Click to verify



```
There are several common indications that 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, sudden 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 ways you might be attacked. Here are seven
ways to tell that you might have been hacked. Watch for pop-up messages and antivirus warnings Pop-up windows warning you about viruses and malware attacks sound helpful in principle, but be sure you're seeing an authentic message from the antimalware software you actually have installed before responding to or acting on its
recommendations. The reality is that many of these messages are evidence that your computer has been hacked — infected with malware that's masquerading as antivirus software. If you see any kind of unexpected warning message, don't click. Instead, close your web browser and run your computer's antimalware software to look for the presence
of malicious software. Unauthorized email sent from your account One common goal of hackers is to infect as many computers as possible. One way to do that is to take control of email apps and email services, and use them to send infected email messages to as many people in the hacked address book as possible. A serious signal that you've been
hacked: hearing from friends and colleagues that they've received spam from your computer than you regularly use. Your computer than you regularly use that there are more programs installed on your computer than you regularly use. Your computer than you regularly use.
unexpected apps running when you start your computer, or you see new programs in the taskbar or notification tray, then it's likely you've been hacked or infected with malware, and these unknown programs are performing malicious acts on your PC. You can inspect the list of startup apps on your computer to see if there are any new or unexpected
ones installed. Dave Johnson If the uninstaller does not work or you can't otherwise remove these unknown programs, there's a very good chance your computer has been compromised. Password and access changes to apps and services In most cases, you should get an email or text message notification when your password or access settings change
for common online apps and services — especially banking and other financial services. If you get emails notifying you about changes to your account settings that you've been hacked. Contact the financial institution or other service to see if you still have control of the account. Be very
careful, though. A common phishing trick involves sending a fake email about a password reset or some other account change. If you click a link or call the phone number in the message, you could be reaching out directly to the hackers, who will milk you for personal information and possibly get enough information to hack your account for real.
When you follow up on a possible hack, always contact the service using an email or phone number you have found in the service's app or on its website. Slow performance and frequent crashes As your computer ages, it often starts to feel like it's running more slowly than when you first brought it home, whether because Windows slows down or the
hard drive fills up and doesn't access data as efficiently. But if your computer suddenly starts acting weird — it slows down, crashes frequently, seems to get hotter than usual while running — then that might be a sign that your computer has been hacked and is running malware. Malware is typically buggy and inefficient, which can lead to poor
performance and lots of crashes. Changes to your web browser browser browser browser 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 activity Your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see your webcam has a status light that comes on when it's in use. If you see you have a status light that you have a statu
may turn on the camera to see if they can read passwords as you enter them on the keyboard or see 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 hacker like these. Keep your operating system up to
date. First and foremost, make sure that your computer is operating system is up to date. Modern PCs and Macs install automatically, so make sure you don't pause, disable or interrupt that process. For best results, don't power off your computer after hours; put it to sleep so updates can install automatically when you are not using it. Check
your computer to make sure all the latest OS updates are installed. Dave Johnson Run antimalware software that comes with Windows or
XProtect for the Mac, you should be adequately protected. Always use strong passwords. When you create accounts for apps and services, always use strong passwords. That means not repeating the same passwords on multiple accounts for apps and services, always use strong passwords.
login info to get into your banking app. And a strong password is a long string of numbers, letters, and symbols. Implement two-factor authentication (2FA). No matter how good your password is a long string of numbers, letters, and symbols. Implement two-factor authentication (2FA).
your account without having physical access to the device (like your phone) that you use for authentication. Any kind of 2FA is good, but using an authenticator app that generates one-time codes every time you want to log in is especially secure. Use two-factor authentication with an app like Authy to ensure you can't get hacked using a username and
password alone. Dave Johnson Don't use public or unsecured WiFi. Most public WiFi networks are unsecured while you're online. Avoid using public WiFi networks are unsecured while you're online. Avoid using banking and
financial services. Dave Johnson Freelance Writer Strange device behavior, unexplained account lockouts, password reset request emails, and unauthorized financial transactions are all common signs indicating that you've been hacked. While hackers can trick you into downloading malicious software that gives them access to your computer,
iPhone, or other devices, it's more likely that your accounts were hacked through no fault of your own. In 2024 alone, cyberattacks and data breaches have exposed the sensitive personal information and passwords of nearly 1.25 billion victims [*]. It's critical to be able to recognize the warning signs of a hack so you can react quickly and protect your
accounts, finances, and identity. Protect your devices and identity for as little as $3/month. Aura combines award-winning identity and credit monitoring with advanced antivirus and digital security tools. Download Aura today. {{show-toc}} How To Tell If You've Been Hacked: 12 Warning SignsCybercriminals can hack your devices and accounts in
many ways — via phishing emails and text messages to tech support scams, compromised public Wi-Fi networks, and credential-stuffing attacks. The signs of a hack ultimately vary depending on the type of attack, the hacker's intent, and the security measures you have in place. These are the most common warning signs to look out for: 1. You can't
