**What is Spy-Phishing?**

Spy-Phishing is a variant of simple phishing, and refers to an attack that makes use of other threats such as spyware and Trojan, downloaded into a system when a user clicks a phishing link. It is a malware that intends to “spy” on the user’s information, including their identity and financial credentials; hence the name “spy-phishing”. This information is then sent to the creator of the spy-phishing message.

Spy-Phishing tends to be dangerous not only for individuals but also for large organizations, because of the strong potential of Trojans to be used in industrial espionage. Though banking and other financial information is the main target of spy-phishing messages, they can also be employed for spying on business and proprietary information. Spy-Phishing is a blend of threats that makes use of both phishing and spyware components. It utilizes a number of techniques and exploits to download and then install spyware applications into a user’s system, and then makes use of phishing techniques to make a user visit a targeted URL. As soon as this is done, the malicious third party receives the information it requires. Spyware applications often prompt and trick a user into downloading extra spyware applications, in order to develop a stronger foothold.

Spy-phishing has gained popularity only recently, and the reason may be attributed to the fact that malware designers are now more interested in financial gain; as opposed to their previous generations who did so only for bragging among peers. Successful spyware can be used for stealing credit card numbers, bank account details, passwords, etc.; or even for larger gains such as selling enhanced bot networks to other individuals or malicious groups.

**Now let us closely understand the threats that together blend into a spy-phishing attack.**

**Spyware.** A software designed to install itself secretly on a computer and run in background. Once installed, it logs personal information of the user without their knowledge. Most of the times, spywares are designed to steal information such as credit card numbers, passwords, banking credentials, social security numbers, etc.

**Phishing.** Though intended to achieve the same purpose, phishing works by inviting a user to visit a fake website or click a malicious link, by posing as a reliable and legal entity.

**Backdoor Trojan.** Malware that carries out unauthorized and unexpected actions and also allows remote systems to have access on user systems.

**How does Spy-Phishing Work?**

A spy-phishing attack can better be explained in three steps or phases.

1. A phishing email is sent to trick the user. The email is either seeded with a Trojan or has a link for downloading the Trojan or spyware.
2. The author opens the link and Trojan is downloaded into the system either manually or through an exploited vulnerability.
3. The Trojan/spyware monitors and reports the user activity and sends login or other confidential data to the malicious user as soon as it detects user access to the target page.

Consider, for example, that a phisher sends spam message to a large number of users on behalf of a bank, hoping that some of the recipients will actually be the customers of the bank and will respond to the email i.e. be lured into visiting the phishing site. The site will have Trojans already residing in it and upon being visited by a user, they will utilize browser, html and other vulnerabilities to get installed on the system.

Another technique would be to directly attach the Trojan to the initial email in the form of pictures, account details or any other content of interest to the user. The advantage of using this technique is that it bypasses the requirement of a phishing site and avoids any downsides associated with them.

Going back to the example, upon visiting the phishing site or the forged website, the user may enter the credentials directly, causing immediate occurrence of theft. However, if the user does not enter the credentials, the Trojan that has been downloaded and installed will now monitor the user’s system continuously and sends the credentials to the attacker as soon as the user visits the legitimate banking site.

So what do we learn from this? Never underestimate the deceptive capabilities of malicious users and never think that phishing sites are easier to recognize. As cyber criminals are becoming more sophisticated in their attacks, they are now adopting all means of tools and technology to successfully deceive users. Phishing sites look as legitimate as the real ones, with the real logo, same web content, and even same interface, to make it look as genuine as possible.

**Why is it gaining popularity?**

Though spy-phishing is more complex to conduct as compared to traditional phishing, its higher probability of success is the prime reason why it is gaining probability and momentum in recent times. The use of Trojans and spyware enables the attacker to use it beyond the short lived life span of phishing websites, as they stay active on the systems for as long as they remain installed.

The distinguishing factor of spy-phishing is the flexibility it provides to the attacker. They can spam a spy-phishing message to thousands of users or a small group of people within an organization; they can attach a Trojan directly to an email or get it installed on the user’s system by making them visit a website; the Trojan can be used for targeting a specific site or a number of sites at the same time; most important of all, due to availability of a large number of malicious code freely and easily available over the internet, it gives the attacker enough flexibility to mix and match different modules and create new threats.

**Who is more at risk?**

Traditional phishing scams are mostly directed towards individuals and customers but when it comes to spy-phishing, it has a greater potential of successfully targeting small and large corporations for the purpose of corporate espionage. The stealth property of Trojans and spyware make spy-phishing a long lasting threat to corporate information and deem it more dangerous for corporations as compared to individuals. What makes spy-phishing powerful is its lasting impact on the victim, in addition to having all the benefits of a regular phishing attack.

**How to Prevent Spy-Phishing?**

As with any other phishing attack, defense against spy-phishing requires precautions from individual customers and large enterprises. Below we will discuss spy-phishing prevention tips for corporations and individual customers, to create a complete sense of awareness and develop vigilance amongst users against this relatively new threat.

**Corporations**

* Regularly update your security definitions. Regularly means, preferably, daily. This is particularly important to defend against viruses that can be hosted on webpages. Beta definitions are also provided by many vendors which come with the same quality as that of daily downloads.
* Keep your security product complete. It doesn’t matter which security provider you choose to use, just make sure it provides a comprehensive suite including multiple protection layers. This includes the gateway, servers and individual systems. For example, laptops or other removable devices that can be operated outside the office premises require your security solution to include built in antispyware and client side firewall to prevent threats from entering your network once they reestablish a connection to your system.
* Deploy a vigorous anti-spyware solution which checks windows startup and registry, thereby blocking any attempts of spyware installation. Update the definitions daily.
* Choose an antivirus or antispyware with URL filtering feature. This ensures that any access to malicious sites is prevented through accidental or intentional clicking.
* Keep your knowledge updated on ActiveX vulnerabilities. Though user-friendly, ActiveX controls are known for vulnerabilities. Either turn off ActiveX in browser or install a plugin that displays real address of the website being viewed.
* Train and aware your personnel. This is probably the first line of defense that ensures the protection of your network and clients. A security solution can never be effective unless your employees are not fully trained to develop security consciousness. They need to be given information security awareness trainings, understand organizational security best practices and security policies, and also be able to respond effectively to your security product warnings.
* Limit access to critical devices and services by employing access control policies. This will limit potential for damage.

**Individual Consumers and End-Users**

* Be vigilant and examine every email in depth. Though most of the emails are harmless and very much required for daily communication, it is very important to be extra cautious with email containing attachments and coming from unknown senders. Even when emails seemingly come from known sources but are out of context, inspect them closely.
* Aware yourself with communication policies of your bank. Since attachments and links are common and known ways of conducting phishing and social engineering, banks almost never communicate with their clients that way. Avoid the urge to click. If you feel there is something really important in there, always type the bank address manually and check if the same information is available on their website or not. Also, banks and other companies never share their confidential information through email. Always remember this.
* Have your system and applications installed with the latest patches. Enable automatic updates and make sure your system is updated daily.
* Keep your security products updated, preferably with daily automatic updates. Install updated anti-virus, anti-spyware and firewall to protect your system.
* Keep your email client configuration such that it only displays plain text. Though HTML formatted emails look more attractive, they can carry a range of easily exploitable vulnerabilities. Plain text or rich text format helps you avoid scripted mail embedded with malicious code.
* Do not provide personal information needlessly. In situations where you need to provide personal information to legitimate websites, such as online shopping, always remember that they employ security protocols like SSL or TLS protection. If the URL of a site starts with ‘https://” that means it is secure.