Recognizing and Avoiding Phishing Attacks

"Phishing" is a technique of misleading people to divulge their sensitive information such as their usernames, passwords, credit card numbers.

In fact, Phishers apply "social engineering" techniques to deceive their victims, and exploit the vulnerabilities of the system.

"The word phishing originally comes from the analogy that early Internet criminals used emails to "phish" for passwords and financial data from a sea of Internet users."

Phishing attacks can trick you into giving up your passwords or trick you into installing malware on your system.

In order to prevent Phishing attacks, it is vital to comprehend their behavior first, so this guide will help you to identify phishing attacks when you see them and how to defend against them.

Popular Phishing attacks are:

- A malicious email which pretends it is from a legitimate company but it contains some links which are from the attacker website.

- A fake website with similar content as the legitimate website.

- A malicious message which guides the victim to a website which has a vulnerability such as "XSS".

- An attacker fools the victim to setup a malware. This program redirects the important websites, such as "PayPal.com", to the attacker website to steal user information via the web browsing.

Tips to Avoid Phishing Scams

- Don’t trust unsolicited email.
- Treat email attachments with caution.
- Don’t click links in email messages.
- Install antivirus software and keep it up to date.
- Install a personal firewall and keep it up to date.
- Beware of keywords like “verify,” account process in the site name.
- Secure the websites to have no vulnerability such as XSS.

By Juravlea Nicolae