इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

G20 भारत 2023 INDIA

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Digital India
Power To Empower

75 Azadi Ka Amrit Mahotsav

USB STORAGE DEVICE SECURITY

In association with

cert-in

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

NeGD
National e-Governance Division

myGOV
मेरी सरकार

ISEA
www.isea.gov.in

www.InfoSec awareness.in

Universal Serial Bus (USB) - Storage Device Security

Universal Serial Bus (**USB**) storage devices are very convenient to transfer data between different computers/ devices.

USB (Universal Serial Bus) storage devices are very convenient to transfer data between different computers. It is a widely used interface for connecting devices such as digital cameras, keyboards, printers, scanners, pendrive, external hard drives etc., to Laptop/Desktop.

To use a device with a computer, you typically need to connect it using a **USB cable** . The cable has a USB connector on each end, and one end is plugged into the device and the other end is plugged into a computer via USB interface.

USB drives or USB devices or USB storage devices, all of them are synonymous and are very convenient to transfer data between computers and devices. 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

There are several **advantages** to using USB devices:

- **They are easy to use** - most computers have built-in support for USB devices, so you don't need to install any special drivers or software.

There are a few potential **disadvantages** to using USB devices:

- **They can be lost or stolen** - because USB devices are small and portable, they are easy to misplace or have stolen. This can be a problem if you have sensitive data stored on them.

- They are fast - USB devices can transfer data at high speeds, making them suitable for transferring large files.

- **They are versatile** - USB devices come in a variety of forms, including flash drives, external hard drives, and more, so you can choose the one that best suits your needs.

- **They are portable** - USB devices are small and lightweight, so you can easily take them with you wherever you go.

- **They are convenient** - you can use a USB device to transfer data between computers, and you can also use them to charge some types of electronic devices.

- **They are relatively inexpensive** - USB devices are widely available and are generally not very expensive.

- **They can be damaged** - USB devices are vulnerable to physical damage, such as being dropped or having their connectors bent. This can make them unusable.

- **They may not be suitable for all types of data** - depending on the type of data you are storing, a USB device may not be the most suitable option. For example, if you are storing large amounts of data that need to be accessed quickly, a USB device may not be the best choice.

- **They may not be compatible with all devices** - some devices, such as older computers or certain types of gaming consoles, may not have support for USB devices.

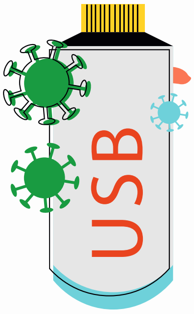
- **They may not be as secure as other options** - depending on the level of security you need, a USB device may not provide enough protection for your data. For example, if you are storing sensitive financial information, you may want to consider using a more secure storage option.

Associated Threats

Misplacing your USB drive
There is a chance of misplacing the USB which may result in loss of important data. So, always use a password protected drive and copy the encrypted files to it.

Malicious USB drives

When we use in an unsecured environment/PC, the USB may get infected by malicious virus/malware. Malicious USB drives contain a pre-programmed attack strategy that allows them to steal a user's data by gaining access to their confidential files.

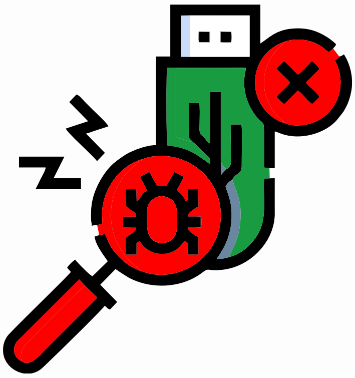


Data breaches and losses

Data loss or leakage is another concern that might arise while utilizing insecure USB drives.

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 through USB Storage devices using autorun.exe, which is by default enabled.



Unauthorized Usage

Somebody may steal your USB storage device and misuse the device/data stored in the USB.

How to stop data leakage via USB storage?

- Design and adopt a good security policy to limit the usage of USB storage devices.
- Store and carry only password protected (Encrypted) files using a strong password.
- Scan before connecting the USB to any device for virus/malware protection with an updated antivirus.

What to do when you lose the device?

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

Ways in which fraudsters may attempt stealing USB drive :

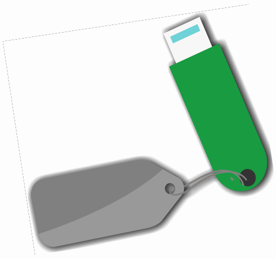
There are chances that some of the miscreants may try to steal confidential and critical data stored in USB drives or infect them with some malware so that one cannot be able to use it.

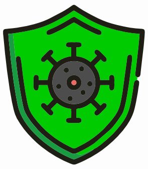
They may be doing it in many of the following ways

- Look for an opportunity to steal the USB drive, if we are not careful while handling it.
- Requesting for USB drive for short time use and on that pretext they may steal or save our personal data or even delete it .
- They may even get the USB drive infected with Virus or any other malware while being used by them, which once connected to our computer, it may get installed or resides on personal/official computer and can be used to steal our confidential information which may lead to its misuse.

Best practices for improving the security of USB storage devices:

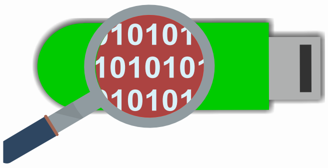
Keep your USB drive with you - it's a good idea to keep your USB drive with you at all times to prevent it from being lost or stolen. If you do need to leave it somewhere, make sure it is in a secure location. Always secure the USB drive physically by tagging it to a key chain.

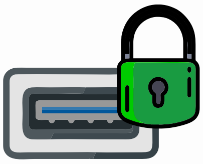




Use latest Antivirus software while accessing USB : Always scan USB disk with latest Antivirus before accessing it on any system.

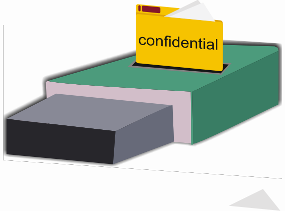
Enable encryption - some USB drives offer the option to enable encryption, which can help protect your data from being accessed by anyone who doesn't have the correct encryption key.

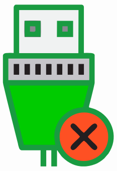




Use a USB port lock - a USB port lock is a physical device that prevents unauthorized access to your computer's USB ports. This can help prevent someone from connecting a rogue USB device to your computer and accessing your data.

Don't store sensitive data on a USB drive - if you have sensitive data that you need to store, it's best to use a more secure storage option, such as a cloud-based storage service or an encrypted hard drive.





Disconnect your USB drive when you're not using it - if you're not actively using your USB drive, it's a good idea to disconnect it from your computer to prevent any unauthorized access to your data.

Keep your USB drive up to date - make sure to keep your USB drive's firmware and security software up to date to ensure that it is as secure as possible.

Follow secure practices while using mobile as USB storage: Smartphones can also be used as USB storage device when connected to computers, a USB cable is provided with the mobile phone to connect to a computer.

- When a Smartphone 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 a mobile from a computer, the data should be scanned with the latest installed Antivirus.
- Remember to eject the USB connection from your computer while leaving the organisation.