What are the security issues involving removable storage devices?

The ease with which large amounts of data can be transferred to a removable storage device and its portability allow for information to be easily stolen. These devices also provide an easy way to transfer malware which can cause immeasurable harm to a network. A 2011 report stated that 70% of businesses have traced loss of sensitive data to the use of USB flash drives and 55% of those incidents introduced malicious code to the network.[[1]](#footnote-1)

What is malware?

Malware is a term describing malicious software intentionally designed to disrupt computer operations, gather sensitive information, or gain access to private computer systems.

What are removable storage devices?

Removable storage devices transfer data between the device and a host computer. Broadly speaking these devices are broken into two categories: **Wired Devices** which require a direct connection to a computer usually using a USB port, or **Smart Media Devices** which connect wirelessly to the Internet to transfer data to a host computer.

Wired devices encompass a broad variety of technology whose storage capacity is constantly improving.

* **USB Flash Drives** also referred to as Memory Sticks, Jump Drives, or Thumb Drives connect to a computer through its USB port.
* **Portable Hard Drives** connect to a computer through a USB port and can store large amounts of information.
* **CDs, DVDs, and Blue-ray discs** with read / write capability allow for the storage and transfer of information.
* **Media Cards** found in cameras and picture frames are capable of storing and transferring information through direct connectivity to a computer or in wireless mode

Wireless devices are capable of transferring information and malware.

* **Tablet Computers**, such as the Surface or iPad, are a boon to the traveling lawyer but also susceptible to malware when using unencrypted connections to access a network.
* **Gaming Devices**, such as the Xbox, Playstation or Wii, can be easily modified to act as personal computers or servers. This can make them suspects in the transferring and hiding of confidential data.
* **Music Players** such as iPods or MP3 players are also susceptible.
* **E-readers** access the internet wirelessly which could download a virus that when connected to a computer could populate its new environment.

Best Practices – Avoiding Security Risks with Removable Storage Devices

Know and follow your firm’s polices for using removable storage devices. To deal with the real threat of removable storage devices, protection comes first. A user model that includes smart, enforceable policies and is proactive is crucial. Taking the following steps permits removable storage devices to be an important component in increasing firm productivity and lessens the fear of loss of information.

* Report any lost or stolen devices
* Be suspicious of any unwarranted network access.
* Avoid connecting unknown devices to your computer. Instead give the device to the appropriate individual at the firm to review and scan for viruses.
* Always scan devices connected to your computer with virus protection software.
* Password protect a device with strong passwords. Increase security by password protecting individual files copied to the device.
* Use removable storage devices that are capable of encrypting data.
* Store data types separately. It is best practice not to comingle business and personal data.
* Ensure that no information is lost by regularly backing up data to a secure location.
* After using a removable storage device, use secure data removable procedures to delete data from the device.

1. Schwartz, Mathew J. “How USB Sticks Cause Data Breach, Malware Woes.” Information Week. August 8, 2011. http://www.informationweek.com/storage/security/how-usb-sticks-cause-data-breach-malware/231300434 [↑](#footnote-ref-1)