Phishing Attacks: A threat to the Global Organization

Technological evolution and the wide use of Internet in the day-to-day business and social life besides providing a fast and easy method of electronic communication has also left each and every internet user open to security threats, frauds through phishing attacks. The attacks are ways and means to extract information, usernames and passwords for unsuspecting public, which are later, used for frauds and security breaches.

Fraudsters who masquerade as genuine entity and claim to be from popular social web sites, auction sites with online payment gateways and IT administrators carry out Phishing attacks. Though the users are mostly tech-savvy group of people, phishing attackers exploits the poor usability of the interfaces and web security tools. Hence, the global organizations with technology as their lifeline need to take expert advices from the leaders in the field of IT security and protection and equip their corporate network and applications with anti phishing tools and other phishing protection measures. The first recorded phishing attack was in 1996. Today, there are a number of phishing techniques prevalent on the World Wide Web. These are –

- Spear phishing or enterprise spear phishing that are targeted phishing attacks
- Cloned phishing
- Whaling- targeted at high profile business executives
- Link Manipulation
- Filter evasion,
- Phone phishing
- Website forgery
- Tabnabbing and Evil twins.

Whatever be the mode of phishing, these attacks causes serious damages from access of denial of the electronic communication mails financial losses to the corporate sectors well as individuals totalling to millions of dollars. With the rising need for phishing protection measures, enterprises have developed a number of legislative and technology based anti phishing tools to combat phishing attacks. The Internet browsers use anti phishing software, which integrates with web browsers and email clients to identify the phishing content in websites and email.
To combat the challenge posed by the **phishing attacks**, the leaders in the field of information risk management and security services have designed and developed solutions to protect the vulnerable and difficult areas such as the people and process. With the help of an automated tool installed in the organization network a **simulated phishing attack** on the target audience of the organization is activated. This facilitates the authorities to understand and analyze the social behaviour of these target audience during the attack. With the statistics generated, these organizations then can work out measures for security awareness, identify data leakage and prevent data loss.