access your online accounts (or they look different) Any changes to your online accounts or your ability to access them are clear warning signs that you've been hacked. Specifically, you should watch for: Sudden logouts from your social media, email, or online banking accounts Passwords that no longer work when you try to log in Unexpected emails or
texts about login attempts, password resets, or two-factor authentication (2FA) codesChanges to your settings, back-up account details, or security questions Related: What To Do If You Were Hacked (How To Recover Hacked Accounts) → 2. Suspicious or unusual activity in your email or messaging appsHackers who gain access to your accounts often
use them to target your contacts and spread malware or scams. "White hat" hacker Ash Shatrieh warned users to watch out for new messages that don't trigger corresponding notifications [*]: "This could be an indication that hackers have set up rules which can divert or hide emails from your inbox, suggesting that the hacker may be selectively
releasing certain messages while concealing others."Keep an eye on your email and messaging activity for signs of a compromise, including: Strange emails, especially those containing threats or extortion attempts Friends or family members telling you they've
received odd messages from your email or social media accounts Related: How To Tell If Your Facebook Account Has Been Hacked →3. Notifications alerting you that your data was part of a data breachIn April 2024, a cybercriminal group known as USDoD posted a database entitled "National Public Data" on a Dark Web forum, which exposed nearly
three billion records from 170 million victims [*]. If you receive a data breach alert from a service you use, take it seriously. While a notification doesn't necessarily mean that you've been hacked, it does mean you're at a higher risk of being targeted. Look out for emails, alerts, or news about data breaches related to your accounts, update any leaked
passwords, and actively monitor potentially compromised accounts. Many password managers (including the one included with every Aura plan) can also warn you if your passwords were part of a breach or are at risk of being compromised. 4. Strange device behavior or performance Malware and other viruses can seriously impact the performance of
your devices — such as by causing them to run more slowly, heat up, or make strange noises. Pay attention to any sudden changes to how your devices are operating, including: Devices that suddenly slow down, crash, overheat, or run low on battery more frequently Unfamiliar browser plugins, add-ons, or toolbarsApps that open on their own,
requiring you to keep closing or quitting them repeatedly5. Unauthorized control of your deviceSome types of malware (or even legitimate software such as AnyDesk) allow hackers to take control of your device remotely. If hackers breach your emails,
and even steal your money. On Reddit, a user reported seeing activity on his computer when he awoke at 3:00 a.m. [*]. Watch for your cursor moving on its own when you're not touching the mouse or trackpad. Another red flag is if your webcam light turns on unexpectedly, even when you're not using it for video calls or recordings. Related: Do
Hackers Have Remote Access To Your Computer? Do This! →6. Missing money or unrecognized transactions or changes to your credit reports indicate that you've been hacked or
have had your identity stolen. Be on the lookout for: Unfamiliar charges on your credit card or bank accounts from your cryptocurrency wallet, or suspicious emails that appear to be from crypto platforms like Coinbase Strange inquiries, accounts, or changes added to the personal information on your credit reports 7. Someone's
impersonating you online (especially with work contacts) Hackers may use your stolen information or access to your accounts to scam your professional contacts or impersonate you online. In April 2024, a 58-year-old former hospital employee was charged with stealing another man's identity. Matthew David Keirans used William Woods' information
for everything from bank accounts to car purchases for over 33 years. When the real William Woods tried to convince authorities he was the victim, the police didn't believe him and sent Woods to a prison and then to a mental institution [*]. Be alert if business partners or potential clients mention strange interactions they've had with "you" on
platforms you don't use. Also, watch for signs that someone is using your identity to apply for jobs, loans, or submit insurance claims in your name. Shut down hackers fast. If you've been hacked, your bank account, email, and other online account, email, and othe
as $3/month.8. Ransomware attacksRansomware notices are among the more obvious signs that you've been hacked. Scammers use this aggressive form of malware to lock you out of your system and encrypt your files until you pay a ransom. While ransomware has typically been used to target valuable companies, hackers can also use it against
mobile devices and individuals. An Android malware called BingoMod masks itself as trusted apps on Google Play — even going so far as to use the same icon as the free AVG AntiVirus & Security tool. If you download this program, it can take control of your device, before stealing login credentials, intercepting SMS messages, and taking screenshots
[*]. Watch out for any app that requests permission to use Accessibility Services. If you see a pop-up claiming your data is encrypted and demanding a ransom, your device has likely been infected with ransomware.9. Your antivirus or anti-malware software to
maintain access to your devices. A woman asked for help on Reddit after her device was infected with a Trojan horse virus. The virus enabled the hacker to add 5,000 followers to the victim's TikTok account and pay for ads through her Facebook account [*]. Malware, such as trojan horses, can evade antivirus programs. If you notice your antivirus
software has been turned off without your knowledge, it could indicate a breach. Always ensure that your security software is up to date and running. Related: How To Remove Viruses From Your Computer (Mac and PC) →10. Unexpected pop-ups and redirects Adware is a type of malware that triggers pop-ups, redirects you to scam websites, or
changes your browser and app settings — such as by changing your default search engine or homepage. In July 2024, Dark Reading revealed that a program approved and signed by Microsoft was actually a dangerous form of adware [*]. Instead of removing ads from your device, HotPage opens the door to more ads and malware by intercepting
traffic and manipulating content in web browsers. You can spot adware when you see a sudden increase in pop-up ads, especially those claiming your device is infected. Also, take note if you're being redirected to unwanted websites or if you see new tabs open automatically behind your browser window. 11. Identity theft and fraud Sometimes, the signs
