Salman Anwar (22-10391)

Zarek Asif (22-10582)

**Phishing Attack**

Phishing is the most common type of attack. It has many types but deceptive phishing is mostly used to put a threat to information security. In this ploy, attackers impersonate a legitimate company to steal people’s personal data or login credentials. Those emails use threats and a sense of urgency to scare users into doing what the attackers want. Techniques that are involved in this attack are:

1. **Legitimate links**
2. **Blend malicious and benign code**
3. **Redirects and shortened links**
4. **Modify website logos**
5. Personal Communication

**What we are going to do?**

We will be doing phishing type called (Deceptive Phishing) that can put an attack on users of a particular platform, we can afterward obtain sensitive information of users of those platforms.

**Steps Involved**

1. Planning. We will decide which business to target and determine how to get the e-mail addresses & login details of the users of that platform. We will use the same mass-mailing and address collection techniques as spammers.
2. Setup. Once we know which platform or website to spoof and who their victims are, we will host that spoofing web page on hosting sites by using their HTML scripts to make them online, deliver the message and collect the data. Most probably, it is going to involve e-mail addresses and a web page.
3. Attack. Will send a phony message that appears to be from a respective reputable source.
4. Collection. We will record the information victims enter into Web pages or popup windows.

**Outcomes**

Deceptive Phishing Attacks will trick victims into giving over credentials for all sorts of sensitive accounts, such as email, and corporate intranets.

Carrying out this attack involves duplicating the strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.