Everything you need to know about router security to avoid getting hacked by cybercriminals

msn.com/en-us/news/technology/everything-you-need-to-know-about-router-security-to-avoid-getting-hacked-by-cybercriminals/ar-BBV2zLi

Kim Komando

The bad news: most people don't give a second thought to their routers.

This lack of know-how puts a lot of households in a dangerous position. The United States Computer Emergency Readiness Team (US-CERT) has issued an alert about Russian state-supported hackers carrying out attacks against a large number of home routers in the U.S.

Some routers are inherently flawed and can never be fixed. To help beef up your router's security, here are five tactics for protecting your home network, devices and files from hackers.

First, check your router's admin page

Before you start, make sure you can get into your router's administration console; this is where you manage your router's settings, including password management to firmware updates.

First, make sure your computer is connected (either wired or wirelessly) to your router, open a web browser and type in the router's IP address. The IP address is a set of numbers, and the default depends on your router's manufacturer. The common ones are 192.168.1.1, 192.168.0.1 or 192.168.2.1.

If you're don't know your router's IP address or password, it's on the internet.

© Getty Images
Wireless Router

1. Select the best encryption

Criminals love unsecured home Wi-Fi networks. Securing your Wi-Fi network can also shield you from unwelcome connections that may be using your network for illegal activities.

This is why it's important to protect your Wi-Fi network with strong encryption. If you are required to enter a password to connect to your Wi-Fi, you already have some encryption enabled on your router.

There are different types of Wi-Fi encryption, and you have to make sure that it's the most secure one you can employ.

The most widely-used Wi-Fi security protocol right now is still Wi-Fi Protected Access 2 (WPA2) encryption. However, this standard is over a decade old, and it is already susceptible to serious security vulnerabilities like 2017's KRACK attack.

If you're shopping for a new router, look for one that supports the newest security standard called WPA3. These models have just started rolling out. Every router has a different menu layout, but you should be able to find encryption under the "Wireless" or "Security" menu. You'll have a number of encryption options: if you still have an older router, you want to select one that starts with "WPA2." If your router is not WPA3 compatible, then "WPA2-PSK AES" is your best option right now.

However, if you have older Wi-Fi gadgets, you might have to select the hybrid option "WPA2-PSK AES + WPA-PSK TKIP" to get them working.

Never choose Open (no security), or if it is using WEP, change the security setting immediately. An open network will make it easy for someone to steal your Wi-Fi, and the older WEP security is easily hacked.

If the only encryption options your router has are WEP or WPA, tell your router to check for a firmware update. Look in your manual for the instructions.

If there's no firmware update or your router updates but you're still stuck with WPA or WEP, it's time to buy a new router. These encryption methods are too unsafe to use, plus it means your router is probably more than 7 years old.

2. Pros set up an additional separate network

A great tactic is to put visitor devices on a separate network. You do this by setting up a completely different Wi-Fi router or enabling your router's "Guest Network" option, a popular feature for most routers.

Guest networks are meant for visitors to your home who might need a Wi-Fi internet connection, but you don't want them gaining access to the shared files and devices within your network.

This segregation will also work for your smart appliances, and it can shield your main devices from specific Internet-Of-Things attacks.

To avoid confusion with your primary network, set up your guest network with a different network name (SSID) and password. Please make sure you set up a strong and super-secure password on your guest network, as well. You still won't want crooks and strangers mooching off it for security reasons.

Newer routers do this segmentation automatically. With this feature, it allows users to put Internet-of-Things appliances on a separate network, shielding your central computers and other personal gadgets from attacks.

With this virtual zoning of your network, you can still allow all your smart appliances and hubs to communicate with each other while keeping your main computing gadgets safe in the event of an Internet-Of-Things attack.

Also, if you're worried about "wardrivers" or people roaming around looking for Wi-Fi spots to hack, you can disable the broadcasting of your network and your guest network's name (SSID) entirely.

3. Use the free parental controls

To shield your kids from inappropriate sites, most routers have built-in content filters, parental controls and time-based restrictions.

To enable these filters, visit your router's administrator page or app again and look for a section called "Parental Controls" or "Access Controls." Here, you can choose what type of sites to disable access to, set the schedule when the filters are in effect and set curfew hours for certain gadgets.

You can even set filters for specific IP and MAC addresses. The downside of this method is the inconvenience and it takes a bit of technical skill to pull this off. The good thing about this is that you'll have a map of all your connected gadgets and their corresponding IPs.

To take this a bit further, turn on MAC (Multimedia Access Control) filtering. With MAC filtering on, you can specify which MAC addresses will be allowed to connect to your network at certain times. Note: MAC addresses can usually be found in the gadget's settings, label or manual. Look for a set of 16 alphanumeric characters. (Here's an example of what a MAC address will look like: 00:15:96:FF:FE:12:34:56)

4. Turn on the VPN

You have likely heard of a VPN (Virtual Private Network), which is an excellent way to boost your online security and privacy.

With a VPN, your gadget's IP address is hidden from websites and services that you visit, and you're able to browse anonymously. Web traffic is also encrypted, meaning not even your internet service provider can see your online activity. It is a good way to hide your internet tracks from would-be snoops.

VPN services are typically accessed via software, but some newer routers can be configured with VPN capabilities straight into the router itself. Instead of protecting each gadget protected with its own VPN service, your router will protect every connected

device.

Routers with this capability have open source router software support (such as DD-WRT), and they can be configured to use services like OpenVPN.

Currently, there are a variety of open source and OpenVPN capable routers to choose from, but the most popular models are the Linksys AC3200 and the Netgear Nighthawk AC1900.

5. Turn on and test the firewall

One valuable tool that can protect your router from hackers is a firewall. With it, even if they manage to know your router's location and IP address, the firewall can keep them from accessing your system and your network.

Almost every newer router has built-in firewall protections in place. They might be labeled differently, but look for features under your router's advanced settings like NAT filtering, port forwarding, port filtering and services blocking.

With these controls, you can configure and specify your network's outgoing and incoming data ports and protect it from intrusions. Be careful when tweaking your port settings though, since a wrong port setting can leave your router vulnerable to port scanners, giving hackers an opportunity to slip past.

To check if your router's firewall and your ports are secure, you can use an online tool for a quick test.

This article originally appeared on USA TODAY: Everything you need to know about router security to avoid getting hacked by cybercriminals