Basement Haven Media LLC
56 33rd Avenue South #345
Saint Cloud, MN 56301-3722

https://basementhavenmedia.com

Joseph Jachimiec, Owner & Copywriter
joseph@basementhavenmedia.com
612/293-7561

Technology/Information Security Writing Sample
Keyword: Wi-Fi security

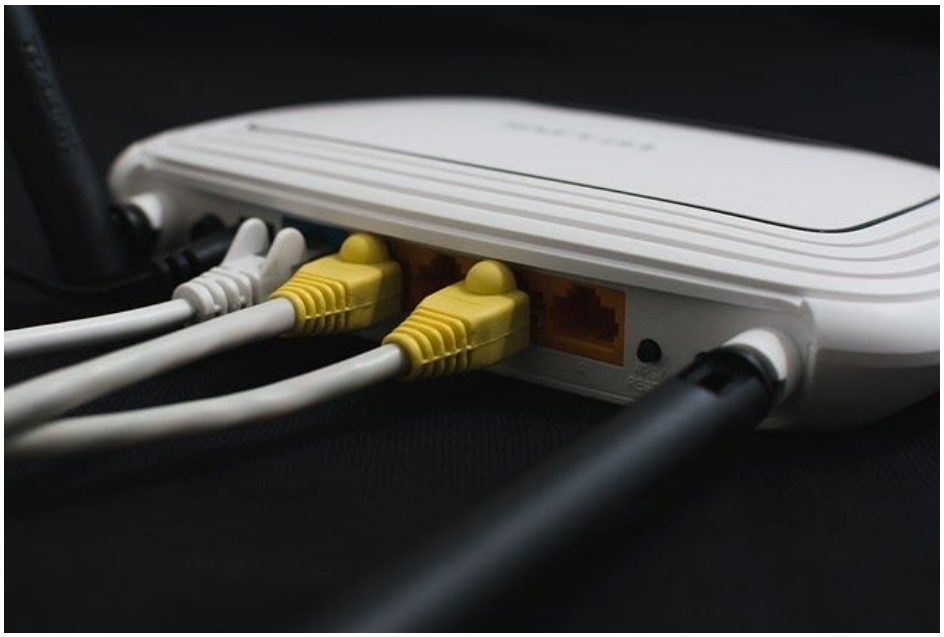
Wi-Fi Security: Three Easy Steps to Keep the Bad Guys (and Your Nosy Neighbors) Off Your Home Network

When you're connected to the Internet, you get access to the world.

That's a pretty cool thing!

But Internet traffic is a two-way street. The traffic flows not only *from* your home but *to* your home. So, although you get access to the world, surprise! The world also gets access to YOU unless you take steps to protect your home network.

The Wi-Fi router is your first line of defense for your home network. So it makes sense to set it up right so it provides the security and protection that you need.



Here are the top three things you should do to improve your Wi-Fi security right now. These tips will give you the most bang for your security buck with the least amount of effort.

1. Change the Default Administrator Password

From the factory, the router manufacturer has set up your device with a default administrator username and password. These credentials allow full access to all router settings so you can customize the setup, performance, and security.

Unfortunately, these default credentials are well-known and found with some simple Googling. The bad guys know this information all too well and it’s the first thing they’ll use when trying to hack into your device.

So first things first, change the default administrator password to something different.

It's best to include numbers and symbols along with lowercase and uppercase letters. It doesn’t need to be super-complex (unlike your WPA2 password, see number 3 below), but it shouldn't be a plain dictionary word either.

If you can change the “admin” or “administrator” username, do that too.

2. Keep the Firmware Updated and Patched

Buy a Wi-Fi router from a trustworthy brand. You'll have a better chance that the manufacturer releases regular firmware updates, especially when researchers find new security holes.

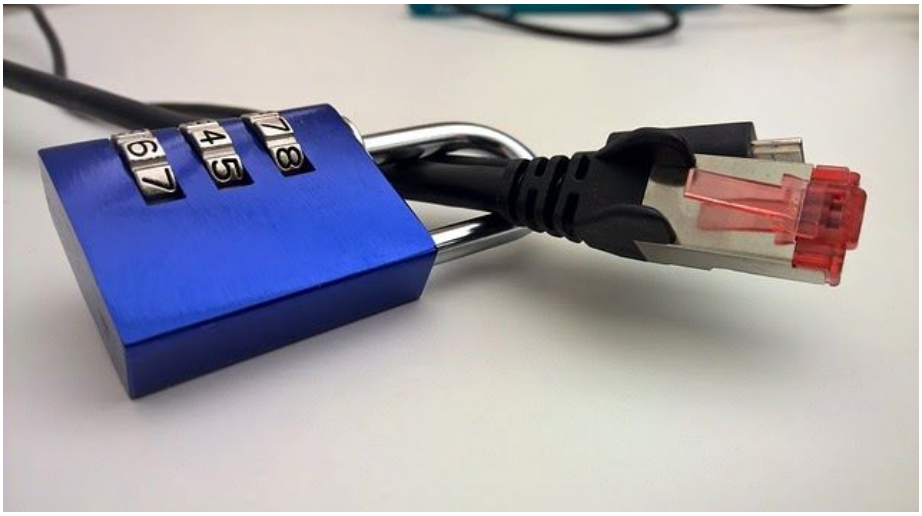
Keeping your router patched with these updates is a great way to beef up your home’s Wi-Fi security.

Bookmark the website support page for your router model, register your device, and get on the manufacturer’s email list. That way, you're alerted to any newfound vulnerabilities and fixes.

3. Use WPA2-AES Encryption with a Long, Crazy Password

This step could cause the most pain if you have to type the password into a lot of wireless devices. But it can be one of the most important, so don’t skimp here.

When choosing encryption options for your wireless network, use WPA2 with AES encryption. It's currently the industry standard and the strongest protection we've got right now.



A good Wi-Fi password can be the difference between a bad guy (or neighborhood teenage hacker) wreaking havoc on your network versus staying locked out and having your private data kept safe.

The longer and more complex your Wi-Fi password is, the better. You'll never remember it, so write it down or use a secure password manager like LastPass or KeePass.

Here are two examples of the types of passwords you should be using (but don't actually use these!):

sB4WajfJ0IcxhrbxnIXsZWOMN63e7ln8S5Lgf3iAvX6EybQN4820DAvk52xou2X

Or even this:

[DD0D/}9dJv~oJU/C%RSA;Z+tW\`x+4Z!~'>|PG7QF2]\B~Yko,F<zufKb~sM0\

See what I meant when I said "crazy"?

Wrap Up

Follow these three tips to get the most benefit with the least effort when putting together your home Wi-Fi security.

Is there more you can do? Sure, a lot more. Security can be a rabbit hole! But if it interests you and you have the right mindset it can be fun, useful, and even rewarding.