

Attacks and Their Effectiveness:

Phishing: Phishing is tricking people through digital messages to steal sensitive data or install malware.

Types:

- Business Email Compromise (BEC): Fake emails that look real to get money or info.
- Spear Phishing: Targets specific people or groups using trusted-looking emails.
- Whaling: Targets top executives for sensitive data.
- Vishing: Voice calls pretending to be trusted sources.
- Smishing: Fake text messages to steal information.

Malware

Malware is harmful software made to damage devices or steal data.

Types:

- Virus: Needs user action (like opening a file) to spread and damage data.
- Worm: Spreads automatically without user action.
- Ransomware: Locks data and demands payment to unlock it.
- Spyware: Secretly collects and sells your personal data.

Social Engineering

Social engineering tricks people to gain private access or information by exploiting trust.

Types:

- Social Media Phishing: Uses your public info from social media to attack.
- Watering Hole Attack: Infects a website often visited by a target group.
- USB Baiting: Leaves infected USBs for people to plug in.
- Physical Social Engineering: Pretends to be an employee or visitor to access secure places.

