

Forum:[Hack Forums](#)

Thread: [Secure USB/EXTERNAL-HDD from any threats/writeup \(make it usable on infected PC\)](#)

Replac - November 9, 2025, 8:07 am

This is an old but useful method I been using for years now. It's to help my USB drive or external HDD to stay secure from infections if I wish to attach it to other infected PC or maybe have some files transferred to a 3rd party PC and might not know if the PC be infected or not. This will help you copy your files to another device without the worry of writeup by a malware and get your own PC infected after. Stay safe - stay secure!

You will only be able to copy the files off the drive and not write/paste anything into that drive until you remove the write-up protection. Earlier we could do it using going to properties and saving the disk as read-only but now that can be changed easily by malware so we go the old ways to do it using CMD thus read-only cannot be modified unless its done using Promt.

Connect your USB Drive or External Drive to your PC and transfer any file/doc you wish into that drive from your original PC.

Then open cmd (as administrator) and type the following commands:

diskpart > list disk > select disk 1 > attributes disk set readonly (See the picture below to understand)

Hit enter and you are done. In my case, it will show only 2 disks which is disk 0 and disk 1. Select your USB/external disk which in my case is 1.

Once done, you just need to exit the cmd and have to eject your drive and connect it back to any 3rd party PC you wish to connect into.

As you can see in the picture below, after i open my drive files, and, tried to delete one of them and it appears the disk is write protected.

Thus making the files in your drive very well protected and even write protected by any malware.

Now to revert this to its original state, plug it back in, and open cmd and type in the following commands in the format,

diskpart > select disk 1 > attributes disk clear readonly

and press enter. After closing the CMD repeat the process which is to eject your drive and connect it back.

Once you connect it back, you'll see the drive is already back at it's default state and is ready to be re-written again.

Stay safe and stay secure! Have a good day and do not forget to like this post! ??

RITARI - November 9, 2025, 8:28 am

Nice guide! Correct me if I'm wrong, but malware with admin privileges can still bypass that.

Replace - November 9, 2025, 1:50 pm

(Nov 9, 2025 09:28 AM)RITARI Wrote: [\[CITE\]](#) Nice guide! Correct me if I'm wrong, but malware with admin privileges can still bypass that.

They will need to be able to rewrite read only to read/write using CMD instead of doing it through manual properties settings and not all malware or I should say none even thought that someone would use this old school method to make a drive read only and the only way to revert is using the same process using CMD and the malware will need a script built in for this exact purpose which I have never seen in any malware until date.'

It's old but works very well.

Bastille - November 10, 2025, 12:29 pm

Interesting thread, thanks for the share and how you made the thread with the images, sounds like we have an interesting new member :)

Replace - November 10, 2025, 8:47 pm

(Nov 10, 2025 01:29 PM)Bastille Wrote: [\[CITE\]](#) Interesting thread, thanks for the share and how you made the thread with the images, sounds like we have an interesting new member :)

Thank you, just wanted to explain as not many might understand when I write a command sequence as cd > ls > filename, just reading and leaving the thread and not even experimenting with it, thus wanted to give an insight with a little bit of visual images, encourages the human mind to at least give it a shot. Just my side of view, so did that. ?