of hacking extend beyond your devices and into the real world. Hackers often sell stolen personal data on the Dark Web, which can cause you to become the victim of identity theft. In some instances, the thief is a family member with easy access to all of your personal information — like the case of a Redditor whose dad took out a $25,000 loan in his
name and defaulted on the payments [*]. Watch for unexplained credit inquiries, unfamiliar accounts opened in your name, or debt collectors contacting you about loans you didn't take out. Related: 25 Warning Signs of Identity Theft You Need To Know →12. Strange social media activitySocial media accounts are valuable targets for hackers looking
to gather personal information or target vulnerable people with scams. Regularly review your social media activity for unfamiliar posts, messages, and friend requests sent from your account without your knowledge. You should also keep an eye on your list of trusted devices or logged-in devices — regard any unfamiliar additions that you see as red
flags.Do You Think You've Been Hacked? Do This Now!If you've been hacked, speed matters. As soon as you see any warning signs, take action to secure your devices from the internet. If your device has been hacked, it could infect others connected to the same network. When you see
signs of a hack, turn off your internet connection to minimize damage. You can disable Wi-Fi on individual devices to make sure they don't automatically reconnect. Freeze your credit freeze with each of the three major credit bureaus (Experian, Equifax, and to make sure they don't automatically reconnect.
TransUnion). This will help prevent hackers from opening new accounts or taking our loans in your name. Scan for malware, and delete unfamiliar apps. If hackers have tricked you into downloading malware or spyware, it could give them "backdoor access" to your accounts — even after you change your passwords. Use antivirus software to scan for
hidden malware, or delete any unfamiliar or new app that could be infected. Recover a hacked accounts. Most platforms have specific steps for account recovery. Search online for: "how to recover a ccess to hacked accounts with Google, Facebook,
Apple, Microsoft, Twitter, Instagram, LinkedIn, TikTok, Snapchat, or Dropbox. Update your passwords for all of your accounts, especially those that were compromised. Create unique passwords for all of your accounts, especially those that were compromised. Create unique passwords for all of your accounts, especially those that were compromised.
password manager for easier access. Enable two-factor authentication (2FA). Adding an extra layer of security can prevent unauthorized access even if your password is compromised. Enable 2FA on all of your important accounts, particularly email, banking, and social media. The best method to use is an authenticator app instead of SMS to receive
more secure 2FA codes. Warn your contacts that you've been hacked. Hackers often use compromised accounts to spread malware or scams. Alert your friends and family about the hack, and advise them not to open any suspicious activity
Hackers may have accessed multiple accounts. Review your account activity logs across all platforms for any unfamiliar logins or devices. Pay special attention to financial accounts, email, and social media. If you spot anything suspicious, secure those accounts immediately. Update your operating system and apps. Ensure that all of your devices are
running the latest versions of their operating systems and applications; otherwise, hackers can exploit vulnerabilities in outdated software. Here's how to update Windows, macOS, iOS, Android, and Linux devices. Factory reset your device. Even after running antivirus software, you may still deal with deeply rooted malware. As a last resort, you can
factory reset your device and reinstall your operating system to completely wipe persistent malware. Here's how to do this on macOS and Windows. Proactively protect yourself against hackers. Aura's all-in-one digital cybersecurity solution can help safeguard your devices and data against malware, ransomware, and other cyberattacks. Plans start at
just $3/month. How To Protect Yourself From Being HackedWhile you can be hacked by no fault of your own, there are still precautionary measures you online, the harder it will be for hackers to target you. Here are five ways to
information. Enter fake information when signing up for online services. You should never enter false information for anything official, like your taxes or police reports. However, you can be more guarded with your sensitive data on retail sites, surveys, apps, and email newsletters. If any of these companies suffer a data breach, hackers won't be able
to target you as easily if your profile has an incorrect date of birth or old phone number. Tighten your profile. Without open visibility of your location tracking, photos, and content, hackers won't be able to glean information from your profile to target
you with phishing scams. Remove your personal data from Google searches and data brokers collect and sell your personal information, which can be exploited by hackers. Opt out of these services by contacting major data brokers directly or by using a data removal service. Beware of shoulder surfing. Pay close attention to your
surroundings when logging in to sensitive accounts or unlocking your phone — as hackers can watch you enter your phone in to sensitive accounts or unlocking password, and even your devices. It's much easier and safer to take a
proactive approach to digital security by downloading a dedicated cybersecurity platform. With Aura, you get advanced antivirus protection, a military-grade virtual private network (VPN), secure password manager, robust identity and credit monitoring, 24/7 U.S.-based support, and more. It's not a secret that hackers don't make victims aware of the
fact that they have hacked. And that's not without reason. This might sound obvious, but just because everything "seems to be fine" doesn't mean that's actually the case. Hackers create is hidden in a system to do the work, and hackers are not all
about rushing it. That means that they can come back at any given moment to see if the malware was able to do any damage to a system, and to see what other things they can do to it. For that reason, you might not realize a hacker is always
better to be safe than sorry, so I decided to create an overview of 12 signs that don't lie that you've been hacked. If any of these signs are familiar to you, it's fair to say that you're a victim. So, let's get to it. Here are 12 signs that should trigger all of your alarm bells. Constant and Random Browser Pop-ups Constant, frequent, and random browser
