Phishing

1. Phishing attacks: Phishing is a type of social engineering attack where attackers attempt to trick victims into giving up sensitive information such as login credentials, credit card details, or other personal information through email, text messages, or fake websites.
   1. Deceptive Phishing: The most common type of phishing attack, where attackers send fraudulent emails, text messages, or social media messages to trick victims into providing personal information, such as login credentials, credit card details, or social security numbers.
   2. Spear Phishing: A targeted phishing attack that is directed towards a specific individual or organization. Attackers use personal information gathered from social media or other sources to create a personalized message that appears to be from a trusted source.
   3. Whaling: A type of spear phishing attack that is directed at high-level executives or individuals in an organization, with the aim of stealing sensitive information or gaining access to confidential data.
   4. Clone Phishing: A type of attack where attackers create a replica of a legitimate email or website, with the aim of stealing login credentials or personal information from the victims.
   5. Smishing: A type of phishing attack that is conducted through text messages, where attackers send a message with a link to a fake website or a malicious app.
   6. Vishing: A type of phishing attack that is conducted over the phone, where attackers impersonate a legitimate entity and use social engineering tactics to trick victims into revealing sensitive information.
2. Phishing attacks affecting casual internet users:
   1. Phishing attacks: All types of Phishing are similar to one another, and they are mostly used on careless users and organization executives, who don’t check the legitimacy of a website, email or message. They can lead to leaks of personal and confidential company information.