

Click to verify

































are several common indications that your computer has been hacked, dmaricrucio/ty ages This story is available exclusively to Business Insider subscribers. Become an Insider and start reading now. You can tell your computer has been hacked if you see frequent pop-up messages, mass emails sent from your account, or unexpected programs appear. If your computer has been hacked, you run the risk of losing data, having your identity stolen, or suffering financial losses. Here are seven signs that your computer has been hacked and five steps you can take to prevent hacking. Computer hacking doesn't only happen in the movies. Unless you take precautions and make your computer's security a priority, it's possible you can get hacked, which can result in lost or stolen data, ID theft, and worse. But what does getting hacked actually look like? The signs might be subtle, but they're often easy to identify. You might find unexpected changes to your computer, slow performance, and an increase in unwanted behavior like pop-up windows. Here are seven of the most important signs you've been hacked, as well as tips on how to protect your computer from getting hacked. Common signs of a hacked computer There's no single set of signals that you've been hacked, mainly because there are a lot of different ways you might be attacked. Here are seven signs that your computer has been hacked, as well as tips on how to protect your computer from getting hacked. 1. Unexpected pop-up messages and redirects. If you see frequent pop-up messages, mass emails sent from your account, or unexpected programs appear, it's a sign that your computer has been hacked. Computer hacking doesn't only happen in the movies. Unless you take precautions and make your computer's security a priority, it's possible you can get hacked, which can result in lost or stolen data, ID theft, and worse. But what does getting hacked actually look like? The signs might be subtle, but they're often easy to identify. You might find unexpected changes to your computer, slow performance, and an increase in unwanted behavior like pop-up windows. Here are seven of the most important signs you've been hacked, as well as tips on how to protect your computer from getting hacked. 2. Slow performance and frequent crashes. If you notice a significant decrease in your computer's performance, or if it crashes frequently, it could be a sign that your computer has been hacked. Malware is typically buggy and inefficient, which can lead to poor performance and lots of crashes. Changes to your web browser: Did your web browser's home page change without your permission? You might be hacked. Also, watch out for unexpected browser toolbars, plugins, and extensions, as well as a sudden increase in the number (and kind) of ads that your browser displays. Any of these are signs that you've lost exclusive control of your computer and hackers are installing malware in your browser. Unusual webcam activity: Your webcam has a status light that comes on when it's in use. If you see your webcam come to life unexpectedly — such as when you are not using any web chat software — it probably means you've been hacked. Criminals may turn on the camera to see if you can read passwords as you enter them on the keyboard or access other personal information. How to prevent your computer from getting hacked Even though there are serious risks from hackers, a few common sense and simple precautions can protect you from hacks like these. Keep your operating system up to date: Make sure you're running the latest version of your operating system. Windows, macOS, and Linux all have security updates that patch vulnerabilities. If you don't update, you're leaving your computer open to attacks. Use strong passwords: Create strong, unique passwords for all your accounts. Use a password manager to help you remember them. Enable two-factor authentication: This adds an extra layer of security to your accounts. If you're hacked, the hacker will need your password and a second factor, like a text message or a security key, to access your account. Be cautious of phishing emails: Phishing emails are designed to trick you into giving up your personal information. Don't click on links in suspicious emails, and don't provide your personal information to anyone who asks for it. Use antivirus software: Antivirus software can help protect your computer from malware. Make sure you have it installed and that it's up to date. Backup your data: Regularly back up your important files to a secure location. This way, if your computer is hacked, you won't lose your data. If you see any of these signs, it's important to act quickly. Here are five steps you can take to prevent hacking: 1. Update your operating system and software. 2. Use strong, unique passwords and enable two-factor authentication. 3. Be cautious of phishing emails and suspicious links. 4. Use reputable antivirus software. 5. Backup your data regularly. If you're concerned that your computer might be hacked, there are several steps you can take to investigate and protect yourself. First, run a full system scan using your antivirus software. If you find any malware, remove it immediately. Next, check your account settings for any unauthorized changes. If you find anything suspicious, change your passwords and enable two-factor authentication. If you're still unsure, consider consulting a professional cybersecurity expert. Remember, staying vigilant and taking proactive steps can help you protect your computer and personal information from hackers.