

Remove Shortcut Virus: 9 Powerful & Easy Tweaks!

Table of Contents

What exactly is a shortcut virus?	3
Types of Shortcut Virus.....	4
Drive Shortcut Virus:	4
Folder Shortcut Virus:	4
File Shortcut Virus:.....	4
Preventive Measures in the First Place	5
Method #1: Using UsbFix – Shortcut Virus’ Quick Remedy	6
Method #2: Fix Folder and Trojorm Removal Tool	7
Method #3: Using WinRAR to Retrieve Your Original Files.....	8
Method #4: Kill USB Shortcut Virus with VBScript File!.....	9
Method #5: Removing Shortcut Virus using CMD.....	10
Method #6: A Coded .bat File to Permanently Remove Virus.....	11
Method #7: Removing Shortcut Virus from Registry	12
Method #8: Config Tweaking to Remove Shortcut Virus!.....	13
Method #9: Shortcut Virus Remover Tool.....	14
Bonus: How to Prevent Future Injections of Shortcut Virus?	15

One of the most common question asked is: **How to Remove Shortcut Virus?**

Every one of us has experienced the Shortcut Virus atleast once in our lifetime. Actually, it has become so common that people often overlook and underestimate it. In the beginning, it looks like nothing problematic has happened to be worried about. Afterall, it's just a shortcut file.

But it starts becoming worse:

As soon as days start passing after the shortcut virus initially enters in, you'll start finding almost all of your files, folder and finally drives turning into shortcut, which shows that the shortcut virus is spreading furthermore.

Shortcut Virus, once entered, tries to conquer every file on the device. So, the best possible remedy is to take quick preventive actions as soon as you spot it.

What exactly is a shortcut virus?

There's no wiki definition as such; but, as the name suggests, a shortcut virus is a virus (a malware) that hides your original files inside shortcuts.

The way it hides the file remains unknown though the effect is quite visible. The original files are there in the drive itself, but in such a position that you can't recognize it nor take it out (in the advanced stage).

Initially, it doesn't harms your files but later on, it may make them corrupt or even delete all the files; depends on the type of shortcut virus.

Types of Shortcut Virus

Depending on its effects, it can be broadly classified into 3 types:

1. Drive Shortcut Virus
2. Folder Shortcut Virus
3. File Shortcut Virus

Let's dive a little deeper into what each one of it exactly means.

Drive Shortcut Virus:

As the name suggests, Drive Shortcut virus creates a shortcut of the whole removable drive. This not only limits to Flash Drives or USB Drives but can also affect External as well as Internal Hard Disks also.

This type of virus is purely trojan where after entering into your Removable Drive, starts overtaking your files, grouping them and finally making shortcut of your flash drive.

Folder Shortcut Virus:

Self-explanatory, folder shortcut virus creates shortcuts of folders and wraps it's contents (files) altogether.

Less effective, but steal can spread itself after executing to number of other folders from where it can spy over on activities, upload data from that specific folder or do anything within the folder.

File Shortcut Virus:

A virus that makes shortcuts of program files.

While this type of virus is the least effective, it can do more of damage when it attacks an important software's execution file (.exe). On getting executed, this virus can also do just about anything inside the scope of that software. It also rapidly multiplies itself once it's executed.

The way all these viruses work and affect is different.

Preventive Measures in the First Place

I already told you about taking quick preventive measure as soon as you spot it, right?

So, what exactly do you need to do?

You shall first protect the infected drive from spreading furthermore.

To do that, follow these steps:

1. Stop autoplay of removable drives. [This guide from Redmond Pie will help you to quickly disable autoplay of external drives.](#)
2. And when you want to open and get the contents of your USB Drive, don't double click and open it, that will execute the virus. Instead, **Right Click** on the drive, click **Explore**. This way, the shortcut virus won't execute.

Method #1: Using UsbFix – Shortcut Virus' Quick Remedy

[UsbFix](#) is a free malware removal tool to will help you to detect and remove shortcut virus. It can scan infected removable devices, USB's external HDD's, smartphones, digital cameras, etc.

And here's the kicker:

It's sort of plug and play software i.e. **Download** -> **Open** -> **Run** and you're done!

With over 5 Million downloads, it is one of the most trusted software to remove shortcut virus. Also, it is designed in a user-friendly UI which will help you get things done easily and faster. The size of the software too, is quite small (approx. 4 MB) which will run and help you get rid of the shortcut virus instantly.

