Handling Computer Security Incidents

USB Storage Device Security

USB (Universal Serial Bus) storage devices are very convenient to transfer data between different computers. You can plug it into a USB port, copy your data, remove it and be on your way. Unfortunately this portability, convenience and popularity also brings different threats to your information.

Data thefts and Data leakage are everyday news now! All these can be controlled or minimized with care, awareness and by using appropriate tools to secure the information. The tips and recommendations provided in this document helps you to keep your information secure while using USB storage devices.

The Conficker worm spreads via removable devices and drives such as memory sticks, MP3 players and Digital Cameras.

Also 30 percent of new worms have been specifically designed to spread through USB storage devices connected to computers.

The Stuxnet worm was one of the year's high-profile threats that spread through USB drives.

Handling Computer Security Incidents

Threats

Malware Infection

- Malware Spreads through USB storage devices. Somebody may intentionally sell USB storage devices with malware to track your activities, files, systems and networks.
- Malware may spread from one device to another device through USB Storage Devices using autorun.exe, which is by default enabled.

Unauthorized Usage

- Somebody may steal your USB Devices for Data.

Baiting

Somebody intentionally leave USB devices at your Desk or Place with Malware

How to stop Data Leakage via USB storage ?

- Design and adopt a good security policy to limit the usage of USB Storage devices.
- Monitor the employees what they are copying.
- Implement Authentication, Authorization and Accounting to secure your information.

What to do when you lose the Device?

- If you have stored any personal or sensitive information inside the USB drive like passwords etc, imediately change all passwords along with security questions and answers provided during any account creation [There may be chances that hacker can retrieve your online account logon information by using data in the stolen drive].
- Also ensure that all security measures have been taken against the data lost.

How to stop Device theft ?

- Always secure the drive physically by tagging it to a key chain.
- Never leave your drive unattended anywhere.
- Never keep sensitive information without encryption .

certin
Handling Computer Security Incidents

Types of devices which support USB

- Card readers
- Mobile phones
- PDAs
- Digital cameras
- Digital audio players
- Portable Media Players
- Portable flash memory devices

Guidelines in the usage of USB devices

Do's

- Always do low format for first time usage.
- Always delete the drive securely to clear the contents.
- Always scan USB disk with latest Antivirus before accessing.
- Protect your USB device with a password.
- Encrypt the files / folders on the device.
- Use USB security products to access or copy data in your USB.
- Always protect your documents with strong password.

For Small Business or Enterprises

- Monitor what data is being copied.
- Block the unauthorized USB from connecting.
- Pick the device with features and correct level of encryption to meet compliance requirements and organization needs.
- Educate employees on acceptable and inacceptable use of USB flash drives.
- Document policies so that users know who is authorized and what they are authorized to do.

Don'ts

- Do not accept any promotional USB device from unknown members.
- Never keep sensitive information like username/passwords on USB disk.

certin
Handling Computer Security Incidents

Mobile as USB

The mobile phones can be used as USB memory devices when connected to computer. A USB cable is provided with the mobile phone to connect to computer.

Do's:

- When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated antivirus.
- Take regular backup of your phone and external memory card because if an event like a system crash or malware penetration occurs, at least your data is safe.
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.
- Remember to remove the USB connection from your computer before you walk away.

Don'ts:

- Never forward the virus affected data to other Mobiles.

FAQ

How to bypass autorun?

Hold shift key and plug your thumb drive to disable autorun temporarily.

How to encrypt your data?

True crypt is a powerful open source freeware for protecting data on USB drive. It works on Windows, Mac and Linux platforms. It supports full encryption of system hard drives and USB devices.

The tool comes in a very easy to use package. Plug in your USB drive and open true crypt ex ecutable. Create volume for your USB drive and follow the instructions. You provide a pass word to protect the data and that's it! You can view the encryption progress in the pool content. You can select AES, Serpent or Twofish encryption algorithm. To access the data back you just need to enter the password.