ACROPOLIS INSTITUTE OF TECHNOLOGY AND RESEARCH INDORE

Evolution Of Internship
(Phishing)

Submitted To:-

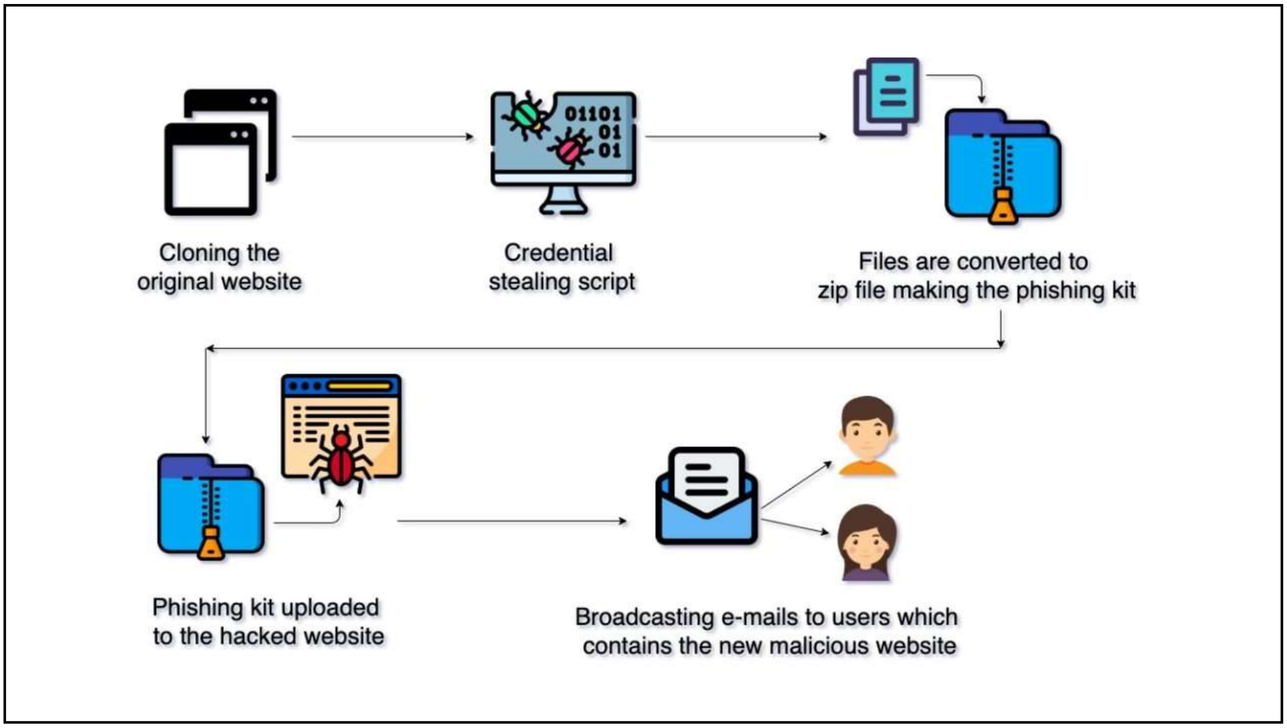
Prof. Nidhi Nigam

Submitted By:-
Nilesh Panchal
0827CI201121

What is Phishing?

Phishing is an online scam where criminals send alluring emails to the organization, user, and more to collect sensitive information. Mostly, this happens through a link sent by an unknown email domain. Clicking the links contained in such emails can put all your data is at risk. These emails can also lead to monetary losses. The intentions can vary from one phishing mail to another, but one thing is guaranteed i.e loss.

It has seen that most of the time, people aren't even aware that they are being targeted by an phishing attack. Therefore, it is important to know the various kinds of phishing attacks targeting many people every day.


01101
01
01
Cloning the original website
Credential stealing script
Files are converted to zip file making the phishing kit
Phishing kit uploaded to the hacked website
Broadcasting e-mails to users which contains the new malicious website

Types Of Phishing

Common Email Phishing: In the form of the most widely known email phishing, this attack attempts to steal confidential information through emails making them appear from valid sources.

Malware Phishing: In this scenario, the attacker's goal is to make you click on the link and download the infected attachment. This attachment further installs malware files to your system to make it compromised. This is currently the most widespread form of phishing attacks.

Spear Phishing: In this type of phishing, the attacker targets a group of people instead of individuals. The communication generally varies so that it appears to be coming from an authentic source. Spear phishing is generally the first step to break a company's security system and make way for further attacks.

SEO Phishing: In this type of attack, Cybercriminals build a fake website and rank them on search engines to collect personal information. They generally target common keywords for ranking, or sometimes also run advertisements to boost the campaign.

How to Prevent Phishing Attacks?

There are few simple and workable tips to not get trap in any phishing activity. See the below key points.
Please **check the "from" address of the email**. If it says from American Bank or Apple or an unknown external domain, it could be an online scam.

The mouse hover on the link in the suspicious email reveals the correct address. You can also check URLs using tools such as Virus total and Google Safe Browsing.

Use Antivirus software to keep your system clean and updated. Also, enable the firewall and other security settings to block malicious attacks.

Develop a habit of using a strong and unique password for your online accounts. This reduces the chances of getting your profile hacked.

Never provide your personal, financial, or any other sort of information over the email unless you have verified everything about the domain.

Conclusion

Phishing is but a modern twist to any number of age-old ploys to trick people into giving up information that can be used against them. From eavesdropping to mail tampering, criminals have always sought to steal information as a precursor to launching other exploits.

As it has always been, each individual must shoulder the responsibility to protect themselves from trickery and deception. There are software tools, such as spam filters and antivirus software, that can help, but in the end, we must all be ever-diligent and even a little suspicious of email and SMS communications.