1) Explain how phishing works and its different types.

Phishing is a type of cyberattack in which malicious actors attempt to deceive individuals or organizations into revealing sensitive information, such as login credentials, financial details, or personal information. Phishing attacks often involve the use of fraudulent emails, websites, or messages that appear legitimate but are designed to trick victims. Here's how phishing works and its different types:

1. Email Phishing:

- In email phishing, attackers send fraudulent emails that appear to come from trustworthy sources, such as banks, government agencies, or well-known companies.
- These emails typically contain urgent or alarming messages, such as warnings of account suspension or security breaches, to create a sense of urgency.
- Victims are often asked to click on links that lead to fake websites designed to capture their login credentials or personal information.
- Alternatively, email attachments may contain malware that infects the victim's device when opened.

2. Spear Phishing:

- Spear phishing is a targeted form of phishing in which attackers customize their messages to specific individuals or organizations.
- Attackers research their targets to make the emails seem highly credible and convincing.
- This type of phishing is often used to target employees of a company, senior executives, or individuals with access to valuable information.

3. Vishing (Voice Phishing):

- Vishing involves using phone calls to deceive victims. Attackers may impersonate trusted entities, such as banks or tech support, and request sensitive information or payment over the phone.
- Automated voice messages and interactive voice response (IVR) systems can also be used in vishing attacks.

4. Smishing (SMS Phishing):

- Smishing is similar to email phishing, but it occurs through text messages (SMS) or multimedia messages (MMS).
- Victims receive deceptive messages that instruct them to click on links or reply with sensitive information.
- These messages often claim that urgent action is required, creating a sense of urgency.

Phishing attacks are constantly evolving, and attackers use various tactics to exploit human psychology and technology vulnerabilities. To defend against phishing, individuals and organizations should stay vigilant, use security tools like email filters and antivirus software, and educate themselves and their employees about the signs of phishing attacks.