Does resetting a hacked router make it safe again?

Can a simple reset really make your router safe again? The answer depends on how you reset the router and what you do immediately after resetting the router.

If you suspect your router has been hacked, turning it off and on again is usually the recommended first step. However, can a simple reset really make your router safe again? The answer depends on how you reset the router and what you do immediately after resetting the router.

Does resetting the router prevent hackers?

Resetting your router will cut all connections and restart from scratch, including any hacker connections. However, if your router reboots with the same login information, there is nothing to prevent the hacker from connecting or logging into your system again.

To remove hackers from your system – and keep them at bay – you want to reset your router and change your authentication information (router login name, router password, network name, and network password).

This way, you are booting hackers off your system by reset and preventing them from regaining access by changing your credentials. Unfortunately, this will not undo anything the malicious hacker has done to your device, data, etc.

This is why it is important to regularly check for suspicious connections and act quickly. Additionally, you should regularly perform router reset cycles as part of your online security strategy.

How to properly reset a hacked router

If you suspect your router has been hacked, follow these steps immediately to reset the device properly:

1. Perform a factory reset

The first thing you want to do is reset your router to factory settings. This will restore all of the router's settings to their original state, including the router's login name, router password, network name, and network password – as well as anything else the hacker may have changed. change.

This is most effective when you have changed your login information from the factory default before the hacker gained access. In these cases, a factory reset will cut off the hacker's connection and prevent them from regaining access using the same credentials.

Tip : You will want to change these login details again after resetting but never reuse details that hackers may have previously compromised.

2. Update the router's firmware

Before you change any authentication information, make sure your router's firmware is updated to the latest version. A factory reset will also revert your router to the original firmware version it came with, so you'll need to install the latest update manually.

Most firmware updates patch security holes, so you always want to make sure you're running the latest software. Again, you should regularly check for router firmware updates as part of your home network security strategy.

3. Change the router's login information

After resetting the router and running the latest firmware, it's time to change your access credentials. First, you'll want to change your router's login name and password, which will allow you to access the administration software.

Enter the router's IP address into the web browser and use the default login information to access the admin panel. The layout and settings available in the router software vary by manufacturer.

All manufacturers allow you to change the password for your router, and some manufacturers also allow you to change the login name. The most important thing here is to choose a secure password that is easy to remember but difficult for hackers to crack, even if they use automated programs.

4. Change the router's network name (SSID)

Next, you should change your Internet network name, which is called SSID. This is the display network name that nearby users can see on their device when they search for networks in range.

Changing this will make it harder for hackers to identify your network, and it also sends a signal to others that your network is safe. Default network names can make you an attractive target for hackers because they indicate that other default settings will be left unchanged and overall security is poor.

If you want to further increase security, you can change the SSID for your network, then hide the WiFi network to prevent it from showing up in the list of available networks for nearby users.

5. Change network password

After setting up your SSID, you'll want to create a new password to connect wirelessly to your network. The field that identifies your wireless password may be in several locations, depending on the router you are using.

Many manufacturers group the network name and password fields together, but you may have to look elsewhere – for example, in the security certificate settings section.

6. Disable remote management feature

Remote management is a popular feature that allows users to access your router from anywhere in the world. This allows you – and potentially anyone else – to access the administrator account using the login name and password you set (or the default credentials if you haven't changed them).

This is a major security weakness, but most routers allow you to disable remote management or limit the devices that can access it. For example, you can typically limit access to a device or a group of devices by their IP address.

7. Turn off Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) makes it easier for new devices to connect to the network without providing a password. If you look at your router, you may notice a button labeled WPS. Pressing this button temporarily allows nearby devices to connect to the network without needing to select a network on their device or enter a password.

WPS is a convenient feature if you have multiple devices connected to your network, but it's also a security risk. If multiple people have physical access to your router, you should turn off WPS. You can always create a guest network for people to access without a password if you want it to be easy for people to connect to your network.

What should you do after resetting a hacked router?

After resetting the hacked router and changing your login information, you should do the following:

1. **Check which devices are connected to your network** : Log in to your router's admin panel and check which devices are currently connected to your WiFi network to ensure there are no devices connected without permission. identification.

2. **Monitor your network for strange behavior** : Watch for the signs of a hacked router that we discussed earlier – especially the ones that first made you suspicious.
3. **Scan your devices for malware** : Run quality antivirus software on all your devices to check for viruses, malware, and other malicious programs that hackers may have targeted Friend.
4. **Check if your personal data has been leaked** : Hackers may try to access your personal data (email address, passwords, payment details, etc.), so Look for any signs of a data breach: Suspicious login attempts, unusual account activity, password changes you didn't make, etc. Also, turn on security features like authentication two factors if you haven't already done so.
5. **Keep an eye out for suspicious payment activity** : Some hackers will go straight to your bank balance, so monitor payments for anything suspicious - including any activity Payment on registered account.

By following these steps, you can double check whether your router is secure or not. Second, you're investigating any potential hackers may have had access to your router and taking steps to minimize any risks.