

5 reasons to set up a guest network on the router

One way to increase WiFi security is to set up a guest network on the router. Here are 5 reasons why a wireless guest network helps improve network security.

A router is an Internet gateway. It is also an entry point for hackers looking to exploit a vulnerability. Do you trust your router to protect the network?

One way to increase WiFi security is to set up a guest network on the router. Here are 5 reasons why a wireless guest network helps improve network security.

Why set up a guest network on the router?

1. Help the network be safe from hackers
2. Keep the smart home devices separate
3. No need to share the primary router password
4. Manage access to the router
5. Disable the guest network to restrict access

1. Help the network be safe from hackers

Hackers want your data. They want to control the devices, forcing you to pay ransom, sniff around for valuable data, identity theft, etc.

You can take steps to combat this by securing the router.

For best results, make sure you have changed the default password on the router. Also, take the time to change (or even hide) the SSID for the primary network.

Then create a guest network to hide the 'real' network. Unless you are specifically targeted by hackers, they won't spend the time searching for a secondary network.

2. Keep the smart home devices separate



Keep smart home devices separate from the network

Smart home technology and Internet of Things (IoT) devices are not very good at security. Many devices (such as cameras, lights, smart locks) are sold with security errors.

These vulnerabilities allow hackers to access devices remotely. There is potential for additional access to other devices on the network from there, especially those that run hardware to control smart home devices.

By using guest networks for smart home and IoT devices, you will protect other hardware. Laptops, PCs, tablets and phones, NAS devices, game consoles can securely connect to the main network. It makes sense for devices with less strong security to be kept away from your important data storage devices.

3. No need to share the primary router password

When you have guests, for example at a party or simply a babysitter, guests want access to your WiFi network. So do you give them the password?

Although it is tempting to suggest that they use their own mobile Internet connection, it is better to allow visitors.

Now, many routers ship with a feature called WPS. Wi-Fi Protected Setup is designed to help devices connect to wireless routers more easily. However, it creates an opportunity for hackers to exploit, and so is not recommended for use.

In fact, WPS should be turned off on the wireless router. If you have not already done so, disable it immediately. Instead of WPS, you just need to suggest that visitors use the guest network and keep the password for the primary router secret.

4. Manage access to the router



Manage access to the router

Another advantage of using a guest network is that you can manage access to the router. Therefore, connect the TV, console, PC, etc. to the main network. Keep guest networks separate for guests, children, smart home devices, etc.

That way, you know that the hardware you rely on is safely and securely connected from intrusion from other devices.

Occasionally take the time to check who has access to the network. You can do this by logging into the router admin screen. Also, use an app like Fing (this network tool is available for Android and iPhone). It displays all devices on a selected network.

This is a great way to see what connections have been made and which devices you might want to eject from your network.

Download Fing for Android

<https://play.google.com/store/apps/details?id=com.overlook.android.fing>

Fing for iOS

<https://itunes.apple.com/app/id430921107>

5. Disable the guest network to restrict access

Finally, you can disable the guest network without losing connection with other hardware. Why can you do this?

First, there may be a problem with your IoT or smart home technology. Keeping it separate from the main network is clearly a must. Disabling that hardware Internet connection while keeping other reliable technology online is also a wise thing. This can help you understand the problem.

Second, you can simply deactivate access to the guest network, when a visitor is no longer welcome or a child is watching children's programs on Prime Video beyond the allotted time.

Although parental control software is a better option for managing children 's access to the Internet, this is also very effective. Just remember to turn on the guest network again when needed.

For how to set up guest network, please refer to the article: [How to set up guest network for Router](#) for more details.

You finished reading the article "**5 reasons to set up a guest network on the router**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
