---------- PHISHING ATTACK ----------

How Phishing Links Are Generated:

1. **Domain Spoofing –** Attackers register fake domains resembling legitimate websites (e.g., "paypa1.com" instead of "paypal.com").
2. **URL Shorteners –** Links are masked using services like bit.ly or tinyurl to hide malicious intent.
3. **Homograph Attacks –** Cybercriminals use lookalike characters (e.g., “amazon.com” with a Cyrillic ‘a’ instead of a Latin ‘a’).
4. **Compromised Websites –** Hackers inject phishing pages into legitimate but vulnerable websites.
5. **Malicious Attachments** – Links inside email attachments redirect users to phishing pages.

How Phishing Links Are Sent to Targeted Victims:

Cybercriminals use various methods to distribute phishing links to their targets:

1. **Email Phishing –** Fake emails pretending to be from trusted sources (banks, social media, companies) contain phishing links that lead to fake login pages**.**
2. **SMS Phishing (Smishing) –** Attackers send phishing links via text messages, often impersonating banks, delivery services, or government agencies.
3. **Social Media & Messaging Apps** – Phishing links are sent through Facebook, WhatsApp, Telegram, or Instagram, often disguised as giveaways, fake job offers, or urgent security alerts.
4. **Malicious Advertisements (Malvertising) –** Fraudulent online ads lead users to phishing websites when clicked.

5. **Fake Websites & Pop-ups –** Attackers create fake websites mimicking legitimate ones and spread the link through forums, ads, or search engine manipulation.
6. **QR Code Phishing (Quishing) –** Attackers generate malicious QR codes that, when scanned, direct users to phishing sites.
7. **Voice Phishing (Vishing) with Follow-up Links –** Scammers call victims pretending to be from banks or support teams and send phishing links via email or SMS during the call.

How to Avoid Phishing Links:

1. Check the URL Carefully

- Look for misspellings or extra characters in domain names (e.g., "faceb00k.com" instead of "facebook.com").
- Ensure the URL starts with "https://", as secure websites use SSL encryption.

2. Hover Before Clicking

- Hover your mouse over a link (without clicking) to preview the actual destination.
- If the link doesn’t match the displayed text or looks suspicious, don’t click!

3. Be Wary of Shortened Links

- Scammers use URL shorteners like bit.ly, tinyurl to hide malicious destinations.
- Use a link expander tool (like CheckShortURL or Unshorten.It) to reveal the full URL before clicking.

4. Watch for Urgency & Threats

- Phishing emails often create urgency like "Your account will be locked in 24 hours!"
- If a message pressures you to act fast, verify it by visiting the official website directly.

5. Avoid Clicking Links in Unsolicited Emails/SMS

- If you get a message from a bank, company, or government agency asking you to click a link, verify it directly on their official website.
- Never enter your login credentials from a link in an email or text.

6. Use Email & Browser Security Features

- Enable phishing protection in your browser (Chrome, Firefox, Edge).

  Use email security tools like Spam filters and Multi-Factor Authentication (MFA).

7. Scan Links Before Clicking

- Use tools like VirusTotal (virustotal.com) or Google Safe Browsing (transparencyreport.google.com/safe-browsing/search) to check if a URL is safe.

How to Stay Safe:

- ✓ Don’t trust unsolicited emails/SMS with links.
- ✓ Verify links before clicking (hover over them on a desktop).
- ✓ Use official websites instead of clicking links from messages.
- ✓ Enable spam filters and phishing protection in browsers.
- ✓ Check links with security tools like VirusTotal or Google Safe Browsing