

5 ways to protect your USB device and prevent data loss.

If you have a habit of frequently storing important data and documents on USB devices, protecting and closely monitoring them is essential. This article from TipsMake will introduce you to 5 ways to safely protect your USB devices and prevent data loss.

In a previous article, TipsMake provided readers with the best USB data recovery software to retrieve data in case of accidental deletion or other related issues.

However, prevention is better than cure. Instead of waiting until your data is lost before trying to recover it, you can set up security measures to protect your USB device and prevent data loss. Refer to the article below from TipsMake to learn how.



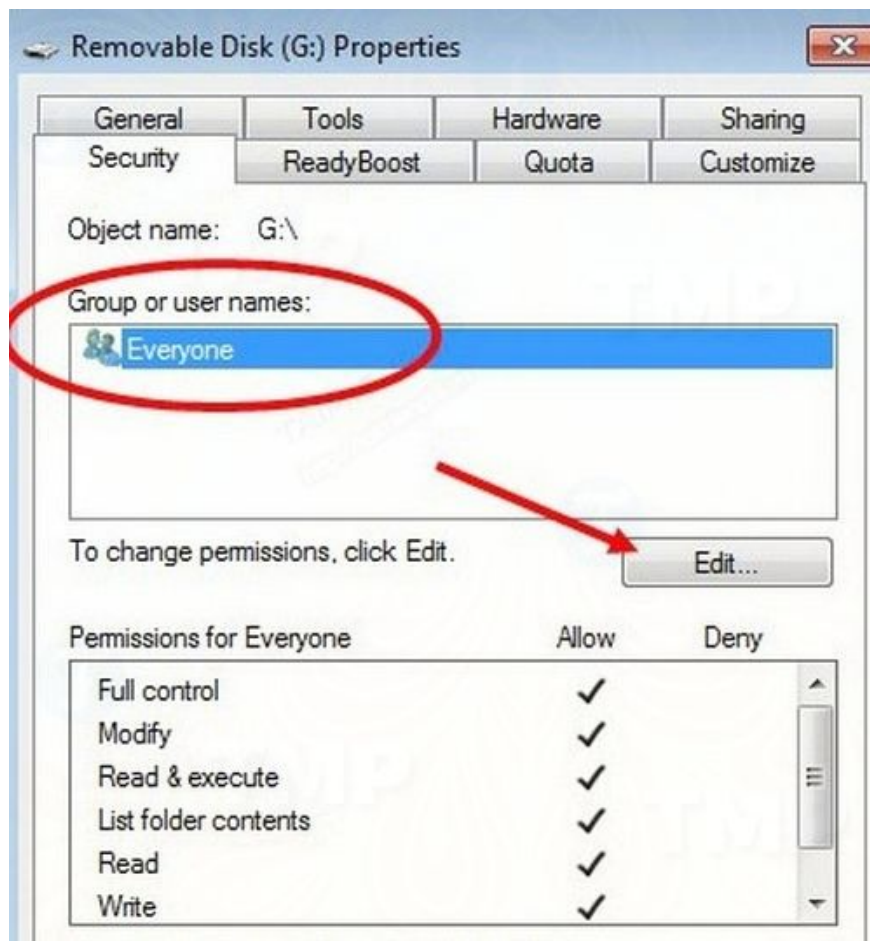
5 ways to protect your USB device and prevent data loss.

5 ways to protect your USB device and prevent data loss.

Below, TipsMake will introduce and guide you through 5 ways to protect your USB devices and prevent data loss:

Method 1: Setting up write permissions

To prevent other users from modifying important files and data on a USB device, you can edit the Registry values. This way, other users will only be able to access the data on the USB drive and will not have the right to change or modify it.



Method 2: Controlling USB virus attacks

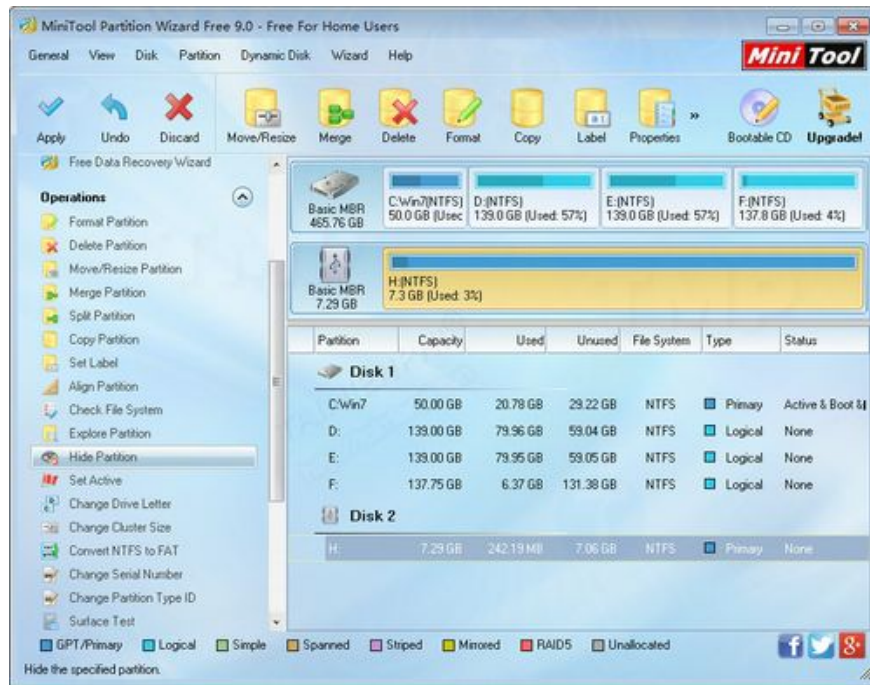
Sometimes your computer can be attacked by viruses or malware, Trojans, without your knowledge. Unintentionally, when connecting a USB device to your computer, viruses can attack your USB drive and corrupt your valuable data. To control USB virus attacks, the best way is to deny access to all accounts on USB devices.

