

## **1.1 Lesson: What is Cybersecurity?**

Cybersecurity refers to the practices, technologies, and processes designed to safeguard computers, networks, programmes, and data from unauthorised access, attacks, damage, or theft. It encompasses a wide array of measures that are aimed at protecting electronic systems and sensitive information from cyber threats such as hacking attempts, malware infections, phishing scams, and data breaches.

The field of cybersecurity is critical in today's increasingly digital world where individuals and organisations rely heavily on technology. This reliance has made them vulnerable to a variety of cyber threats that can compromise personal privacy and undermine business operations. As a result, cybersecurity involves not only technical solutions but also policies and procedures that ensure the secure operation of information systems.

Key components of cybersecurity include risk assessment to identify vulnerabilities within an organisation's infrastructure; the implementation of firewalls and antivirus software; encryption techniques to protect sensitive data; intrusion detection systems which monitor networks for suspicious activity; employee training programmes aimed at raising awareness about security threats; as well as incident response strategies for managing any breaches or attacks that may occur.

Overall, effective cybersecurity is essential for maintaining trust among users while ensuring compliance with regulations governing data protection. As cyber threats evolve continually, so too must the strategies employed in cybersecurity to mitigate these risks effectively.