Phishing is a type of cyber-attack in which attackers attempt to deceive individuals into divulging sensitive information such as usernames, passwords, or financial details by posing as a trustworthy entity. This is typically done through fraudulent emails, messages, or websites that mimic legitimate ones. Here's an example of a phishing attack:

Example of Phishing:

- Email Spoofing: An attacker sends an email that appears to be from a well-known and trusted organization, such as a bank or an online service provider.

- Subject and Content: The email subject may convey urgency or a problem that requires immediate attention, creating a sense of panic. The content of the email often includes a call to action, such as updating account information or resolving a security issue.

- Fake Website Link: The email contains a link that, at first glance, appears to lead to the legitimate website of the trusted organization. However, the link actually directs the recipient to a fraudulent website controlled by the attacker.

- Imitation of Legitimate Site: The fake website closely mimics the appearance of the genuine site, including logos, colors, and page layouts. It may even have a similar web address, further deceiving the victim.