USB Flash Drive Security  TIP of the Month  June 2007

A USB flash drive (also known as a thumb drive, jump drive or key drive) is a convenient, low cost and physically small device that can store vast amounts of data. These “features” are also their major weakness and can pose an extremely high security risk if security controls are not implemented.

Security Concerns

The good news is USB flash drives are small and portable making data transport very convenient. The bad news is USB flash drives are small and portable and pose a high risk for loss and theft. They are a tremendous source of data leakage if not properly secured.

USB flash drives are susceptible to viruses and malware. If you use your USB flash drive in a public or foreign computer system, your flash drive can become infected. Alternatively, bad guys can plug their USB sticks into your PC and plant spyware, viruses and other malicious programs onto your computer.

USB flash drives can be configured to be bootable and run programs. This is a popular way for technicians to perform diagnostic work, but it is also very convenient for the bad guys to use as a USB attack device. Plug a USB flash drive configured by a bad guy into a PC running Windows and the device can literally take over the machine, search for confidential documents, copy them back to the USB’s internal storage, and hide them as “deleted” files.

USB flash drives can become corrupted so be sure to backup your data on the flash drive just as you would on any other device.

Security Controls

Purchase USB flash drives that include built-in security features such as encryption and password protection. There are also anti-virus applications that can be run directly from the flash drive to ensure that it won’t get infected by a public or foreign computer system that may have a virus. These devices are readily available in stores now and the additional cost is minimal when you compare it to the security provided.

Do not copy sensitive data to a USB flash drive if possible. If you do have sensitive data on the USB, be sure that the device is password protected and the data is encrypted. Always keep your USB flash drive physically secure. In addition, if you happen to find a USB flash drive that someone lost, DO NOT plug it into your computer as it could be infected or contain other malicious software.

Your responsibility!!

You are responsible for protecting sensitive information.

Be sure that you implement the appropriate security controls to eliminate a significant source of risk. The repercussions of data security breaches that stem from theft or loss of USB flash drives can cost millions of dollars and do irreparable harm to the trust customers and partners have placed in our organization.

Be aware that unauthorized use or release of sensitive information may subject the violator to personal, civil, and/or criminal liability and legal penalties.

Violations may constitute grounds for corrective action up to and including termination of employment or student status, loss of UNC Health Care and UNC School of Medicine privileges or contractual or affiliation rights in accordance with applicable UNC Health Care procedures.