Hello Everyone! In this exercise, you will learn what are phishing attacks & how to prevent ourselves from these attacks?

What is Phishing Attack ?

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

How Does a Phishing Attack Work?

A phishing attack is usually a part of a large campaign, aiming to capture as many victims as possible in a big sample space of targets. Starting from its place of origin to the successful retrieval of credentials, a phishing attack consists of four independent phases that need to be executed. Let us learn more about each individual phase in detail, as denoted in the image below.

Phase 1: A malicious hacker sends an email or a message to the target, acting as a reputed source. More often than not, it asks the target to follow a third-party link for a security inspection or a simple feature update.

Phase 2: The target thinks the email came from the mentioned sender, be it a bank or a company, and follows the malicious link to a counterfeit web page designed to look as similar as possible to an authentic website.

Phase 3: On the fake website, the user is asked to submit some private information, like account credentials for a specific website. Once the details are submitted, all the information is sent to the hacker who designed the website and malicious email.

Phase 4: On receiving the account credentials, the hacker is free to use them by logging in or selling consequent information retrieved on the internet to the highest bidder.

In this exercise, you will learn how hackers are targeting people and making them victim of phishing attack.
Here are some examples of harmful Phishing Links:

- www.gmai1.com
- www.icici6ank.com
- www.bank0findia.com
- www.yah00.com

Here are some of the attack indicators, if your device has been targeted using Phishing Attack You may see changes in access privileges, Hacker can add, read, delete or modify data files in victim machine, turn on and off configurations and modify services. If you suspect that your device has been compromised by Phishing attack, it's essential to take immediate action to secure your device. This may involve

- Disconnect your device from the internet and any network it is linked to. This'll reduce the risk of the malware spreading through your system.
- Change your credentials.
- Scan your System for any Malware or Virus.
- Create a Backup of your Important data.

After successful execution of Phishing attack on target device a lot of malicious folders and files may be created on

the victim machine and a lot of cmd tabs may also get open automatically which indicates that your machine is compromised, and hacker has full access to it.
In this Exercise, Malicious URL will be created by hacker and once victim will click that URL his device will be compromised.

Some of prevention tips from such type of attacks are:

- Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. Emails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
- Verify the sender by checking their email address
- Check the link, before you click — make sure the links start with https:// and not http://
- Do not rush or panic react — scammers use this in order to pressure you into clicking links or opening attachments.
- If you gave sensitive information, don’t panic — reset your credentials on sites you've used them. Change your passwords and contact your bank immediately.
- Report all scams.

Thank you.