What Is Adware, Malware, and Spyware?

As a business owner, it is always important to keep your employees informed about the Cyber threat landscape that is out there. One of the best ways to do this is to conduct regular security awareness training programs, on a quarterly basis.

One of the concepts that you will need to cover are the primary differences between Adware, Malware, and Spyware? This may seem like a simple question, but it can be a bit more complex to answer. In this blog, we outline some of the fundamental details of them.

1) What is Adware?

   According to the security experts, Adware can be specifically defined as:

   "The name given to programs that are designed to display advertisements, and your redirect your search requests to advertising websites and collect marketing data about you".

   (SOURCE: www.usa.kaspersky.com)

   Adware used to appear merely as annoying pop up messages in your web browser that you could just exit out of. But now, they have become much more covert and malicious in nature. For example, they can now deploy the Trojan Horse virus. These days, adware cannot even be seen; and there are two ways that your computer can get them:

   *Via free software packages or other share ware that you may download:

   These are often used by the open source software community as a way of funding their projects. But very often, Cyber attackers can take advantage of this, and often create spoofed ads that look like the real thing. If ever in doubt, always contact the organization in question to confirm the legitimacy of their ads.

   *Visiting an infected website:

   Web browsers these days will warn you about a malicious website before you visit it; so therefore, it is important that you pay attention to it. Any Adware that is deployed from such a site is known specifically as "Browser Hijacking".

2) What is Malware?

   Malware is an abbreviation that stands for "Malicious Software". It is defined as follows:

   "This is a software that is specifically designed to gain access or damage a computer without knowledge of the of the owner. There are various types of malware including key loggers, viruses, worms, etc."

   (SOURCE: www.us.norton.com)

In a way, Malware can be considered as a step up from Adware. The goal is not to just merely deploy a Trojan Horse virus, but the intent of Malware is to cause as much damage as possible to your computer, or even your Smartphone. As noted in the definition, even a worm can be considered as a form of Malware. In this regard, unlike Adware, ***Malware can actually spread itself from one computer to another, in just a matter of a few minutes***. Some of the common objectives of the Cyber attacker when deploying Malware include the following:

*Gain covert, remote control to an unsuspecting machine;

*Send unwanted spam messages from an infected machine to other unsuspecting targets (this is also known as a "Botnet" attack – where the malware that resides on the infected device can be used to target thousands of other computers);

*Investigate in more granular detail the kind and type of network that the infected computer is using, and steal any relevant information and data.

3) What is Spyware?

As the name implies, Spyware is designed to literally "spy" on you. It does not mean that you are being tracked down in a physical sense; but rather, you every move is being watched virtually. A formal definition of Spyware is as follows:

"It is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission."

(SOURCE: www.veracode.com)

Spyware is actually a subset of Malware. But the main difference between the two is that the ***former will collect your personal information and data.*** The latter is just meant to cause widespread turmoil by spreading itself to hundreds if not thousands of computers. Spyware literally uses up most of your network bandwidth and collects such items about you as your name, home address, web browsing habits, website preferences, and even what you download. This is mostly done with what is known as a "Keylogger". So, if you notice a drastic slowdown in your network connectivity for long periods of time, there is a good chance that your computer has been infected with some sort of Spyware. Other telltale signs include that of unexpected "behaviors" on your computer, such as new icons appearing, a different toolbar in your web browser, system crashes, and even failure to boot your computer up properly. Worst yet, if your computer is indeed infected with Spyware, it can also serve as an invisible beacon alerting other Cyber attackers that your computer has a weak spot and can thus be easily penetrated into. So, in the end, you may not be dealing with just one Cyber attacker, you could be dealing with many at the same time.

Now that as a business owner, you have a better understanding of what Adware, Malware, and Spyware actually are, a future blog will demonstrate some actual examples of them. We will also outline the steps that you can take to protect business from these threats.

In the meantime, if you have any questions, don't hesitate to contact us!