Steps to Remove Shortcut Virus using UsbFix:

1. Download USBFIX.
2. Connect your USB drive / External HDD drive which contains the shortcut virus.
3. Run UsbFix software.
4. Click on Deletion. On clicking it, the process to remove shortcut virus will start. It will then ask you to restart your PC.

A blue, rounded rectangular button with a slight gradient and a shadow, containing the text "Download UsbFix" in white, sans-serif font.

Method #2: Fix Folder and Trojorm Removal Tool

Trojorm Removal Tool is a piece of code that automatically runs and fixes all the files and removes shortcut virus completely from the external drive. This code is written by Archie Mercader, so special thanks to him for it!

Along with it, using fixfolder vbs file works the best. Fix Folder is a simple Visual Basic program that consists of a single loop that finds all the shortcut folders, and replaces it with the original folder name removing the shortcut virus.

Trojorm Removal Tool does the work of recovering the files from the virus while fixfolder fixes the actual shortcut of the drive and turns it into a normal application.

Steps to removing shortcut virus using Trojorm Removal Tool and FixFolder Script together:

1. Copy the Trojorm Removal Tool inside the infected drive and run it. (Make sure you copy it by "exploring" the infected drive or the virus will spread out).
2. Copy the Fixfolder Script to the infected drive, right-click on it and open with Notepad (or your preferred text editor) and change the letter H with the infected drive's letter. Save the file and run it.

[Download Trojorm & Fix Folder](#)

Method #3: Using WinRAR to Retrieve Your Original Files

As I've stated earlier, shortcut virus gets executed when you open your infected removable drive and hides all your files under shortcuts.

But, WinRAR is an application which doesn't allow execution of any malwares and hence, you'll be able to retrieve all your files back from the WinRAR interface.

This means, the shortcuts will still be there in your removable drive, but you'll be able to take all your files out of it and save it in a safe place.

Steps to remove shortcut virus using WinRAR:

1. Open WinRAR application. (If you don't have it installed, download it from [here](#))
2. From inside WinRAR interface, move on to your infected drive. Inside it, you'll find all your files safe and clearly visible.
3. Select them all, **right click** -> **Add Files to Archive** and choose a name like **USB Drive Backup.rar** (or anything you like). With this, you've created an archive of all the files inside the infected drive.
4. Open My Computer -> open your infected drive. You'll find your created archive there. **Right click** on it -> **Cut**. Paste it somewhere safe in your hard disk drive.
5. Open My Computer, **Right-click on your infected drive** -> **Format**. Choose **Quick Format** option and **Start**. After the format is over, just extract the backed up .rar file back into the removable drive.

Method #4: Kill USB Shortcut Virus with VBScript File!

Shortcut Virus gets dangerous when it starts multiplying on your PC creating shortcuts everywhere.

It can even go to limit of infecting the C: Drive of your PC and locking you out of it.

To prevent this before it happens, here's the solution:

A VBScript File coded to scan all infected drives, find out the virus and delete it.

And all these things are done within 30 seconds.

Actually, a VBScript is a Visual Basic Script that commands the PC to do certain tasks according to the code in it. In this case, it is directed to remove shortcut virus completely from your system.

So, it's not a software. It's just a script. The code for removing shortcut virus is already precoded in a way to delete shortcut virus from your PC.

All you need to do is, download the script, run it. It'll automatically start doing things on it's own.

A dialog box will pop up, asking you to click **OK** and again disappear for some moments, appear again. The same procedure for about 4-5 times.

So, all you need to is, run the script and you're all set!

[Download VB Script](#)

Method #5: Removing Shortcut Virus using CMD

Shortcut Viruses once entered in your PC, is then difficult to remove. It may inject into any of the files and create shortcuts.

It's better not to completely rely on a single method to remove it. Can't say, if it goes for temporary period and jumps in again!

So, here's another way to do it: **Removing Shortcut Virus using CMD.**

CMD, acronym for Command Prompt, is a command-line interpreter for Windows. It's a sort of compiler which processes your commands giving you an output (in this case, it is finding out and cleaning shortcut virus).

Steps to remove shortcut virus using CMD:

1. Plug your USB drive in PC.
2. Open **Start Menu** -> **Run**. (Alternatively, **Win + R** key combination). In the run dialog box, type **cmd**.
3. Copy the below code and paste it into CMD:

```
ATTRIB -H -R -S /S /D G:*.*
```

Note: You'll need to change the **G** letter of the code to your Pen Drive's letter. G was just an assumption (for the above example.)

