**Understanding Spear Phishing**

Spear Phishing is a kind of cybercrime activity that is achieved by targeting systems and individuals inside the organization's premises. Some of the most notorious cyber crimes in recent history — such as the attacks on major banks, media companies, and even security firms started with just one person clicking on a fraudulent email. Spear phishing is becoming popular due to its high demand among attackers. The defense mechanism for cyber attacks does not detect this easily and hence is one of the primary favorites of the attackers.

The term “spoofed email” refers to an email that looks like it came from a legitimate source,

but is sent by someone who has been compromised (or infiltrated) into an organization.

To be successful, a spear phishing attack must have two components:

A malicious payload contains code that can be executed when the user opens the email and an attacker’s credentials, which allow them to gain access to the organization.

**Example of Spear Phishing**

To understand how these components work, given below are some examples.

**Example 1: A fake bank account scam**

A typical example of a real-world banking fraud where a hacker gains access to the organization’s internal systems through a stolen password. This type of attack is called ‘password sniffing’, and involves sending out a fake login request to the organization’s internal system using a stolen password. Once the victim clicks on the link, they are taken to a page that asks them to enter their username and password. If one doesn’t remember the password, then one will be asked to provide another one. After entering their username and password, the attacker sends them back to the original page asking them to click on a link that says “confirm your account”. When they do, the attacker takes control of the organization’s internal systems and deletes all data stored there. In addition, the attacker also deletes any files that were created during the process.

**Example 2: A fake credit card scam**

This is a typical example of real-world credit card fraud through a stolen credit card number. This type of attack is called ‘credit card sniffing’, and involves sending out a fake credit card request to the organization’s internal system using a stolen credit card number. Once the victim clicks on the link, they are taken to a page that asks them to enter their name, address, and other personal information. After this, the attacker takes control of your organization’s internal systems and deletes all data stored there. In addition, the attacker also deletes any files that were created during the process.

**How to prevent this?**

Spear phishing is a major problem in the cyber security domain and needs critical attention. There are various methods adopted to prevent this malicious activity to tamper with the organization's data.Given below are some of them.

1. Unknown emails that require urgent attention should not be clicked without verifying the source of the e-mail and the sender. Tools that detect unknown and suspected e-mails must be used.

2. Employees should be well educated on the basic methodologies to solve the different types of phishing attacks. Additionally, they also are compatible with the varied number of ways in which an attacker can attack an organization using phishing means like different types of social engineering tactics, CEO fraud, etc.

3. Downloading attachments from any unknown source must not be incorporated as phishing attacks generally happen via. different unknown sources.

4. Checking must be done frequently to check for the presence of malicious emails which generally ask individuals to change or reset the password.

5. Malicious activities that involve DKIM (Domain Key Identified Mail), and SPF(Sender Policy Framework) must be searched for.

**References:**

1.<https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/>

2.<https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing>

3.<https://www.kaspersky.co.in/resource-center/definitions/spear-phishing>

4.<https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing>

5.<https://www.techtarget.com/searchsecurity/definition/spear-phishing>

6.<https://www.imperva.com/learn/application-security/spear-phishing/>

7.<https://terranovasecurity.com/what-is-spear-phishing/>