Securing USB Flash Drives

Posted At : August 30, 2015 11:05 AM | Posted By : Admin
Related Categories: BYOD, Security

Whether you call them USB Memory Sticks, Flash Drives, Jump Drives, USB Drives or whatever, these devices are all the same. They can store many gigabytes of data and programs and if used incorrectly they can comprise the security of the machine they are plugged into or the network they are connected to.

You may have noticed growing reports in the media about the dangers of using USB memory sticks. It is true, they are susceptible to being exploited like everything else, however, and these exploits aren't terribly easy to carry out by hackers. Mostly because an attacker needs physical access to your computer in order to infect it.

What Can a "Bad" USB Stick Do?

A malicious device can install malware such as backdoor Trojans, information stealers and much more. They can install browser hijackers that will redirect you to the hacker's website of choice, which could host more malware, or inject adware, spyware or greyware onto your computer. While the ramifications of these threats can range from annoying to devastating, you can stay protected from these threats.

Staying Protected is Easier Than You Think

- Don't plug unknown flash drives into your computer- this is one of the most important pieces of advice you should follow. This is a tactic used in social engineering, where the attacker relies on the curiosity of people. If you see a USB stick lying out in open, public places, do NOT plug it into your computer to see what's on it.
- Use secure USB drives. Some newer models have safety features such as fingerprint authentication that help protect the device from hackers.
- Don't use the same flash drives for home and work computers, as you could run the risk of cross contaminating your computers.
- Be careful where you purchase your USB drives from, as some shady third party manufacturers are known to manufacture these devices with malware on them. Always buy your flash drives from reputable, well known manufacturers as well as sellers.
- Keep the software on your computer up to date. No one likes to do them, but software updates are crucial to the security of your computer, as they patch known vulnerabilities.
- Make sure to keep your Internet security software up to date. In the event you accidentally use a device that contains malware, you're protected. If you don't have Internet security software, you should get it, as it can protect you from a host of issues other than just USB malware.