Router: Essential Security Settings

Four Steps to Increase the Security of Your Wireless Internet Access

This article shows you how to:

- Check all the important router settings
- Prevent unauthorised access to your Internet connection
- Turn off the riskier features of your router

Your router is the device that provides Internet access to your household's computing devices – your PCs, tablets, smartphones, smart TVs and so on. This unassuming little box ensures you can always get online when you need to.

But is your router also leaving the door open to outsiders and hackers? Follow the four steps in this article to learn which aspects of your router's security you should check and why they're so important.

Contents:

Even ignoring older routers that are no longer on sale, there are hundreds of routers available from dozens of manufacturers, and they're all different from one another. Although they all offer the same vital security settings covered in this article, the exact names of those settings – and where you'll find them – will vary from one router to another.

For this reason, the steps that follow are necessarily fairly general: I'll tell you what to look for, and do my best to point you in the right direction to find it, but it will help to have your router's manual at the ready.

If you don't have a printed manual, you might find it in PDF format on a CD that came with your router. Failing that, pay a visit to the router manufacturer's website where you should be able to find a copy of the manual to read online or download.

Step 1: Change the Router Password

Your router's management console

In order to check or change any of your router's settings, you have to open its 'management console'. This is a collection of web pages stored inside the router itself, and you reach them using a web browser such as Microsoft Edge or Google Chrome.

The console has its own 'web address'

Just like the websites you visit, your router has its own address. When you type the address of a website into your browser and press **Enter**, the address is passed to your router, which passes it on to the Internet, waits for the web page to be sent back and then passes that page on to your browser. However, when you type the address of your router itself into your browser, your router recognises this address as its own and immediately sends back the first page of its management console.

The address you need to type is one of those things that varies from one router to another, so it will help to consult its manual, but here are the addresses used by some of the most popular router brands:

Router Brand	Address
Asus	192.168.1.1
Belkin	192.168.2.1
D-Link	192.168.0.1
Linksys	192.168.1.1
Netgear	routerlogin.com
Sky	192.168.0.1
TP-Link	192.168.1.1

Knowing the address you need to enter, you're ready to start. Follow these steps:

1. Open your favourite web browser, click in its address box and type your router's address, and then press **Enter**.

Ready to log in

2. When the page loads, you may find that you're immediately prompted to enter a username and password. If not, look for a **Login** link and click it, and that will lead you to the username and password boxes.

Here's a suggestion: having arrived at this login page for your router, add it to your browser's Favourites or Bookmarks so that you can return to it easily in future without having to remember and type its address. To do that, press **Ctrl+D** and then type a name like 'My Router' and click **Add** or **Done**.

3. Now I have a question for you: have you chosen your own username and/or password to use for logging into your router?

Have you changed the admin password?

- If you have, enter those now and log in, and then you can skip ahead to 'Step 2: Change the Name of Your Wireless Network' on page 5.

If not, use the default username and password

- If you haven't, your router still uses the username and password that were set by the manufacturer (known as the 'default' username and password), and these are what you'll need to enter. Your router's manual will give you these details, but here are those used by the popular router brands:

Router Brand	Username	Password
Asus	admin	admin
Belkin	admin	[none, leave blank]
D-Link	admin	[none, leave blank]
Linksys	admin	admin
Netgear	admin	password
Sky	admin	sky
TP-Link	admin	admin

You must change the password!

4. You've just logged in using your router's default username and password, but this password is the first thing we need to change. The default password is freely available to anyone who wants to know it, and this means that someone with nefarious intentions could log into your router and change its settings. Consult your router's manual to find out how to do this, looking for instructions on how to change the 'administration password' or 'default password'. (Note that this isn't the same thing as changing your Wi-Fi password, which we'll discuss on page 7.) I suggest sticking with the username **admin** and choosing a new password with six to eight characters using a mix of upper- and lowercase letters and numbers. You'll usually be prompted to enter the old password (the one you just used to log in) and then type the new password twice.

Save the new settings

5. After entering the new password, look for a button marked **Apply** or **Save Settings** (or something similar) and click it to save the new password.