pop-ups are a common sign that you've been hacked. Especially if you receive random pop-ups while browsing websites out there that, for some reason, can easily bypass ad-blockers and show unwanted pop-ups. Obviously, such
websites are not legitimate sources to determine whether your device has been hacked. If this unexpectedly happens while browsers offer pop-up blocking, so be sure you have it turned on in your browser's
settings. There are also browser extensions that offer pop-up blocking, Be aware, however, that blocking pop-ups may cause some sites to not operate properly. Also, make sure you have antivirus and anti-malware installed on your computer. Scan for malware or viruses, as these can cause pop-ups. Browser Toolbars Installed Without Your Knowledge
Image Source If your browser is suddenly showing toolbars you don't recognize and clearly didn't install, it's almost certain that your computer has been compromised. Unwanted toolbars you don't recognize and clearly didn't install, it's almost certain that your browser settings and, for example, change your standard homepage to a spammy website. Additionally, these
toolbars can open the door to other malicious files and open ad windows without your permission. Is this happening to you? If so, it's time to get rid of these annoying toolbars. The longer you let them sit in your toolbar, the higher the chance other malware will nest itself in your system. It's not unusual to have a new toolbar in your browser after
your browser settings. Also, install the latest versions of antivirus and anti-malware or viruses, as these can install toolbars. Installation of Unwanted & Unexpected Software Image Source Similar to unwanted installations of browser toolbars, it's a clear sign that you've been hacked if software automatically
installs itself without your consent. It's highly likely that these software programs can control or modify other software programs installed on your system. The worst-case scenario is that it could modify or disable your antivirus, allowing other types of malware to flood into your system. There are quite a few software tools that install additional
sure to read the license agreements before installing software, and during the installation. What Should I Do? Click "Cancel" first. Then, make sure you are using the latest version of your browser. Also, make sure you have antivirus and anti-malware installed on your
computer. Scan for malware or viruses, as these can try to install unwanted software. Auto Redirect to Unwanted Websites redirect users to these sites, so once a user opens a URL, it will automatically redirect them to a different website without their
permission. This could also happen without the site owner's consent, so they don't actually realize that hackers are forcing the clicks. What normally happens is that you enter a string of keywords in the search bar and, regardless of what URL you click on, the malware in your system will redirect you to another website (which had nothing to do with
what you searched for). You can perform a test by searching for a very specific term and clicking on the first URL to appear. Then, if you're being taken to a completely different site, you wanted (the one
you should actually see in your browser), you're not actually on that site. So, you won't even be aware of the fact that you're not actually on that site. So, you won't even be aware that your internet search was redirected through the use of a proxy. That means that the returning URL is well hidden from you, tricking you into thinking you're on the page you
intended to be on. What Should I Do? Make sure you are using the latest version of your browser. Also, make sure you have antivirus and anti-malware installed on your device. Scan for malware or viruses, as these redirects can include malicious payloads. In addition, if possible, contact the owner of the infected website so that they can attempt to rid
their website of the malicious redirect code. Fake Protection Alerts Image Source A fake warning message by your antivirus software - or any other protection software or old programs in your browser toolbars to take over your
entire system and send out fake warnings. When you get such a message, you can be sure that the damage has already been done and your system is infected. The strategy behind this type of hacking is to have users click on the URLs in the fake message, which will redirect them to websites that appear to be legitimate and trustworthy, which are
(supposedly) offering protection software. This is where the real damage happens. Hackers trick people into buying fake software, while at the same time entering their credit card and personal information on the website - which falls right into the hands of the hackers. Now, you might think: who would fall for that? But you'd be staggered by how
many people take the bait. At this point, the hacker will have control over your entire system - and worst of all, access to your browser window where the "warning" appeared. Then, make sure you are using the latest version of your
browser. Always have antivirus and anti-malware installed on your device. Make sure your malware or virus detection app is updated to the latest version, then scan for malware installed on your device. Make sure your malware or viruses. If you know that the website is on the up-and-up, contact the owner of the website so that they may rid it of the malicious code causing these fake warnings. You
See a Random Message that Your Files Have Been Encrypted One of the most vicious and recent ransomware attacks was WannaCry. Hackers used this extremely aggressive form of malware to hack Windows computers worldwide. The malware takes complete control of your system and locks it down - in other words, you won't be able to do
anything on your PC anymore. As shown in the image, ransomware attackers ask for a "ransom" to unlock your data. In this recent example, they demanded $300 worth of Bitcoin as payment. Also, a timer, located in the box on the left, is counting down. If you do not pay the ransom, the hackers will permanently delete all your data - which is often
unrecoverable. What Should I Do? Most importantly, don't freak out. This may be a fake ransomware notification. Even if it's real, you may still have recovery options, such as restoring from a backup. For more information about what to do if you experience a ransomware attack, and also how to prevent such happenings, read my article,
Ransomware: What Is It And How Can You Prevent It? Social Media or Skype users have been introduced to the phenomenon of receiving weird messages (often containing some kind of a URL) from a friend or a person on their contact list. Generally, the hacker is using your
account to send out a message to all of your friends with either a link that will instantly start the download of a malicious site. It could be a standard message to increase the likelihood of someone clicking the link.
