Downloaded malware? Try these fixes before factory reset!

Getting infected with malware is basically a given at some point; when it happens to you, follow these tips to save your malware-infected computer.

With billions of malware attacks every year, chances are you've been targeted more than once—maybe even a victim. Unfortunately, getting infected with malware is almost guaranteed at some point; when it happens to you, follow these steps to save your malware-infected computer.

Try to remove malware

One of the easiest and quickest ways to remove malware (though not 100% effective) is to perform a factory reset. The problem is that this is a pain, as factory resetting your computer will erase all of your photos, videos, passwords, and other important personal information, but it may not remove the rootkit or bootkit. Before you do this, try removing the malware by following these steps.

1. Disconnect from the Internet

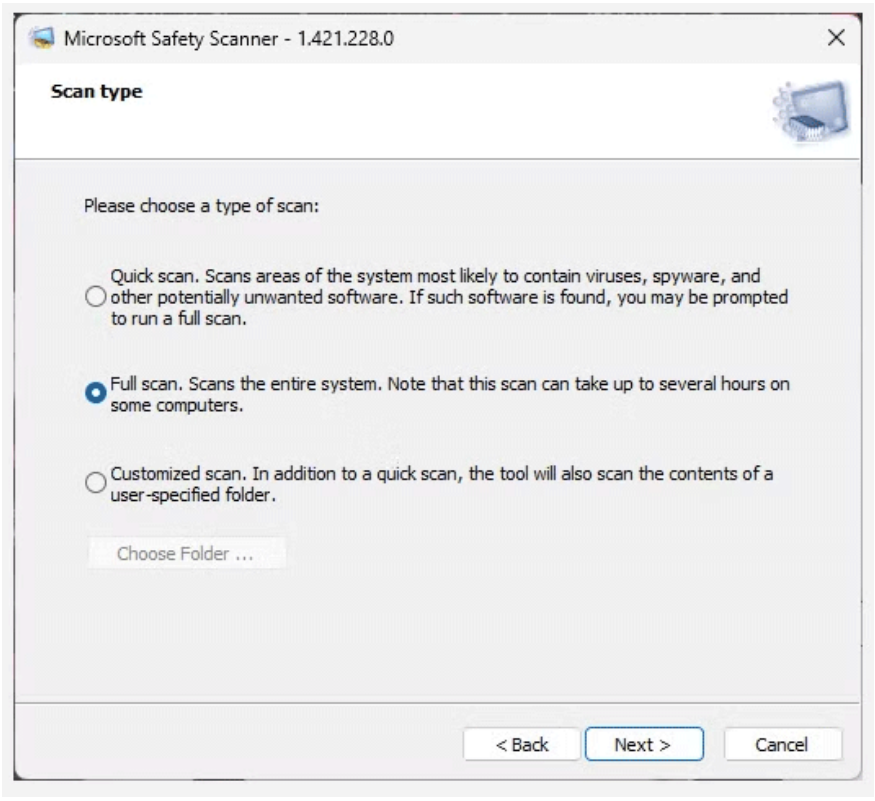
If you suspect your device is infected with malware, first disconnect it from the Internet. There are many types of malware, each with its own characteristics. Some malware, such as worms, must connect to the Internet to spread to other computers on the network.

Other types of malware communicate with command and control servers so hackers can remotely control your computer, while other forms of malware require an Internet connection to download more malware. For example, the Excel Remcos phishing malware requires an Internet connection to download the malware that contains its most dangerous attacks.

2. Start your computer in Safe Mode and scan for malware

Booting into Safe Mode is an easy process that only allows essential files and programs to run. Running in Safe Mode ensures that if your computer is infected, the malware in question will most likely not be able to run.

From Safe Mode, you can run a malware scanner like Microsoft Safety Scanner, which will scan all the files on your computer using the latest malware definitions. That's why downloading the latest version is important - you'll have the latest virus definitions, which means more malware will be detected.