Method 3: Hide USB drives on your computer

If you don't want other users to be able to view the data on your USB device, you can set it to hide all USB drives except your local hard drive. Even if another user gains unauthorized access to your computer, they won't be able to access this data.

Additionally, to hide USB drives on your computer, TipsMake recommends using the **Hide Partition** option in MiniTool Partition Wizard to avoid having to set up or configure your computer.

To download MiniTool Partition Wizard, click here: [Download MiniTool Partition Wizard](#)



Method 4: Disable Auto Play

When a USB device is connected to a local computer, Windows automatically opens the corresponding device window, allowing users to quickly access their files and data. Network viruses can exploit this process to corrupt data.

Method 5: Setting a password for the USB drive

If you find it annoying having to manually display the device every time you connect and use a USB drive, you can instead set a strong, hard-to-guess password for it. You can refer to the guide **on setting a password for a USB drive**, creating a password to protect your USB drive using USB Security to do this.

Additional information about USB and USB devices.

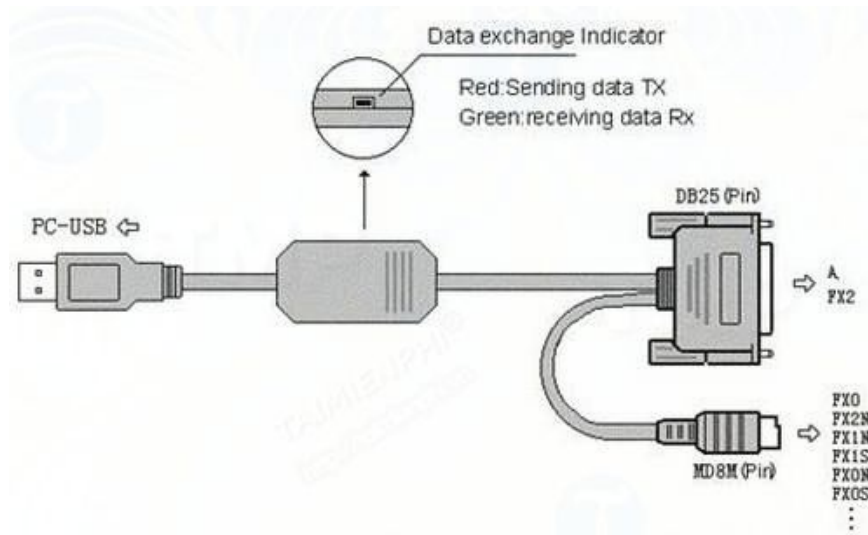
USB was first launched in late 1994, specifically on November 11, 2014, and was proposed by Intel, Compaq, IBM, Microsoft, and several other companies. USB 3.1 is the latest version of the device currently available.

The outstanding features and advantages of USB include fast transfer speeds, convenience, flexible connectivity, independent power supply, etc. The device plays a crucial role in connecting computers to most external devices, such as mice, keyboards, printers, scanners, cameras, chargers, USB drives, MP3 players, mobile phones, digital cameras, portable hard drives, USB drives, ADSL modems, and cable modems.

USB structure

The USB drive structure is divided into two parts: software structure and hardware structure. Specifically:

1. Software Structure: Each USB drive has only one host, and the host software is designed based on a modular and object-oriented approach. USB software typically includes three main modules: Universal Host Controller Driver (UHCD), USB Driver (USB D), and USB Client Software.



2. Hardware structure: USB uses a 4-wire cable. Two of these are channels used for data transmission, and the remaining two wires are used to power the downstream device.

For high-speed peripherals requiring high bandwidth, USB data transfer speeds can reach up to 12Mbps. However, for low-speed peripherals, USB will only transfer data at 1.5Mbps. In other words, the USB bus will automatically switch between these two modes depending on the peripheral device.

USB applications in daily life

1. USB data storage devices: including external USB hard drives, USB flash drives, SD memory cards on mobile devices, TF cards, USB memory cards, etc.



2. USB ports on a computer: Both the front and back of the computer case have USB ports for connecting to external devices, such as portable hard drives, USB flash drives, etc. Connecting these external devices to the computer allows users to manage data easily.

3. **Wireless USB Technology:** Wireless USB technology allows users to connect peripheral devices to their computers without the need for complex cable connections.



The standard data transfer speed on wireless USB devices is the same as the wired USB 2.0 standard (480 Mbps), the only difference being that wireless USB requires a wireless transceiver to be equipped on the computer and peripheral devices.

4. Some specific USB applications include:

- USB modem.
- USB speaker.
- USB hub.
- USB sound card.
- USB camera.

Above, TipsMake has introduced 5 ways to protect your USB devices safely and prevent data loss. Prevention is better than cure; waiting until you lose data before trying to recover it, and if your data cannot be recovered through traditional methods, it will be very costly to rely on experts or data recovery services, right?

You finished reading the article "**5 ways to protect your USB device and prevent data loss.**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