Either way, this is a clear sign your system or social media accounts have been hacked. What Should I Do? Immediately change your password to a strong, secure password that you're not using for any other account. If you have reused the password on other accounts, immediately change those to a non-duplicated secure password. Also, scan your
computer or mobile device for malware or viruses. Unexpectedly Invalid Password(s) If you attempt to log in to a platform or website (which you use regularly - so you are sure that your account has been compromised. Note: It could also be that
the site is dealing with temporary technical problems that disabled the login form. However, if you are absolutely sure that you've entered the correct login details - and the site is not experiencing technical problems - and it's no longer working, then it's highly likely that someone stole your details and changed the password. Phishing emails might be
the culprit of login issues. Such scams usually redirect you to a look-a-like page where you enter your account details, but unknowingly present the data to a hacker on a golden platter. What Should I Do? Follow the platform or website's password resetting procedures and set up a new unique and secure password. Also, if available, set up two-factor
authentication on the platform or website. This will ensure that you will know when someone has attempted to access your account, as it will foil their login attempt and may also notify you of login attempts by asking you for an additional bit of information before allowing the login. Randomly-Moving Mouse Pointer A moving mouse pointer is a sign
that you've been hacked, though it could instead be that you're suffering from technical issues. There's an important difference between the two scenarios, though. If the mouse cursor is randomly flying all over your screen without a clear path of direction, it's most likely caused by a glitch or a technical problem. In the case that the mouse cursor is
making clear movements and systematically opening software tools or other programs, you can be sure that someone else has full control. This person is controlling your computer to become inactive and then strike. While you're asleep, someone is
using your computer to do whatever they want. What Should I Do? Before panicking, make sure your mouse sensor and the surface it uses for tracking are both clean. Dirty mouse sensors and desk or mousepad surfaces can often cause your mouse pointer to think it is being moved around. Also, if the surface the mouse sits on has a "busy" design, try
using the mouse on a solid color desktop surface or mouse pad. Busy designs can confuse the mouse, causing it to move randomly. It's when you see your mouse pointer moving purposefully, opening applications and files, closing windows and other usually "user-related" actions that you will want to worry. If you have recently used TeamViewer or
another remote control app, check to make sure it isn't still connected. The user on the other end may be screwing with your mind as a joke. If none of the above seems to be what's causing your drunken mouse actions, turn off your internet connection momentarily by turning off your computer's WiFi connection or unplugging its Ethernet
connection. This will disconnect from any outside control of your mouse. If you regain control, that means an outsider is controlling your mouse. Make sure your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware software and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running the latest version of antivirus and anti-malware and scan your computer is running to the latest version of antivirus and anti-malware and anti-
Protection & Task Programs Image Source The most advanced viruses can potentially disable your antivirus software. The only option wouldn't be able to open either of these two programs, as they
might also be disabled. Such kinds of viruses are extremely dangerous, as your computer is basically completely vulnerable to any type of malware and hackers. Disabled protection software is a crystal-clear sign that you've been hacked, and immediate action is required to restore a secure environment. What Should I Do? If your antivirus or anti-
malware apps will not run, visit an online scanner in your browser. eSet, Trend Micro, F-Secure and other antivirus and malware vendors offer free online virus and malware scanning services. Your Financial Account Is Missing Funds If you lose money without transferring funds yourself, it's a clear sign that someone hacked into your device and
compromised your bank account. I wouldn't be surprised if the hacker was able to transfer all of your funds to a different account or make purchases on a website. These situations are often triggered by phishing emails, which I also mentioned in a previous section. Note: The loss of funds on your credit card statement could be because of different
reasons. For example, entering your credit card information on the wrong website could result in one of the bad guys using your details to make other payments. That doesn't necessarily mean that your device or bank account itself has been hacked. What Should I Do? Immediately contact your financial institution to inform them about the activity or
your account. They may be able to help you recover the stolen funds. Also, immediately change the password on that account, and any credit or debit card connected to the account. In addition, make sure to change the password on any account that may be withdrawing funds from the account. Make sure all of your passwords are unique and secure
A password manager can help you create, maintain and recall unique passwords on all of your accounts. Unexpected Goods Shipped to an Unknown location, it's clear that someone has hacked your account on a platform where you saved
your payment information. The hacker used your payment information and personal details to ship the items. Clearly, the person who hacked into your account changed the shipping address. In addition, another sign that this has happened is if you have credit funds on a website and you suddenly receive a message that you ran out of funds, yet you
didn't order anything. Unfortunately, you would probably only be notified after the damage had already been done. What Should I Do? If the unexpected shipment was from an online merchant that you have an account with, immediately contact customer support - they may be able to help you track the shipment and possibly recover your funds. Also
change the password on your affected account and on any other accounts that might use the same passwords are unique and secure. As mentioned previously, a password manager can help you create, maintain and recall unique passwords on all of your passwords are unique and secure. As mentioned previously, a password manager can help you create, maintain and recall unique passwords on all of your passwords are unique and secure. As mentioned previously, a password manager can help you create, maintain and recall unique passwords on all of your passwords on all of your passwords.
