

## [5 Signs to Tell If Your Computer Has Been Hacked](#)

Computers have become an indispensable part of our lives. They might have made life easier for us but they come with their own set of problems and hacking might be the biggest one. There are a number of threats that come with hacking, like hijacking of accounts and passwords of social media accounts, identity theft to stealing your personal and credit card information.



*Some signs to look out if you suspect your computer has been hacked are:*

### [#1. Website Auto Redirects](#)

Few things are more annoying than trying to reach a website and then you're automatically redirected to another. Hackers love to do this because it potentially is a big money maker. Usually you'll see this when you type keywords into a search engine and you get a list of results. Click on one of them and instead of being taken to that website, you're taken somewhere else. This probably means that your system is compromised.

### [#2. Unknown Software Installs](#)

Malware has changed over the past few years. Initially all you had to deal with was computer viruses but malicious software has today evolved themselves into malicious Trojan viruses and worms that install themselves as legitimate programs. This makes it very hard for you to determine real and fake programs. These programs steal data and sensitive information from your computer. You should also be careful while installing new software. Use control to uninstall any rogue software programs that would harm your computer.

### [#3. False Antivirus Messages](#)

If you've been receiving warning messages about an antivirus on your system, your computer may be hacked. These are fake messages and are a surefire indication of a hack. This message may redirect you to a professional appearing site offering you to purchase antivirus software. Do not enter any financial information on this site. This may lead to you handing out your credit card information to the hackers. If this happens immediately turn off your computer and restart it in *safe mode* and attempt to uninstall any new loaded software. Then carry out a full virus scan with the goal of removing any remaining viruses.

#### *#4. Unwanted Browser Toolbars*

This is one of the most common signs of exploitation. Let's say your browser has multiple new toolbars with names that indicate the toolbar is supposed to help you, but you never installed it in the first place. Unless the toolbar is from a reputable vendor, it's time to dump the bogus toolbar. Most browsers allow you to review active toolbars. Remove any you didn't want to install. If the bogus toolbar isn't listed and you can't remove it, reset your browser back to its default settings.

#### *#5. You Cannot Log Into Your Accounts*

You've double checked and still can't login. Weird, right? Well this is a pretty obvious sign that someone else has the keys to your computer. This can be a very serious situation when your credentials for an account refuse to work. This can be for your emails, social media, bank accounts or even your computer. You should immediately initiate a password reset and change your password. If you can, you should also enable two-factor authentication. This has been proved to be a very effective way of preventing hacking.

Concluding it all up, it's advised to practice safe browsing techniques and to avoid anything dodgy that comes up on the internet.