

Cyber Security: On the Front Line

Issue No. 1
March / April 2010

EITS Cyber Awareness: On the Front Line

The ACIO for IT Operations (EITS) is now responsible for Cyber Security Awareness Training and all other cyber awareness activities at HQ and among EITS DOECOE customers/users.

EITS will work closely with customers and sites to ensure coordination for the Mandatory Annual Cyber Security Awareness Training in July-August of 2010. As with last year, the 2010 training was developed by DISA and will be accessed via OLC2.

More information on Mandatory Cyber Awareness Training will be coming soon!

Thumb Drives: Gone in a Flash!

The careless use of portable media storage devices such as USB drives, also called "thumb drives" or "flash drives", poses a serious threat to system and information security and integrity.

Thumb drives, are small, readily available, inexpensive, and extremely portable, and are popular for storing and transporting files from one computer to another. However, these same characteristics make them an ideal mechanism for security breach and cyber attacks via a PC USB port.

At the most basic level, thumb drives can be a source of unauthorized access to information, due to the small size and potentially very large storage capabilities. In addition to the surreptitious use of thumb drives to copy data by unauthorized people, authorized users can contribute to security problems through careless management leading to drives being mislaid, lost, copied, or stolen.

The common practice of maintaining a large volume of unencrypted data on a thumb drive

and/or the failure to maintain a backup copy of data kept on a thumb drive can result in a significant security breach and/or a catastrophic loss for the Agency (or yourself).

Thumb drives are a convenient tool for cyber-espionage. An attacker with physical access to a computer can download information directly and quickly onto a thumb drive; within a few minutes, a data transfer can occur. A computer recently turned off is still vulnerable, because a computer's memory is still active for several minutes after being turned off. A thumb drive with appropriate software can be used to reboot the system and copy the computer's memory, including passwords, encryption keys, and data.



Thumb drives preloaded with malware software can pose a serious security threat to enterprise computers and other computer infrastructure.

US AF IMAGE 100226-f-00s-001
Malicious code such as viruses, spyware, "bots," and "worms" can be loaded onto a thumb drive. When the thumb drive is plugged into a USB port the software is automatically downloaded and installed; infecting the computer. Thereafter, the infected "host" computer can download the malicious code to other thumb drives, imbed it in emails, or spread it directly to other computers or across networks, without the knowledge or participation of the host computer user.

In this situation, the thumb drive acts as the carrier of the infectious agent, automatically uploading the malware when plugged into another computer or automatically launched by normal computer operations. Attacks through other electronic devices with ports for thumb drives or a USB connection can also serve as a source for

infection. For example, electronic devices that utilize USB ports to upload data, such as electronic picture frames, may be pre-loaded with malware. Infected devices can automatically contaminate a thumb drive or a computer directly through the USB connection.

In summary, thumb drives are an ubiquitous tool for the appropriate transfer of data from one computer to another, but they are also convenient mechanisms used for deliberate security threats. The large data storage capacity, small size, and standard USB port feature makes the drives an almost invisible means for unauthorized transport of information and a powerful tool to transmit malware to computer systems.

How can you use thumb drives safely?

The key to maintaining a secure computing environment is ensuring that data is "safe in place."



Protect all electronic devices and computers through the use of complex authentication e.g. long and complex passwords and 2-factor

authentication, and data and data transfer encryption in order to secure Agency and personal data and systems from viruses, spyware, and other malware.

- **Utilize security features that are provided on thumb drives –**

Only use thumb drives that have password and encryption capabilities. Use passwords and encryption on the thumb drive to protect your data against authorized data access, should it be lost or stolen. Ensure that you have a backup of the information on a thumb drive in case your drive is lost or damaged.

- **Maintain physical security of your computer and storage media –**

Lock your computer, even if leaving your office for a short time, and be wary of intruders in the workplace (even if they have a badge.) Remain in your office for a short while after you turn off your computer to ensure that it has completely shut down before leaving it. Never leave a thumb drive unattended in your computer

or work space: store them in a safe place such as a locked desk drawer.

- **Use and maintain security software, and keep all software up to date –**

Run anti-virus and anti-malware software automatically when a thumb drive is inserted into a computer.

Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and keep the security software current.

- **Limit the volume of data on a thumb drive –**

Unless managing a thumb drive for a secure backup, thumb drives used for data transfer purposes should not become a file "catch all." Manage drives used for thumb drives by limiting the data on the drive, and delete data when it is no longer needed.

- **Do not use "free" thumb drives from a trade show or other venue.**

Free thumb drives can be pre-loaded with malware that can attack computer systems. Accept thumb drives pre-loaded with software or data only from a known and trusted source, and only for a known purpose.

- **Do not insert an unknown thumb drive into your computer –**

If you find a thumb drive, do not plug it into your computer to view the contents or to try to identify the owner. Give it to the **Help Desk, (3-2500)**, to ensure appropriate and safe management.

- **Keep personal and business thumb drives separate –**

Do not use personal thumb drives on DOE computers and be careful of transferring DOE information between your personal thumb drives or personal computer and DOE computers.

- **Dispose of thumb drives properly-**

When a thumb drive no longer works or is not needed, do not casually throw it away. Remember: thumb drives can hold large amounts of data and act much as a computer hard drive.

Data can be recovered from a thumb drive, even if it is no longer working. Instead of throwing it in the trash, contact the **Help Desk (3-2500)** to dispose of unwanted or defective thumb drives.