hacks and viruses don't become an actual threat without any form of human action to open the gates to a potential attack. Simply put, you should always be careful when being active on your computer or other devices. Now, you are aware of the signs that should trigger your suspicion, as well as the fact that you should take action against it. If you
want to read more about the different types of malware from Windows. If your Android device, I recommend reading my Complete Guide to Removing Malware from Android phones. Remember these signs, and make sure to
take action immediately! The longer you wait to battle against hackers, the more damage they'll be able to do. Even if you have the slightest suspicion, take action! It's always better to be safe than sorry. Have You Been Hacked FAQs There are a number of things that can clue you into the sad fact that you have been hacked. You may see that browsen
extensions or applications have been installed without your knowledge, you get a message that your data has been encrypted, you see text messages in your data usage increase by a large amount, or you may see text messages that you know
you didn't send on your history screen (these may be to "premium" text services). You may also see long-distance calls or calls to "900" numbers on your device's performance may also drop precipitously. Keep an eye on all of your accounts, including banking accounts, credit cards, and any other financial accounts. Invest
in a credit monitoring and alerts service (although some hacked firms will offer free credit monitoring in the wake of an attack or data breach). Immediately change your passwords to prevent duplication). Also, install reliable antivirus and
anti-malware protection and scan your device for viruses and malware, keystroke loggers, and other threats. While changing your password does not make them magically disappear from the face of the earth, it can break their hold on you, even if it only does so temporarily. Changing your password prevents hackers from accessing the affected
account. Be sure to use a password manager to generate and manager to generate and manager to generate and secure passwords. This ensures that you will be using unique and secure passwords. While resetting your PC - which in my mind is wiping it clean and reinstalling everything, including your apps, will clean it of malware - hackers will still be after you once you go back online
Make sure to install antivirus and anti-malware protection and set it up to scan your PC on a regular basis. Make sure all of the apps you reinstall are from known reliable sources. Also, scan all of your documents are known for being vulnerable
to this.) Also, when going online, stay out of the darker corners of the web and use a reliable VPN whenever possible Yes, there is a very small chance that someone could hack into your phone's camera and see what you're doing. However, the likelihood of this happening is relatively low, and there are ways to protect yourself from being spied on. One
simple way to protect yourself is to cover up your phone's camera with something opaque, like a bandana or piece of tape. This will prevent anyone from seeing into your camera without your permission. You can also install security software on your phone that will help to protect your privacy. A strong password should be made up of at least eight
characters, with a mix of letters, numbers, and symbols. A strong password is also a unique password is also a unique password is also a unique password for multiple accounts. Identity theft - in this case, we're talking about online identity theft - involves a bad actor using your personal information to fraudulently gain access to money or goods
The stolen information can be gained via physical theft, gleaning information from social networks, or obtaining it via data breaches. Using another known good computer, immediately change all your other logon names and passwords. Check your bank account transaction histories, stock accounts and so on. Consider paying for a credit-monitoring
service. If you've been a victim of this attack, you have to take it seriously. Complete restore of the computer is the only option you should choose for recovery. If you've lost any money, make sure to let the forensics team make a copy first. If you've lost any money, make sure to let the forensics team make a copy first. If you've lost any money, make sure to let the forensics team make a copy first. If you've lost any money, make sure to let the forensics team make a copy first.
real money losses, if any. This is a huge sign of malicious compromise. If you notice that your antivirus software is disabled and you didn't do it, you're probably exploited — especially if you try to start Task Manager or Registry Editor and they won't start, start and disappear, or start in a reduced state. What to do: Perform a complete restore because
there is no telling what has happened. If you want to try something less drastic first, if on a Windows computer, try running Microsoft Autoruns or Process Explorer (or similar program, which you can then uninstall or delete. If the malware "fights according to the malicious program," which you can then uninstall or delete. If the malware "fights according to the malicious program," which you can then uninstall or delete. If the malware "fights according to the malicious program causing the problems. They will usually identify your problems. They will usually identify your problems to the malicious program causing the problems.
