



Abstract

The rapid development of information technology, digital communication, cloud computing, and interconnected computer systems has transformed the way individuals, organizations, and governments store, process, and exchange information. However, this increasing dependence on digital technologies has also created significant challenges for cybersecurity. Cyber threats such as malware, ransomware, phishing, identity theft, data breaches, social engineering, and unauthorized access are becoming more sophisticated and difficult to detect. The widespread use of mobile devices, Internet of Things (IoT) systems, artificial intelligence, and remote working environments has further expanded the potential attack surface. Organizations face additional challenges, including inadequate security awareness, outdated software, weak passwords, insufficient data protection, and shortages of skilled cybersecurity professionals. Protecting computer systems requires continuous monitoring, regular security updates, effective access controls, data encryption, and comprehensive backup and recovery mechanisms. Moreover, cybersecurity is not solely a technological issue; human behaviour and organizational policies play an equally important role in preventing cyber incidents. This paper examines the major challenges associated with cybersecurity and computer systems and highlights the importance of adopting proactive, multi-layered security strategies. It emphasizes the need for cybersecurity awareness, technological innovation, effective regulatory frameworks, and collaboration among individuals, organizations, and governments. Addressing these challenges is essential for ensuring the confidentiality, integrity, and availability of digital information and for building a secure and trustworthy digital environment.

Keywords: Cybersecurity, Computer Security, Cyber Threats, Data Protection, Malware, Ransomware, Phishing, Network Security, Privacy, Information Security, Digital Safety.