Some routers will simply store this new password and allow you to carry on using the management console. Others might need to 'reboot' first (to shut down and then restart), which will take a minute or two. If yours has to reboot, you can press the **F5** key in your browser every so often until your router's login page reappears (indicating that your router has now started again and your PC has reconnected to it). When it does, use the new username/password combination you've just chosen to log in again.

Make a note of the login details

It's a good idea to make a note of your router's username and the new password you've chosen for it so that you don't forget it. If you do ever forget the password, you can reset the router to its factory settings and log in with the default password, but this causes all its settings to be erased, requiring you to set it up from scratch again!

Step 2: Change the Name of Your WLAN

Your network has a name (or 'SSID')

If your router provides a wireless network (a 'WLAN'), so that your computers and other devices can connect to the Internet wirelessly, you should make sure the name of your WLAN doesn't give any clues to the make of router you're using.

Are you still using the factory-set name?

The name of your WLAN is technically known as its 'SSID', and this is what you'll see referred to in your management console and in your router's manual. For many routers, the factory-set SSID includes the router's brand name: if you have a Netgear router the SSID

might be 'Netgear52'; for a Linksys router it might be 'Linksys4567'; with a Sky router it could be 'SKY56789'.

This is a security risk. The range of your wireless network probably extends well outside your own four walls – perhaps up to 150 yards – so anyone using a computer (or tablet or smartphone) nearby can see your wireless network.

The default name is a useful clue to hackers

Some of those people might be tempted to break into your network – it's a surprisingly common pastime! – and if your router's SSID includes the brand name of the router, that makes the job much easier: they can find out exactly what security weaknesses that router has and set about exploiting them. (This is another reason why we changed the default password in the previous steps: if a would-be hacker knows your brand of router, the first password he'll try is its default password!)

Choose a different name for your network

So the next step is to check your router's manual for instructions on how to change the name of the wireless network (the 'SSID') and follow them to give your WLAN a different name. You'll usually find this option on a page named 'Wireless Network' or 'Wireless Settings' in the management console.

As well as choosing a name that doesn't include the make of your router, pick one that doesn't identify you personally or your address. Choose something anonymous but memorable such as 'MyNetwork2022' or 'BridesheadRevisited' or 'OldSocks'.

Save this change

After entering a new name, click the **Apply** or **Save Settings** button. As before, some routers may reboot at this point and others won't. However, one thing that certainly will happen is that the computer you're using will be disconnected from your wireless network. This is because your PC is connected to a network that no longer exists – its name has just changed.

You'll have to connect to your network again

Wait until your router has restarted (if it had to do that), and then connect to your wireless network again, this time looking for its new name in the list of available networks. In all versions of Windows, you can do that by double-clicking the network icon that appears near the clock at the right of the taskbar, then clicking your network's (new) name and typing the WLAN password. (Any other devices that connect to your WLAN will have to be reconnected to your newly-renamed network too.)

Step 3: Use Strong Encryption and Change Your WLAN Password

Your wireless network must be 'secure', and that word relates to two things:

Wireless networks must be password-protected

- First, it must be protected by a password. If it isn't, you have an 'unsecured' or 'open' network to which anyone within range can connect. That doesn't just mean people living nearby: some people actually drive around looking for unsecured networks and then park a little distance away to use their tablet or notebook with someone else's wireless Internet.

Of course, if anyone connects to your network and uses the Internet to do something illegal, their actions will be traced back to you. What's far more likely, however, is that a neighbour takes advantage of the free Internet access you're offering to do their casual surfing. That's unlikely to land you in any trouble, but it may well slow down your own Internet access. Worse, if you have a monthly download limit imposed by your broadband provider, your neighbour's surfing could push you above that limit and start costing you money in extra charges.

Use a secure type of encryption

- Second, it must use strong encryption to ensure that no-one can monitor the information passing wirelessly between your computer and your router. Various systems of encryption have been used for wireless networks over the years, and some systems – the newer ones – are more secure than others. It's important to be using the newest and most-secure encryption system you can.

Have you chosen a strong password for your network?

