The other name for link manipulation is **Phishing** or you can say link manipulation is type of phishing attack done generally to mislead the user to a replica website or a "look-a-like" of some well-known site. The main trick used in this kind of phishing is use of sub-domains. These are the technicalities which are not acquainted to Non-I.T users and hence they are the major targets of the black hats.

The Process:

Link manipulation is the method in which the phisher sends a link to a website. When the victim clicks on the misleading link, it opens up the phisher's look-a-like website instead of the website mentioned in the link. And when the victim provide there his/her valuable information like user name, password and bank details, the information is sent back to the attacker and the page is redirected to original website showing an error message. One of the anti-phishing trick used to avoid link manipulation is to move the mouse over the link to view the real address. There are a lot of phishing techniques, below are some popular phishing techniques...

- **DECEPTIVE LINK MANIPULATION:**

Deceptive link manipulation is an attack by which attackers fake a legitimate company. Then try to steal people's sensitive information or login details. Those emails commonly use threats and a sense of urgency to panic users into doing the attackers' bidding.

For an example, PayPal fraudsters might send out an attack email that instructs them to click on a link in order to resolve a problem with their account. In reality, the link leads to a replica PayPal login page that gathers a user's login credentials and sends them to the attackers.

- **SPEAR LINK MANIPULATION:**

Not all phishing attacks lack personalization – some use it rather heavily.

In this type of link manipulation , the attackers customize the attack emails with the target's name, designation, company, phone number and other information in an effort to trick the victim into believing that they have a connection with the sender.

The objective is the same as deceptive link manipulation, here the victim clicks on a fake URL or email attachment, so that they will give up their personal data. Spear link manipulation is generally common on social platforms like LinkedIn, where attackers can use different sources of information to craft a targeted attack email.

- **SESSION HIJACKING:**

In session hijacking, the attacker exploits the web session control mechanism to take information from the victim. A simple session hacking technique is known as session

sniffing, here the attacker can use a sniffer to interrupt significant information so that he or she can enter the Web server illegally.

- **CONTENT INJECTION:**

Content injection is the method where the attacker changes a portion of the content on the page of a trustworthy website. This is done to mislead the user to go to a page outside the genuine website where the user is then asked to enter important information.

- **DROPBOX LINK MANIPULATION :**

While some hackers no longer bait their targets, others have customized their attack emails according to a specific company or service.

For example, take Dropbox. Millions of people use Dropbox each day to back up, access and share their files. It's no surprise, therefore, that attackers would attempt to capitalize on the platform's reputation by targeting users with phishing emails.

One attack operation, for example, tried to trap users into entering their login authorizations on a replica Dropbox sign-in page hosted on Dropbox itself.

- **WHALE LINK MANIPULATION:**

Phishers can target anybody in an organization, even top administrators. That's the logic behind a "whaling" attack, where scammers attempt to spear an executive and steal their login authorizations.

In occasion their attack gets successful, fraudsters can choose to operate CEO fraud, the second stage of a business email compromise (BEC) fraud where attackers imitate an executive and misuse that individual's email to approve fraudulent wire transfers to a financial institution of their choice.

Whaling attacks work because administrators often don't take part in security awareness training with their employees. To counter that threat, as well as the danger of CEO fraud, all company employees – including administrators – should go through ongoing security awareness training.

- **PHARMING:**

As users become savvier to traditional phishing attacks, some fraudsters are leaving the idea of "baiting" their victims completely. Instead, they are resorting to pharming – a type of attack which stalks from domain name system (DNS) cache poisoning.

The Internet's naming system uses DNS servers to translate alphabetical website names, such as "www.microsoft.com," to numerical IP addresses used for finding computer services and devices.

Under a DNS cache poisoning attack, an attacker targets a DNS server and changes the IP address linked with an alphabetical website name. That means an attacker can send users to a malicious website of their choice even if the victims entered in the accurate website name.

Precautions:

- Be guarded of emails from financial institutions or other organizations that ask you to provide personal data online. Reliable firms never ask for information in this way.
- Look carefully for clues to fake emails like a lack of personal greetings and spelling or grammatical mistakes.
- Verify a telephone number before calling it – if someone left you a message or sent an email appealing to be from your financial institution, make sure you check that the number is the one provided on the credit card or your bank statement.
- Check the basis of information from incoming mail.
- Never ever go to Your Bank's Website by Clicking on Links Contained within Emails.
- Improve the security of your computer.
- Enter your personal data in secure websites only, the URL must begin with 'https://' and your browser should show an icon of a closed lock and 'https://' is in green color.

"Have the Least Doubt, Do Not Risk It"