

Cyber Threats and Attack Vectors

Cyber threats are malicious attempts to disrupt, damage, or gain unauthorized access to digital systems, networks, or data. Attack vectors are the pathways or methods used by cybercriminals to exploit vulnerabilities and launch attacks. Common types of cyber threats include malware, ransomware, phishing, denial-of-service (DoS) attacks, advanced persistent threats (APTs), and insider threats. These threats target both individuals and organizations, often resulting in data theft, financial loss, and reputational harm. Attack vectors vary widely. Examples include malicious email attachments, infected websites, compromised software updates, weak or stolen passwords, unsecured Wi-Fi networks, and social engineering tactics. Each vector provides an entry point for attackers to exploit weaknesses in security systems. To defend against threats and attack vectors, organizations implement layered security measures such as intrusion detection systems, firewalls, endpoint protection, employee awareness training, and strong authentication practices. Understanding threats and attack vectors is essential for building effective cybersecurity strategies.