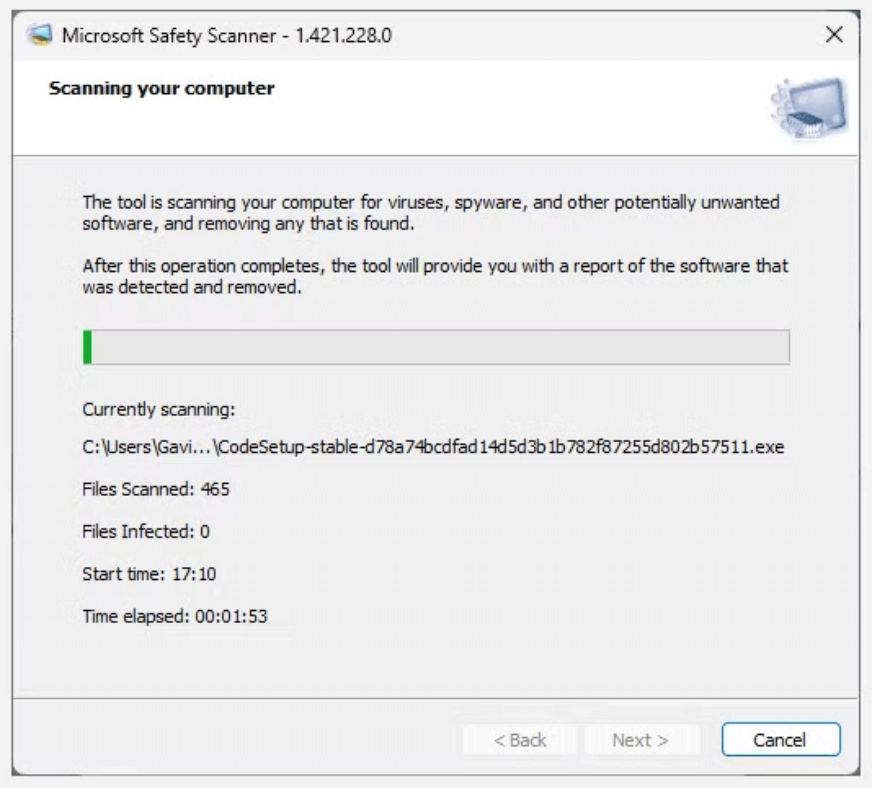


However, you will need to download Microsoft Safety Scanner (or another anti-malware suite) before entering Safe Mode and while still connected to the Internet. If you believe your computer is infected, download the program on another computer and put it on a USB drive, then you can run the program from the USB in Safe Mode.

Once Microsoft Safety Scanner is up and running, you can run a quick scan, a full scan, or a custom scan.

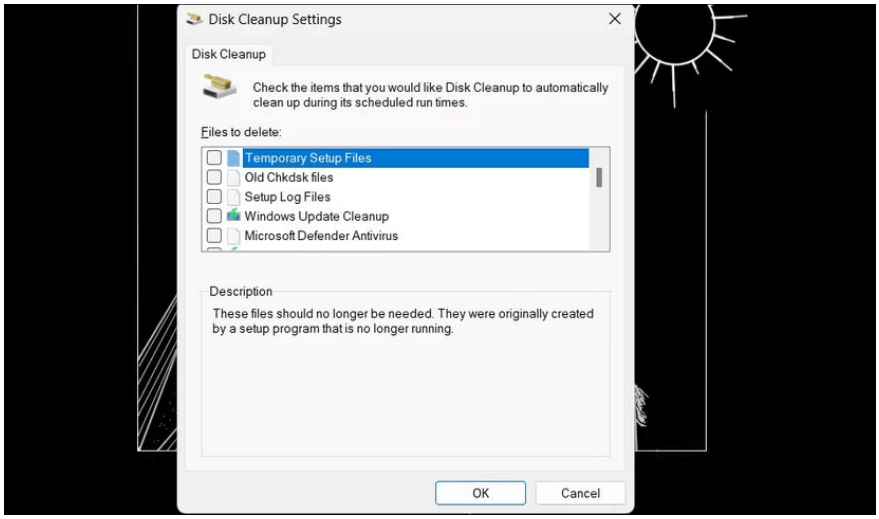
Of course, if you're not on Windows, you'll want to check out the best malware removal tools for macOS and Linux.

3. Remove suspected malware



Once the malware scanner runs, it will determine if there is malware on your computer. It will then allow you to remove the malware or remove it automatically for you. Even if the malware is detected and removed, you should still follow the steps to remove any remaining malware just to be sure.

