

How to Remove A Computer Virus – 5 Simple Steps

Learn how to remove a computer virus in 5 easy steps!



Illustration: [Gordon McAlpin](#)

So you've got a virus, and it's messing up your PC in multiple ways. You want to get it out of there, but it's not letting you download a antivirus application. Lucky you Googled and found this blog, right?

Here are the five steps you absolutely must take to escape the virus, hunt it down, and eliminate it. Think of yourself as the angry teenager that finally turns the tables on the monster and kills him dead.

1. REBOOT INTO SAFE MODE WITH NETWORKING

Stay alive! Most viruses become disabled in Safe Mode, which is a protected mode of Windows that's missing a lot of extraneous features. Windows Safe Mode With Networking will give you the opportunity to download and install a few antivirus applications, so you're sure to squash any issues your PC has.

To reboot into Safe Mode with Networking, click the Start Button, then Restart. As your PC starts up, tap on the F8 key. If the Windows logo appears, you didn't press it early enough, and you'll have to start over.

Click Advanced Boot Options, then Windows Safe Mode With Networking. Don't be alarmed when Windows looks different as it starts up ... that's just how Safe Mode is. You'll still be able to launch your browser and download things.

2. DOWNLOAD AND INSTALL ANTIVIRUS APPLICATIONS

Time to turn the tables! For the sake of simplicity, we're going to pick two free antivirus applications that each do an extremely thorough job.

The first is [Windows Security Essentials](#).

Once that's downloaded and installed, grab this one too: [Malwarebytes Anti-Malware](#).

3. RUN EACH OF THE ANTIVIRUS APPLICATIONS SEPARATELY

Go on the offensive! Run Microsoft Security Essentials and have it do a complete scan, then close it down and do the same with Malwarebytes. You don't generally want two antivirus apps scanning at the same time or even open at the same time, as they'll interfere with each other. One or the other application should nab the virus or viruses on your PC. You may be asked to reboot so the application can finish cleaning your PC.

4. USE ONE OF THE ANTIVIRUS APPLICATIONS AS A SHIELD AGAINST FURTHER ATTACKS

Protect yourself! After you've run a thorough scan, you should use Windows Security Essentials' built-in real-time protection. This will ward off most viruses before they have a chance to infect your PC. Don't have more than one real-time protection on from more than one antivirus application as, like with step 3, they'll interfere with each other.

5. BE CAREFUL WHAT YOU CLICK ON

The calls are coming from inside the house! The most common way of getting viruses is opening spam attachments in your e-mail. Use your e-mail program's spam filter, and don't click on anything in it. If someone sends you an e-mail forward, don't click on that either. Don't go to questionable websites. Stay safe, and you'll worry less.

Good luck, and remember, the virus isn't dead until it's dead!

