West Virginia Executive Branch
Privacy Tip

USB Drive Safety



We've all seen them, and most of us have used them to store or transport information from one computer to another. They are so popular now that they've become a fashion accessory – super heroes, movie icons and even food shapes. USB drives (also known as thumb drives, flash drives or memory sticks) are given out at conferences and trade shows loaded with promotional materials you can download later.

But to Internet Security experts, these little storage devices can be a disaster in the making. They are so small and so inexpensive, they can be found everywhere. The more common they become, the greater the chance they can be lost, stolen, or used to spread malicious programs. A virus-infected USB drive plugged into a computer could inadvertently upload a bug and cripple an entire system.

A lost or stolen USB drive could contain sensitive data that may not be encrypted or secured. It is estimated that that more than 12,000 hand-held devices, including USB drives, are left behind in taxi cabs every year. London dry cleaners estimated they found over 9,000 in pants pockets.

Here are some tips for USB safety:

- ✓ Minimize the amount of personally identifiable information (PII) and other sensitive data stored on a USB drive.
  - o If you must absolutely put PII or sensitive data on it, encrypt it! Talk to your IT department for instructions.
- ✓ Keep the USB drive safely in your possession, or lock it up when not in use.
- ✓ If you find a USB drive, NEVER EVER plug it in your computer! It could be full of malware.

Protected USB drives are available for purchase. They cost a bit more, but how much is the confidentiality of you information worth?

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.