The explanation of the above code:

Attrib specifies the attribute (as you might have guessed it)

-H is to unhide all the files on Flash Drive (which were hidden as shortcuts due to the virus)

-R is to create the files in your Pen Drive (recreate the shortcut files retrieving the original contents)

-S makes all the file on your USB drive not to be the part of system again (which makes it easy to do the process)

G is the Assumed USB Drive's Letter (you'll have to change it according to your Pen Drive / External HDD drive's letter)

Method #6: A Coded .bat File to Permanently Remove Virus

A bat file is an executable file which contains some pre-written script.

Just like the VBScript, it's made to do certain tasks, and in our case, it's removing the shortcut virus.

Steps to remove shortcut virus using bat file:

1. Open a Notepad File.
2. Paste the code below in it, and save it as with a .bat extension (Save As -> All Files -> .bat extension)

```
@echo off  
attrib -h -s -r -a /s /d G:*.*  
@echo complete
```

Note: Replace letter **G** with the Drive letter of infected removable drive at every instance.

Method #7: Removing Shortcut Virus from Registry

Shortcut virus once enters, spread quickly and multiplies!

So, this method is specifically to identify the virus in registry and if present, remove it.

Steps to remove shortcut virus by tweaking registry:

1. Open **Task Manager** by pressing **Ctrl + Shift + Esc**.
2. Click on the **Processes** tab, find **Wscript.exe**. If you find it, **select it** and then click **End Process**.
3. Open **Run dialog box** (Win + R key), type **regedit**. This will open the **Registry Editor**.
4. Navigate to **HKEY_CURRENT_USER / Software / Microsoft / Windows / CurrentVersion / Run**. Here, look for a registry key named **odwcamszas**, **right click** on it and **Delete** it.

Note: This doesn't always have to be the case. If you find the virus during the steps, then the shortcut virus has affected the registry and you must follow the steps above. If not found, skip this step.

Method #8: Config Tweaking to Remove Shortcut Virus!

Tweaking configuration is an alternative in which, instead of using software, search for virus and remove it.

So, following the below steps, if you identify the virus, you can directly remove it.

Steps to remove shortcut virus by tweaking config:

1. Open the Run box and type in **%temp%**. This will open the Temporary Files folder.
2. Search in that folder for **nkvasyoxww.vbs**. If found, delete it.
3. Again, open the **Run box** and type in **msconfig**. Go to **Startup Tab, disable nkvasyoxww.vbs** from there. (In Windows 8, open **Task Manager**, go to **Startup tab**, and **disable nkvasyoxww.vbs**)

Note: Again, chances are there, that you might not find the given processes and entries. In such situations, skip this step and move onto next one.

Method #9: Shortcut Virus Remover Tool

Shortcut Virus Remover is another powerful tool to remove the shortcut virus easily.

Using this software is quite easy. Follow the on-screen instructions and you're done!

A blue, rounded rectangular button with a slight gradient and a shadow effect. The text is centered and reads "Download Shortcut Virus Remover".

Download Shortcut
Virus Remover

Bonus: How to Prevent Future Injections of Shortcut Virus?

It's quite easy for a virus to get injected and hundred times harder to remove it!

This is what I'm trying to convince you about right from the beginning of this article!

It gets worse:

That same virus starts spreading all over to make you helpless and just get sick of it..

So, let's start with the best ways to tackle future virus injections:

1. **Using an antivirus:** If you are on a low budget or don't want to spend for an antivirus, there are excellent freewares out there like [Avast](#), [AVG](#), etc.
2. **Using an anti-malware:** A malware can be more destructive than a virus. Some antiviruses already contain anti-malware, but if not, you can try [Malware Bytes](#).
3. **Turning off Autorun for USB Drives:** When there's shortcut virus present in your USB Drive, autorun can spread that virus all over your PC. Thus, it's always better to turn off autorun. If you want to know how to turn off autorun, [here's an article from Redmondpie to do it easily](#).

Your Final Steps:

So, as you reached this far, I'm pretty sure that you might have already tried one of the methods listed above (if you're just scrolling through to know what's there in this eBook, go take action QUICKLY!).

Your final 2 steps: (will take just 30 seconds)

1. [Go over here and vote for the method that helped you to remove shortcut virus easily & quickly.](#)

(I'm running a survey to know which mentioned method helps people more. All of the method works, but differ greatly in different situations.)

2. [Quickly go here and leave your opinion. Which kind of shortcut virus did you encounter, how did you feel looking at it the first time & which method helped you to remove the shortcut virus.](#)

(This will help others encountering similar problem to yours.

Just take out a few seconds to leave a comment and you'll help others to solve a major problem!)