Computer security and privacy tips: Flash drives

In conjunction with the Office of Administrative and Information Management Services (AIMS), the DHS News is offering tips for using your computer safely and securely. DHS employees and contracted personnel are required to adhere to laws and regulations regarding confidentiality and Protected Health Information (PHI). These tips are designed to enhance knowledge on avoiding use that could compromise data. If you have additional questions, contact the DHS Service Desk at 412-350-4357, option 2.

Flash drives

USB flash drives, or memory sticks, are data storage devices for your computer that are typically removable and rewritable. The small size of the device makes it highly portable – but also creates a concern for data security. A recent study by the Ponemon Institute revealed that while these devices may be small, the data breaches that can result from lost or stolen USBs are huge. Organizations and employees need to properly manage the security and privacy requirements of data retained on USB drives.

- Refrain from transporting sensitive data such as Personally Identifiable Information (PII) or Protected Health Information (PHI) on to an un-encrypted USB drive
- If you have a valid or compelling business reason to transport sensitive data to a USB drive, first consult with your supervisor or manager for his or her approval
- Never share or use USB drives that are not issued by your organization to reduce malware infection risks
- USB flash drives can be used safely and securely if the risks are understood and proper measures are taken to mitigate them

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, which 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 people buy the infected products and plug them into their computers, malware is installed on their computers. If you have additional questions, contact the DHS Service Desk at 412-350-4357, option 2.

See more at https://www.us-cert.gov/ncas/tips/ST08-001