3 Steps for Updating Security Settings on Home WiFi Networks

You may have heard of the dangers of connecting to free, open-access WiFi networks. But did you know that your home network can also be hazardous to your personal data? If you have not taken the proper security precautions, your home WiFi is likely to be just as vulnerable as the open wireless network at your corner coffee shop. Without the proper defenses, your network could be accessible to anyone with even a modest set of cyber snooping skills.

Our infosec experts have identified the three most important security safeguards for standard home WiFi networks. "These protections," they said, "should solve 99.99% of issues for 99.99% of users."[1]

Take a read through the following tips and commit to taking these steps to make your network more secure. Though the idea of updating default passwords and changing WiFi settings might sound too technical for you to handle, it's easier than you might imagine. If you've ever programmed a DVR (or—going back in time—a VCR), you can do this as well.

1. Change Your Router's Default Administrator Password and Disable Remote Administration

The "admin" password on your router is totally different from the password that you use to connect to your WiFi network. Where your WiFi password will allow you to connect to the internet using your router, your router password gives you access to the actual configuration settings of the WiFi network itself. (See section 3 for information about setting/changing your WiFi password.)

The problem with leaving a default password in place is that everyone from amateur teenage hackers to sophisticated cybercriminals can find that password somewhere online and use it to get into your network. Changing default passwords helps to reduce cybersecurity risks.

Here's how to **change your default password**:

1. Find the label on your router that lists the default IP address, administrator user name, and administrator password.
2. Open a new web browser tab or window in your browser of choice.
3. Enter the default IP address—it will look something like 123.456.7.8—in the web address bar.
4. Enter the default user name and password on the login screen.
5. Navigate to the administration area and change the admin password. Longer is better, and special characters are a plus. A passphrase that means something to you but would be difficult for others to guess is a great option (for example, I<3SpicyChickenWings).

1 Like most networks, WiFi systems can include different types of equipment and different configurations. For the purposes of this article, we assumed a relatively common residential network setup featuring a single wireless router with a built-in access point.

The next thing to do while you're in this screen is to disable remote administration. When remote administration is enabled, it's possible to connect to your router from outside your home; leaving that on when not specifically necessary makes your network vulnerable to attack.

To turn off the feature, look for a box or button that is labeled with something like "Enable Remote Administration" or "Disable Remote Administration." Check or uncheck the feature as appropriate to ensure that remote administration is not on.

Note: If you can't find the spot to change your admin password within the interface, search "change <Router Brand> <Model Number> password" in your favorite web browser and you should quickly find the directions.

2. Update Your Router's Firmware

While you're in the administration area, take the opportunity to upgrade your router's firmware. As is the case with other electronic devices, router manufacturers often discover bugs and other issues that need to be addressed after products have already been shipped and installed.

Updating the firmware on your router is akin to updating the operating system on your smartphone or tablet, and this step can help eliminate known cybersecurity vulnerabilities and improve performance.

To complete the update, look for and select "Firmware Update," "Router Update," or a similar option in the administrator window. If you see the option to enable automatic firmware updates (look for a toggle feature such as "Router Auto Update" or similar), turn that on to ensure you automatically receive security and feature updates in the future.

As noted in the first tip, if you can't find what you're looking for, an online search can help you identify where to go within the interface to complete the update.

3. Configure Your WiFi Security Settings

There are three key settings to check (and, if necessary, change) within your WiFi network configuration: your SSID (which is the name of your wireless network), your encryption method, and your WiFi password.

Here's how to do it:

1. Look for a tab named "Wireless Setup" or similar. (Again, a quick online search can help you identify the exact location for your specific router if you're unsure.)
2. First, check your level of wireless encryption. WPA3 is the newest wireless encryption standard, but it is currently in its early days. Most routers and devices (like smartphones and laptops) do not yet support WPA3, so it's unlikely to be an available option in your interface (unless you've specifically installed a WPA3-compatible router). Until WPA3 becomes more commonplace, choose WPA2 encryption—a **must**, as earlier WiFi encryption protocols are far more vulnerable. If there are multiple WPA2 options, choose either WPA2-PSK, WPA2-PSK (AES), or WPA2-Personal; all three are essentially the same and offer the best option outside of WPA3 for at-home use.
3. Set or change your wireless network password. (If your service provider gave you a password, choose a new one.) As with your new router admin password, opt for a longer passphrase that has personal meaning and at least some degree of complexity (special characters, numbers, etc.). **DO NOT** reuse your admin password.
4. Change the default SSID to the name of your choice (something like "FBI Surveillance 1" is likely to leave your neighbors amused—or concerned). If you keep the default SSID, you will likely broadcast the brand and type of router you are using, and these are pieces of information that a cyber snoop can use against you.

On a related note, if you are particularly worried about outsiders "piggybacking" on your internet access—that is, using your WiFi network rather than paying for their own connectivity—disable SSID broadcasting. (Unauthorized wireless use tends to be a greater concern in more populated residential areas like apartment complexes and multi-tenant buildings.)

When SSID broadcasting is turned off, your WiFi network name will not be visible to devices when they scan for available wireless networks in your area. The benefit of disabling broadcasting is that it becomes much more difficult for outsiders to connect to your network because they would have to guess both your SSID and your password in order to gain access. The downside of this is that your SSID will not show up in your scans either, which means you will have to manually enter your network name into your devices when you connect.

To disable this feature, look for "SSID Broadcast" (or similar) in the wireless setup area. Check (or uncheck) the box or button as appropriate to disable broadcasting.

LEARN MORE

For more information, visit **proofpoint.com**.