Cyberlitica
Enterprise Threat Intelligence

Phishing is a kind of social engineering attack that are meant to steal user data, that includes credit card numbers and login credentials. This is done by impersonating as a trusted organization, deceives the victim to open the email, IMs or SMSs which further installs deadly malware into the system or locks the system to demand a ransom to unlock the system or disclose confidential information.

How to Identify Phishing Attacks?

Phishing attacks are generally prompted through emails, however, there are ways to differentiate legitimate emails from suspicious.

It is vital to train employees of any organization on how to identify malicious emails to ensure data loss prevention. Data leaks often occur when employees are not equipped with the right amount security awareness on how to protect company's data.

Following are some of the signs and symptoms to understand that the email is a phishing attempt and not a legitimate one

- If you find any generic greetings and if the email doesn't address your actual name to greet you. This is certainly a phish attempt that are launched in bulk
- When emails from suspicious sources requests you to share personal information are most likely to be phishing emails as authorized companies will never ask for personal information through emails.
- Email contents that has a sense of urgency and demands a quick response can be a source of phishing.

- Emails with hoaxed links which when clicked redirects the user to malicious websites. Hover over any such suspicious links to check for its authenticity. Check if it has HTTPS in the URL as 'S' stands for Security and can be sure the website is encrypted.

- **Types of Phishing Attacks?**

Deceptive Phishing – This is a type of phishing, where the attacker impersonates a genuine company in order to steal confidential data.

Spear Phishing – This type of phishing email is customized with the victim's name, company, phone number, position and any other personal information to deceive the user and convince that they are genuine.

CEO Fraud – Phishers implement the use of an email address with the name of an higher authority to demand payments within the company.

Pharming – Hackers hijack the domain name of a website and use it to redirect the users to a malware site and impose an attack.