

3.1 Lesson: Types of Cybersecurity Threats (Malware, Phishing, Ransomware)

1. Malware

Malware, short for malicious software, is a broad category encompassing various harmful programmes designed to disrupt, damage, or gain unauthorised access to computer systems. Types of malware include viruses, worms, Trojans, spyware, adware, and rootkits. Each type operates differently; for instance, viruses attach themselves to legitimate files and spread when those files are shared. In contrast, worms can self-replicate and propagate across networks without user intervention. The primary aim of malware is often theft of sensitive information or disruption of services.

2. Phishing

Phishing is a deceptive attempt to obtain sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in electronic communications. This threat typically manifests through emails or messages that appear legitimate but contain malicious links or attachments. Victims may be prompted to enter their credentials on counterfeit websites that closely resemble the real ones. Phishing attacks can be highly sophisticated and are often tailored to target specific individuals or companies through techniques known as spear phishing.

3. Ransomware

Ransomware is a particularly insidious form of malware that encrypts the victim's data, rendering it inaccessible until a ransom is paid to the attacker. This type of cyber threat has gained notoriety in recent years due to high-profile breaches affecting both individuals and organisations alike. Ransomware attacks typically begin with social engineering tactics or vulnerabilities in software that allow attackers to deploy their malicious code. Once the ransomware takes hold of the victim's system, they are presented with a demand for payment—usually in cryptocurrency—alongside threats regarding data loss or public exposure if the ransom goes unpaid.

These three categories encompass significant dangers within the realm of cybersecurity threats today and highlight the importance of robust security measures and awareness among users and organisations alike.

