An Overview Of Recent Cyber Security Issues

Daniel Casper*

Department of Computer Engineering Technology, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Commentary

*For Correspondence:

Daniel Casper, Department of Computer Engineering Technology, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

E-mail: casperdan@gmail.com

ABOUT THE STUDY

Cyber security refers to the securing of computer systems and networks against data leakage, theft, or damage to their hardware, software, or electronic data, as well as disruption or misdirection of services. Due to the increased reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi, as well as the proliferation of "smart" gadgets such as smartphones, televisions, and the myriad devices that make up the Internet of things, the area has grown in importance. Due to its complexity, both in terms of political use and technology, cyber security is one of the most critical concerns in the modern world. Its main objective is to ensure the system's dependability, integrity, and data security. Cyberspace is rapidly expanding over the world today. With such rapid expansion in information availability, individuals with evil intent have more opportunities.

It is an urgent requirement, as is the act of safeguarding systems and technologies from anomalous behaviours. Maintaining the Integrity, Confidentiality, and Availability (ICA) of computing assets belonging to an organisation or connected to another company's network is what cyber security is all about. Because of the growth and increase in cyber risks, many researchers believe and support for educating the next generation about cyber-security ideas. Cyber-crime occurs as a result of a lack of cyber-security and client knowledge.

Since the advent of the Internet and the digital change that has occurred in recent years, the concept of cyber security has become a common topic in both our professional and personal life. For the last 50 years of technological advancement, cyber security and cyber threats have remained constant. Until the invention of the Internet in the 1970s and 1980s, computer security was primarily relegated to academics. With more connectivity,

computer viruses and network intrusions began to take off. The 2000s saw the institutionalisation of cyber risks and cyber security, following the rise of viruses in the 1990s. As a result, cyber security is a broad word that refers to the prevention of cyber assaults, data breaches, and risk management. The security architecture describes some security characteristics, such as security attacks, which are divided into two types: active and passive attacks, and security objectives. Cyber bullying, identity theft, digital devices, autonomous systems, Wireless Sensor Networks (WSN) and Wireless Body Area Networks (WBAN), and cyber terrorism are all examples of risks that might come from unexpected sources and directions. More complex cyber-crimes and criminal actions are obvious in today's society, which is targeted and exceedingly deadly. The major obstacle of any network connection is data security; as a result, several methods exist to address security concerns. In the section below, we'll look at the history of cryptography as well as encryption techniques. Spartans devised cryptography for secure data transmission between militants around 400 BCE. To encrypt their messages, they used a tool called Scytale. Previously, the data was encrypted *via* a substitution mechanism. It replaces each letter in plain text with a letter that is displaced by a number between 0 and 25. Only if the secret shift is known can the encrypted text be decrypted. For instance, if one knows the secret shift is two, the string "modern" will become "OQFtp" and may be deciphered.