back" and won't let you easily uninstall it, research the many methods on how to restore the lost functionality (any internet search engine will return lots of results), then restart your computer in Safe Mode and start the hard work. I say "hard work" because usually it isn't easy or quick. Often, I have to try a handful of different methods to find one
that works. Precede restoring your software by getting rid of the malware program using the methods listed above. I mean lots of money. Online bad guys don't usually it begins by your computer being compromised or from you
responding to a fake phish from your bank or stock trading company. The bad guys log on to your account, change your contact information, and transfer large sums of money to themselves. What to do: In most cases you are in luck because most financial institutions will replace the stolen funds (especially if they can stop the transaction before the
damage is truly done). However, there have been cases where the courts have ruled it was the customer's responsibility not to be hacked, and it's up to the financial institution to decide whether they will make restitution to you. To prevent this from happening in the first place, turn on transaction alerts that send text alerts to you when something
unusual is happening. Many financial institutions allow you to set thresholds on transaction amounts, and if the threshold is exceeded or it goes to a foreign country, you'll be warned. Unfortunately, many times the bad guys reset the alerts or your contact information before they steal your money. So, make sure your financial or trading institution
sends you alerts anytime your contact information or alerting choices are changed. One of the top ways that any organization finds out they have been successfully compromised is notification by an unrelated third party. This has been the case since the beginning of computers and continues to be true. Verizon's respected Data Breach Investigations
truly been hacked. Make sure everyone slows down until you confirm that you have been successfully compromised. If confirmed, follow your predefined incident response plan. You have one, right? If not, make one now and practice with stakeholders. Make sure that everyone knows that your IR plan is a thoughtful plan that must be followed. You
don't want anyone going off on their own hunting parties or anyone inviting more people "to the party" before it's decided who needs to be involved. Your biggest challenge is going to be actually having people follow the plan in an emergency. Communicate and practice, ahead of time. Nothing confirms you've been hacked like your organization's
confidential data sitting out on the internet or dark web. If you didn't notice it first, then likely the media and other interested stakeholders will be contacting your organization to confirm or find out what you are doing about it. What to do: Like the previous sign, first find out if it's true that it is really your confidential data out there. In more than a
few cases, hackers have claimed to compromise a company's data but didn't have anything confidential. Either they made up the claim and data, only had publicly available data, or they had some other company's data. So, first confirm. If it is your organization's confidential data, it's time to tell senior management, begin the IR process, and figure
                              nicated to whom by when. In many countries and states, the legal requirement to report compromised customer data can be as short as 72 hours. It goes without saying that you need to get legal involved. Literally billions of valid
(at least at one time) logon credentials are on the internet and dark web. They have usually been compromised by phishing, malware or website database breaches. You will not usually be notified by third parties as is the case with other types of data leaks. You have to proactively look out for this sort of threat. The sooner you know this sort of thing
has happened the better. You can check for compromised credentials one at a time using various websites (like Have I Been Pwned), check across multiple accounts using various free open source intelligence tools (like KnowBe4's Password Exposure Test), or any of the commercial services that look for
your company's data and credentials all the time for a fee. What to do: After first confirming whether the dump contains any currently used credentials, reset all your logon credentials. Start an IR process to see if you can figure out how your organization's logon credentials all the time for a fee. What to do: After first confirming whether the dump contains any currently used credentials.
