Cyber Security Tip ST08-001

Using Caution with USB Drives

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks. What security risks are associated with USB drives? Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers. One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer. Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers. Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked. The most obvious security risk for USB drives, though, is that they are easily lost or stolen (see Protecting Portable Devices: Physical Security for more information). If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it. How can you protect your data? There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into: * Take advantage of security features - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see Protecting Portable Devices: Data Security for more information). * Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer. * Use and maintain security software, and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current (see Understanding Firewalls, Understanding Anti-Virus Software, and Recognizing and Avoiding Spyware for more information). Also, keep the software on your computer up to date by applying any necessary patches (see Understanding Patches for more information). * Do not plug an unknown USB drive into your computer - If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your

computer to view the contents or to try to identify the owner. * Disable Autorun - The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In How to disable the Autorun functionality in Windows, Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."

Author: Mindi McDowell
