A strong Wi-Fi password will be meaningless if you ignore the WPS settings.

Wi-Fi Protected Setup, or WPS, can bypass even the strongest Wi-Fi passwords, and your router may have had this feature enabled when it shipped from the factory.

Most people believe that Wi-Fi security begins and ends with a strong password . Of course, that's an important part of Wi-Fi security, but don't let a long and confusing string of characters fool you.

Wi-Fi routers have many other security settings that you should pay attention to, and one setting you need to make sure is turned off.

Wi-Fi Protected Setup, or WPS, can bypass even the strongest Wi-Fi passwords, and your router may have had this feature enabled when it shipped from the factory.

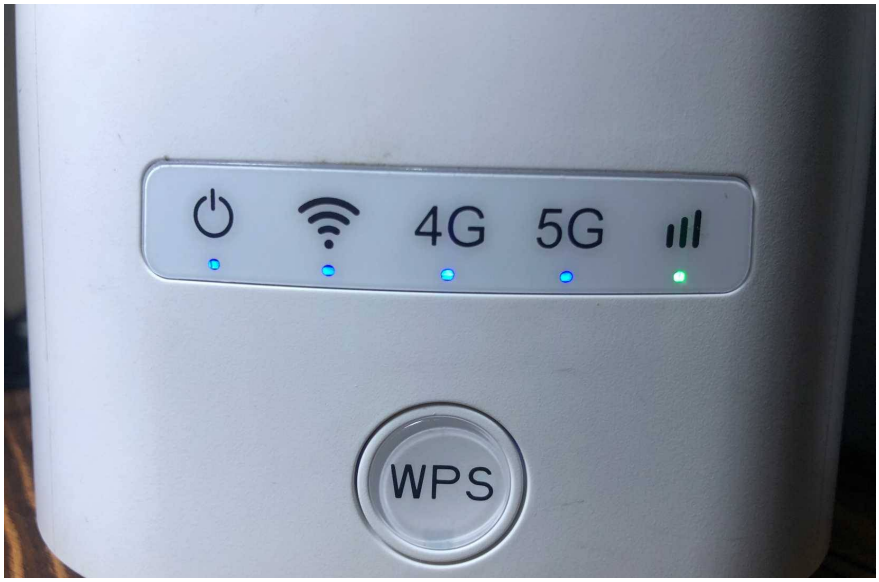
Main functions of WPS

In theory, WPS is extremely useful.

Conceptually, Wi-Fi Protected Setup (WPS) is a truly clever solution to a perennial problem: sharing your Wi-Fi information. Nobody likes spending hours entering a new Wi-Fi password, especially if you type a wrong character and have to start over.

WPS allows devices to connect to your Wi-Fi by pressing a button on the router, authenticating any device trying to connect to your network at that time. It's a great idea for devices with complex inputs, such as IoT devices, sensors, streaming boxes, etc. And to be fair, it works when you want it to.

The big problem with WPS



The big problem with WPS is that anyone who can press that button on your router can connect to your network.

The most common WPS method uses an 8-digit PIN, and importantly, it's not checked all at once. Routers authenticate the PIN in two parts, significantly reducing the number of attempts required for a brute-force attack. In practice, this can take hours instead of years—even on networks protected by strong WPA2 or WPA3 passwords.

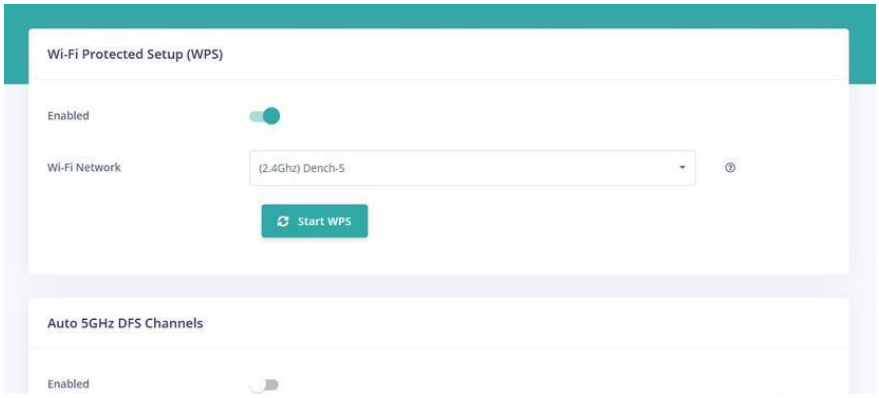
Once the PIN is cracked, the attacker will automatically obtain your Wi-Fi password. No matter how long or complex the password is, WPS will still hand it over to them. Worse still, many routers don't properly lock down repeated attempts. Even if they claim to disable WPS after a failure, the protection is often unreliable or easily bypassed.

Some routers only support WPS "button press," which is a bit more secure. But it still activates WPS after pressing, allowing anyone nearby to connect to the router.

Another major misconception about WPS is that a strong Wi-Fi password will protect you from this type of attack. Unfortunately, that's not true. WPS works in conjunction with your encryption, not within it. If WPS is enabled, WPA3 cannot protect you. Attackers aren't attacking your encryption – they're exploiting an old convenience feature that routers still rely on.

You might have the most secure password ever devised, but WPS can still provide the key. That's why disabling WPS on your router is essential.

Fortunately, modern routers are starting to eliminate WPS.



Most modern routers still support WPS. But the good news is that this feature is a well-known security issue, so many router manufacturers choose to remove the physical WPS button, as well as ship routers with WPS disabled by default.

This is a great move because it means that, unless you really want to use WPS (and there are some cases where it's necessary), you don't need to worry about your security being compromised by this feature.

Furthermore, many router manufacturers are specifically targeting PIN-based WPS, completely removing this option from the user interface, hiding the PIN, and generally trying to avoid this outdated technology. The new routers many people receive when upgrading their internet in 2025 will be the first routers without a WPS button.

That's a clear sign of the times.

WPS is not the only security vulnerability in routers.

There are many other ways to weaken your network.

Did you know that the old WPS vulnerability isn't the only thing that makes your router and home network vulnerable to attacks? There are several other default settings that can compromise your network if left unaddressed.

Older WPA modes	Some routers still allow WPA or WPA-TKIP for compatibility with older devices. In these cases, attackers target the weakest protocol available rather than the password itself. Even a long and complex password offers little protection if the encryption method can be bypassed or downgraded.
Guest Network	A poorly configured guest network can create an unexpected security vulnerability. If guest access isn't properly isolated from your main network, anyone with the guest password can view internal devices, access the admin page, or exploit vulnerabilities elsewhere. At that point, the strength of your main Wi-Fi password becomes almost meaningless.

Router's default login information	If the router's administration interface is accessible from the Wi-Fi network—or worse, from the internet —and still uses the default or weak password, an attacker doesn't need your Wi-Fi login credentials at all. Gaining administrative access allows them to change the password, disable encryption, or completely open the network. This is especially common on routers provided by Internet service providers (ISPs), which prioritize easy setup over strong security.

The reality is that it all accumulates and deserves serious consideration. Wi-Fi security isn't just about what you type once. It also involves the shortcuts your router allows to run in the background.