was first noticed by strange, unexpected network traffic patterns. It could have been a bad distributed denial of service (DDoS) attack against your company's web servers or large, expected file transfers to sites in countries you do not do business with. If more companies understood their legitimate network traffic patterns there would less need for a
third party to tell them they are compromised. It's good know that most of the servers in your company don't talk to every workstation in your company and vice-versa. Most workstations in your company should not be using non-HTTP/non-HTTPS protocols to talk directly to
other places on the internet. What to do: If you see unexpected, strange traffic that you cannot explain, it's probably best to kill the network connection and start an IR investigation. Years ago, we probably would have said to err on the side of operational caution. Today, you can't take any chances. Kill any suspicious transfers until they are proven
legitimate. If you don't understand your valid network traffic, you need to do so. Dozens of tools are designed to help you better understand and document your network traffic. I would recommend checking out the free, open-source alternatives like Bro and Snort, but both require a lot of time, resources and research to use effectively. Instead, find a
good commercial solution that has already done all the hard work for you. The hope that an antimalware program can perfectly detect malware and malicious hacking is pure folly. Keep an eye out for these common signs and symptoms of your computer being hacked. If you are risk-adverse, as I am, always perform a complete computer restore with
the event of a breach. Once your computer has been compromised, the bad guys can do anything and hide anywhere. It's best to just start from scratch. Most malicious hacking originates from one of three vectors: running Trojan horse programs, unpatched software, and responding to fake phishing emails. Do better at preventing these three things,
and you'll be less likely to have to rely on your antimalware software's accuracy — and luck. Realizing your phone has been hacked can be extremely stressful, but stay calm.getty These days, most people are highly reliant on their phone. Three quarters of phone users worldwide use them to chat or send messages, six in ten for banking and nearly
half for navigation, according to Statista. Indeed, according to Pew Research, 15% of U.S. adults are "smartphone-only" internet users who depend on their phone as they don't have a home broadband service. All this means that if something goes wrong and your phone is hacked, your life can be upended — and your bank account cleaned out. Here's
a look at how to know if your phone is hacked, how to avoid it and what to do if the worst happens. Cyber criminals have a variety of ways to take control of, or steal information from, a victim's phone. All types of phone, whether iPhone or Android, are vulnerable — although Apple phones are generally perceived as being safer, thanks to stronger
security controls. There are a number of different phone hacking techniques. One of the most common is to fool the user into clicking on a malicious link, or into downloading software from a fake app store or elsewhere through what's known as social engineering, often through the use of phishing emails. Fake public wifi networks can often fool the
unsuspecting. Another technique involves a SIM swap, in which an attacker persuades a victim's mobile provider to transfer their sim card to a device under their control; infected USB cables or charger cables can also allow an attacker has found a way in, a user's data can be exposed, especially where passwords have
been reused. Perhaps the most high-profile hack of a phone came in 2019, when the Twitter account of the company's CEO, Jack Dorsey, started tweeting out a string of bizarre posts. It was immediately clear that his Twitter account had been hacked. In this case, the attackers appear to have used a SIM swap, which was only possible through a
"security oversight" by his mobile carrier. More commonly, a phone user becomes suspicious after spotting one or more of the symptoms below. There can be a number of signs that a phone has been hacked — but they don't necessarily appear in every case and, when they do, they can be easy to miss. Basically, it's a question of looking for unusual
behavior from your phone. 1. Check The Phone's Battery One common symptom that your phone has been hacked is a fast-draining battery. This can also cause the phone to overheat. If you suddenly see a noticeable difference, there may be a problem. Another sign of a phone hack is higher-than-usual bills, as your phone carries out unauthorized
activities. A jump in the amount of bandwidth you're using could be a sign that the phone is sending unwanted communications. 3. Audit The Apps On Your Phone If you phone is hacked, new apps may appear unexpectedly, existing apps may take a long time to load and apps may open or close on their own. Be on the lookout for suspicious behavior.
4. Recognize Rogue Notifications And Settings Sometimes unexpected notifications, unrequested two factor authentication codes or pop-ups may start to appear, and settings such as camera or microphone permissions may change. 5. Check Your Accounts The biggest red flag of all is to find yourself unexpectedly locked out of your Apple ID or Google
account, or out of other online accounts. 6. Run Antivirus Software Installing and running a reputable security software package should reveal for sure whether a phone has actually been hacked. Find and remove any malware or spyware that may have infected the phone using popular packages are available from the likes of: Bitdefender Norton
Kaspersky AVG McAfee Delete anything suspicious, restart the phone, and then run the software again to make sure that the phone has been hacked, there are a number of important steps that need to be made immediately to try and prevent the
hackers from causing any more damage than necessary. 1. Check With Your Financial Institutions to make sure your accounts haven't been accessed. 2. Change Your Passwords Your next move, and one of the most important, is to change all passwords immediately
to new, strong ones. This should be done for all all apps and websites that are connected to the infected phone. 3. Remove Suspicious or unknown. Restart the phone and check again to make sure the deletions were successful. 4. If All Else Fails, Factory Reset The
Phone If there really are lots of pop-ups or malicious apps and all else fails, you could restore your phone to its factory settings — although as this means losing everything stored on the device, it's very much the nuclear option. 5. Alert Your Friends It's a good idea to let your friends and other contacts know that your phone has been hacked, and warn
them to ignore and delete any messages that appear to be coming from your phone. How You Can Protect Your Phone From Future Hackers Whether or not you've been hacked already, there are a number of basic cybersecurity measures you can take to keep your phone safe from attackers in future. The first, and most straightforward, is to make
sure you have a good security package, like one of those listed above, installed, and keep it updated. It's important, indeed, to keep up to date with all software updates, as these often fix known vulnerabilities. Make sure your passwords are strong. Be wary of public charging stations and public wifi, and as an extra precaution, you might wish to turn
off your wifi and Bluetooth when not in use. For extra protection, you could encrypt your phone, lock your SIM card and use a virtual private network, which should make public wifi safer to use. And be very wary of third-party app stores: playing it safe with Google Play and Apple's App Store is always the best bet. Bottom Line Falling victim to a
phone hack can have a devastating impact, affecting everything from friendships to your bank account. Fortunately, it's possible to recover, and there are ways to make it much less likely that it happens again.
```