4. Delete temporary files and browser cache



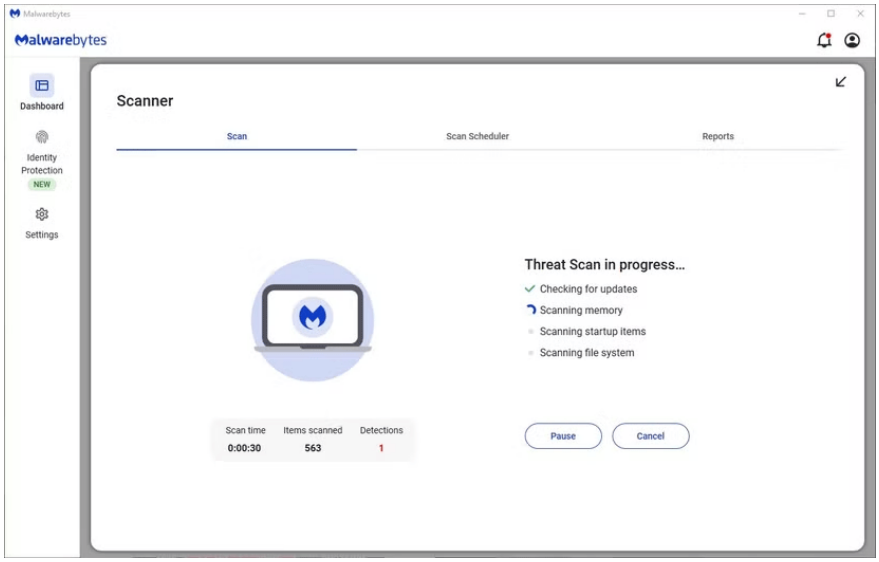
Malware doesn't always hide in plain sight. Computer scanning tools may not detect every piece of malware on your computer. You may need to dig a little deeper to remove an infection from your system.

The Disk Cleanup tool on Windows can quickly delete temporary files. Most temporary files can be deleted without any problems, but if you're worried about a particular file, you can run an Internet search for that file on another device.

To run Windows Disk Cleanup, type **disk cleanup** into the Start menu search bar, then select the best match. From here, you can select the files you want to delete, in this case **Temporary Files** and **Temporary Internet Files** . Doing so will delete any malware installation files if they're lurking there.

You should also clear your browser cache. To do this, go to your browser settings and select the option to clear your browser cache. Doing so will log you out of any services you are logged into, so be prepared for that. However, it is better to log back into your Internet service than to risk potentially dangerous malware.

5. Rerun the virus scan

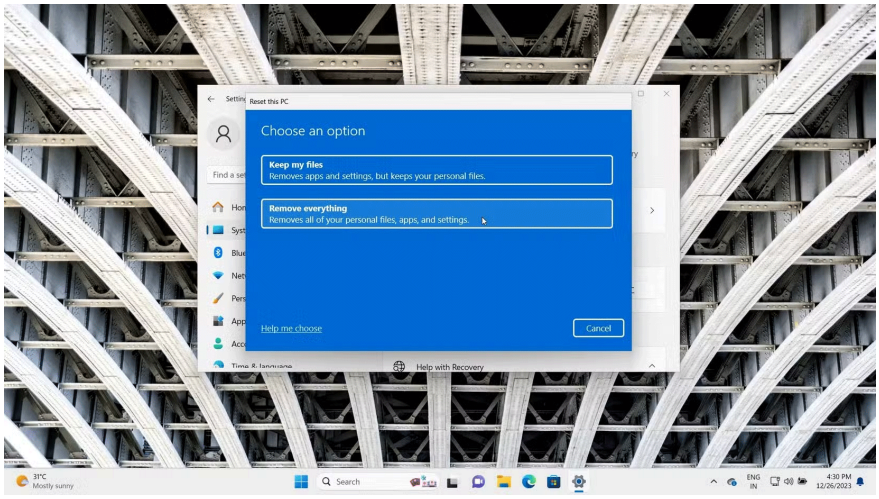


Now, reboot your system and run the malware scan again. If the second scan is okay, you're probably safe and have successfully removed the malware from your system. However, if it finds malware again, you may be dealing with dangerous, persistent malware and should seek professional advice on how to remove it.

Unfortunately, malware scanners don't catch all malware. With thousands of new malware variants being discovered every day, it's possible that your malware scanner won't catch everything. If you've done everything on this list and are still concerned that your computer is infected, you can always choose to perform a factory reset.

In that case, you should consider using a different malware scanner for the second scan. For example, if you used Microsoft Safety Scanner the first time, you should use Malwarebytes Premium for the second scan. However, like the first virus scanner, you'll want to download this scanner on another device, then transfer it using a USB drive.

Restore factory settings



If you are still concerned that malware may be lurking on your device, you can choose to factory reset your device. Doing so will completely erase your computer, including any files and data that may have been infected. If you choose this option, consider backing up important files before wiping your computer.

However, backing up a computer you suspect is infected with malware will transfer the virus to the backup. Restoring the backup may reintroduce the malware to your system. Malware is unlikely to hide in your personal files and folders, such as documents and photos, so backing up and running a thorough scan is usually enough. However, you should run multiple antivirus scans before considering copying it back to your primary (malware-free) system.

Refer to the following 2 articles for details on how to do it: