What is it?

Phishing is a form of cybercrime in which an opponent mimics a real person or institution and shows himself or herself as an agent or entity by e-mail or otherwise. In this type of cyberattack, an attacker sends malicious links or phishing attachments that can perform various functions, including collecting information about a victim or account. These messages are harmful to victims in terms of loss of money and identity theft.

Phishing is defined as the fraudulent collection of confidential data by recipients and the misuse of it. In general, personal information, such as your credit card number or password, are required. When users visit this site, they are asked to provide personal information that is further sent to the attacker.

Phishing is a widespread form of cyberattack from which everyone must learn to protect themselves. There are various ways in which the attackers acquire the needed information for the fraudulent act. In some cases, the malware is downloaded directly to the victim’s computer and the scammers benefit from owning their credit card or other personal information.

Frequently, it is the case that an organization is posing as a target and not a single person. In such situation, emails are being sent to employees to obtain credentials or other confidential information necessary for an advanced attack. Cyberattacks such as Advanced Persistent Threats(APT) and ransomware often start with phishing.

*Getting into the mind of the attacker*

In order for a phishing attempt to be successful, the email that is being sent out needs to seem trustworthy and important for the victim. Therefore, attackers often use social networks to find out as much information as possible about their victim’s interests, social environments, personal and work history and so on. After gathering this information, they are capable of creating the perfect personalized email that would be likely to deceive a person.

How to detect it

Apart from the fact that we should always be vigilant and question any unexpected email, especially when asked to download a program/software/file or to update log in information of specific accounts, one can also identify a malicious email by closely inspecting it, since spelling mistakes within its content or even URL are common.

Protection measures

The first step one can take towards protecting themselves against such attacks is becoming aware of what it implies and how to identify one. There are, of course, methods such as using a network gateway email filter which can capture and reduce the number of phishing emails.