Phishing is a type of cyber-security attack and most common type of social engineering during which malicious actors send messages pretending to be a trusted person or entity. Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a mali-

How Phishing Works:

Phishers are using the social networks to collect informations and background about the victims and any sensitive data are related t them either these informations were relate to their personal life or relate to their work. And activities then use this information to create a reliable fake message. Victims will receive emails it look like as it come from a known company or organization these mails will attached with malicious or links to malicious

Attackers often set up fake websites, which appear to be owned by a trusted entity like

Common Phishing Techniques

Email Phishing:

Social Engineering: uses psychology to manipulate the targets of phishing attacks. A phisher may use deception, coercion, bribery, or other techniques to achieve their goal.

- **Typosquatting:** Phishers may use domains and URLs that look very similar to that of a legitimate, trusted domain. If the target isn't paying sufficient attention, then may believe that the link is legitimate.

Email Spoofing: is designed so that the display name of the email belongs to someone that the email recipient trusts. The sender field in an email is just data and is under the control of the sender. Phishers use this fact to make emails appear to come from trusted email accounts.

- **URL Shortening:** Link shorteners like bit.ly conceal the target destination of a URL. Phishers use this to trick a target into clicking on a link to a phishing page.

- **Malicious Redirects:** Redirects are designed to send a browser to another page if the original URL is unavailable, incorrect, or outdated. Malicious redirects can be used to send a user to a phishing page instead of a legitimate one.

- **Hidden Links:** Links can be hidden in seemingly harmless text or images. If a user accidentally clicks the hidden link, they are sent to a phishing page.

5 Types of Phishing Attacks

1. Email Phishing:

- Attackers send mass emails from fake domains that closely resemble real ones. These emails often create urgency to trick users into clicking malicious links, downloading infected files, or providing personal data.

2. Spear Phishing:

- Targeted emails aimed at specific individuals using personal information (e.g., name, job title) to increase credibility. The goal is to manipulate the victim into actions like transferring money.

3. Whaling:

- Phishing attacks directed at senior executives or privileged roles. These attacks are highly personalized and subtle, often using detailed information about the victim to craft convincing messages without relying on obvious tricks like fake links.

4. mishing and Vishing:

- Phishing via phone communication. Smishing involves fraudulent SMS messages, while vishing uses phone calls, often with attackers posing as credit card company representatives to steal personal information or money.

5. Angler Phishing:

- Fake social media accounts mimic legitimate organizations to deceive users into providing personal information or

Impact of Phishing Attacks

1. **Direct Financial Losses**: Phishing attacks cause significant financial damage by stealing credentials or sending fake invoices.

2-Damage to Reputation: Phishing compromises can severely damage an organization's reputation. Attackers may send malicious emails from compromised systems, eroding customer and partner trust. News of data breaches spreads quickly, making it difficult to repair public opinion and leading to long-lasting negative impacts.

Impact of Phishing Attacks

3-Loss of Customers:
Data breaches drive customers away.

4-Disruption of Operations:
Phishing attacks can disrupt operations by introducing malware or ransomware, leading to system outages and lost productivity.

5 Ways to Protect Your Organization from Phishing Attacks

.1- **Employee Awareness Training**:

Aware employees about the attacks and how protect the informations and sensitive and deploy the new detect and protect security tools .

2. Deploy Email Security Solutions

Modern email filtering solutions can protect against malware and other malicious payloads in email messages. Solutions can detect emails that contain malicious links, attachments, spam content, and language that could suggest a phishing attack.

Email security solutions automatically block and quarantine suspicious emails and use sandboxing technology to "detonate" emails to check if they contain malicious code.

3. Make Use of Endpoint Monitoring and Protection

The increasing use of cloud services and personal devices in the workplace has introduced many new endpoints that may not be fully protected. Security teams must assume that some endpoints will be breached by endpoint attacks. it is essential to monitor endpoints for security threats and implement rapid remediation and response on compromised devices.

4. Conduct Phishing Attack Tests

Simulated phishing attack testing can help security teams evaluate the effectiveness of security awareness training programs and help end users better understand attacks. Even if your employees are good at finding suspicious messages, they should be tested regularly to mimic real phishing attacks.

The threat landscape continues to evolve, and cyberattack simulations must also evolve.

5. Limit User Access to High-Value Systems and Data

Most phishing methods are designed to trick human operators, and privileged user accounts are attractive targets for cybercriminals. Restricting access to systems and data can help protect sensitive data from leakage. Use the principle of least privilege and only give access to users who absolutely need it.