Malware

It is any software code or computer program intentionally written to harm a computer system or its users. Almost all modern cyberattacks involve some form of malware. These malicious programs can take many forms, from expensive and damaging ransomware to merely annoying adware.

What is it used for?

- To hold devices, data, or entire business networks hostage for financial gain.
- To gain unauthorized access to sensitive data or digital assets.
- To steal login credentials, credit card numbers, intellectual property, or other valuable information.
- To disrupt crucial systems that businesses and government agencies rely on.

Types

- Virus: A virus is malicious code that hides legitimate software to damage and distribute copies of itself.
- Ransomware: Ransomware locks a victim's devices or data and demands payment of a ransom, usually in the form of cryptocurrency, to unlock it.
- Cryptojackers: Take control of a device and use it to mine cryptocurrency, without the owner's knowledge.
- Fileless malware: Uses vulnerabilities in legitimate software programs such as web browsers and word processors to inject malicious code directly into a computer's memory.
- Worm: Self-replicating malware that can spread between applications and devices without human interaction.
- Trojan: Disguises itself as useful programs or hides inside legitimate software to trick users into installing it.
- Rootkits: Malware packages that allow hackers to gain privileged administrator-level access to a computer's operating system or other assets.
- Scareware: Scares users into downloading malware or passing sensitive information to a scammer. It usually appears as a sudden pop-up window with an urgent message that usually displays some kind of warning.
- Spyware: Hides on an infected computer, secretly collecting sensitive information and transmitting it to an attacker.