, credit card numbers and other personal information if the user falls into the trap.

Phishing emails often appear as official notices from a well-known company, asking users to update their personal or banking information by clicking on a link or downloading a document or attachment that infects the system with malware.

Another way phishers can try to get into your system is by installing malware on your computer. Malware is a program or file that can harm your system and steal your confidential information.

Ransomware is a form of malware that encrypts the files of a user's computer and demands a ransom in exchange for a decryption key to unlock their files.

Ransomware attacks are distributed through phishing emails and infected websites. After infecting your system, ransomware encrypts all your files and demands that you pay a certain amount of money to unlock them. Such programs do not destroy or harm user data, they simply block the possibility of using them, which increases the risk of financial loss.

Spam is another way cybercriminals get into your system by sending spam emails with malicious links or attachments.

Spam emails often look like official notices from an educational institution or company asking users to update their personal information by clicking on a link or downloading an attachment, which if they fall into the trap, infects their system with malware and viruses and eventually personal information may be at risk.

Spam emails are also used by cybercriminals to spread viruses and other forms of malware through infected files attached to spam emails.

Cyber threats come in many forms and are on the rise. Some of the cyber threats affecting the education sector include:

Secure wireless connections: The use of wireless connections is very common in today's world. However, many problems arise when there is a need to protect these wireless connections. Unsecured wireless connections can be easily compromised by hackers, which can lead to data theft and data corruption or theft.

Wireless routers: Many schools don't care about their wireless routers or they don't install any firewalls on their routers, making them vulnerable to cyber attacks from outside hackers or even from insiders tasked with managing the school's network infrastructure. It also leads to data breaches and data theft. Social Media: Social media has become very popular among students and teachers.

In conclusion, cyber threats pose the biggest threat to students (both personally and academically) in schools. These threats can also hinder schools' ability to educate students by limiting their ability to access digital learning. Schools especially need to improve their cyber security to be ready for the cyber security incidents that come with the digital age. The solution is to train staff to use (and establish) basic cyber security practices to secure all laptops and other internet-connected devices, change passwords regularly, and ensure that school network devices (open or otherwise) are not connected to external networks without proper precautions. We will be able to achieve this by providing training and regular monitoring of this process.

REFERENCES:

1. Decree of the President of the Republic of Uzbekistan "On approval of the national strategy of the Republic of Uzbekistan on human rights"

2. Kevin James “The Importance of Cyber Security in the Education Sector” August 5, 2022
3. "Cyber security against cybercrime" Abdurasul IMINOV, head of the Department of Information Technologies of the Ministry of Internal Affairs, lieutenant colonel
4. "Guide to security technologies and trends in 2022" e-guide