Your router may well already be set to use the strongest type of encryption. However, it may still be using the default (factory-set) password for your WLAN. For some routers, this password is publicly available to anyone who wants to find it, and it's probably also shown on a label on the base of your router. This means that if someone can determine the type of router you use, they may be able to log into your network as easily as you do.

Therefore, it's vital to make sure you're using the strongest type of encryption and to use your own choice of password for your WLAN.

Locate the 'Security' section in the console

Again, I'll have to leave you to consult your router's manual to find the exact steps for doing this, but you'll be looking for a tab or section in the management console named 'Wireless' or 'Wireless Settings' or 'WLAN'. In this section, look for another section named 'Security' or something very similar. Now there are two things to do:

1. Select the encryption type

Choose the encryption type

You'll find a choice between several encryption types: **WEP** (the oldest and least secure), **WPA** (a newer and much more secure type) and **WPA2** (the newest and the most secure). These may appear as option buttons (as in the following screenshot) or in a drop-down list.

Use WPA2 if possible

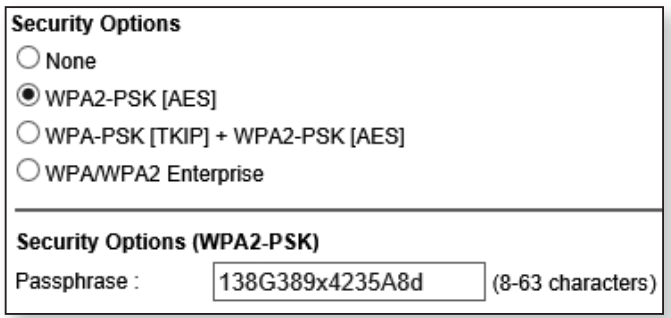
For the best security, choose one of the **WPA2** options: if you have a choice between 'WPA2 Personal' and 'WPA2

Enterprise', choose the 'Personal' option. As a second-best, if you use any wireless devices that are too old to support WPA2, you can choose **WPA**. (I really don't recommend using WEP as it's known to be very easily hacked, but even WEP is better than using no encryption at all and leaving your network wide open!)

2. Choose a password for your WLAN

Choose and type a strong password

The next step is to choose and type a password (which may be referred to as a 'key' or 'passphrase' in your management console). For WPA2, this must be at least eight characters long and – like any important password – must be impossible to guess, consisting of upper- and lowercase letters and numbers. (Be sure to make a note of this password on paper, perhaps popping it under your router, so that you won't lose it!)



Reconnect to your network by typing the new password

Finally, as always, click the **Apply** or **Save Settings** (or similar) button to save your changes. When you do, you'll see a repeat of what happened when you changed your network's name: your router may reboot and, whether it does or not, your PC will be disconnected from the network due to the change of encryption system and/or password. After making sure your router is back up and running, connect your PC to your network again, this time typing the new password you've just set.

Step 4: Turn Off Guest Access

Separate Internet access for visitors to your home

Most routers offer a feature known as 'Guest Access' or 'Guest Network'. As the name suggests, this is a second network which can be made available to any guests or visitors who turn up at your home wanting Internet access for their tablets or notebooks. It has its own name (or 'SSID') which must be different from your main network's SSID, and you can choose its encryption type and password (a different password from that of your main network).

It's another network name and password to manage

The point of this feature is that you can give visitors access to the Internet without having to tell them the password to your main network. However, this means yet another network name is being broadcast to everyone within 150 yards, offering another target for would-be hackers and freeloaders.

It's simplest to turn off Guest Access

Since anyone visiting your home is likely to be someone you trust, it's simplest just to let them connect to your main network. (If you weren't sure you could trust them, it would be very unwise to let them connect at all, since – as I mentioned earlier – any of their actions online would be traced back to you.)

Guest Access is probably turned off on your router by default, but I recommend checking this and, if you do find it's switched on, turning it off.

The one benefit of Guest Access is that it should prevent guests from accessing other devices on the network – your own PC and so on – limiting them to just using the Internet. So, if you have lodgers or you run a bed-and-breakfast, for instance, you might like to switch on Guest Access and give that SSID and password to your guests.