The internet provides us with so many opportunities to learn and stay connected that it's easy to forget there's another side to its story, one that's dark and dangerous. This is not meant to scare. In general, the internet is a safe place where you can find, consume, and share information. But just like anything in life, you need to take some small but necessary precautions to ensure your own safety as well as those who share your home.

Part of the reason this is so important is because we have willingly put so much of our own lives online. The various devices and services we use track nearly everything we do, including our location, and they also have sensitive data such as phone numbers, social security numbers, bank and credit card information, and more.

When you're out in the world, the risks will always be there. But just like we take steps to make sure our homes are safe; we need to do the same thing with our WiFi networks. Keeping our home internet connections secure is an important first step in creating a safe space from which we can use the internet.

Here are some tips on how to do this:

Change the Network Name and Password

This first step is a simple but highly necessary one. For cybercriminals to be able to gain access to your information, they need to fist get onto your network. A password helps put up a strong barrier against unwanted attempts at connection.

Nowadays, almost all WiFi networks will automatically be installed with a password and network name, but you'll want to take things one step further and change both to something you've created.
This is because most hackers use what are called brute force tactics, which means once they target you (something that seems to happen basically at random), they will attempt to log in to your network by using bots to try countless combinations of passwords.

Factory defaults are okay, but passwords and usernames are often issued in batches, which means if a hacker knows which provider you're using and they have some information about that company's passwords, your network is vulnerable.

A simple solution is to just change your network name and password to something different. Choose names and passwords that you'll remember but that are difficult to guess. For example, don't just use your address, or your last name, as these are the first things hackers will try.

When you install a new network, you should get instructions on how to change the name. But if you're working with an existing connection and don't know how to do this, here's a guide to help you out.

Use Anti-Virus Software

Securing your WiFi network with a password helps keep unwanted users off your connection, but it does nothing against the threats you can encounter once online. Bad links will send you to bad websites, and if you're not careful, you can wind up downloading a piece of malicious software that will at best slow down your machine and at worst steal or delete all of your sensitive information.

Anti-virus software puts up another line of defense and also helps point out risks before they become dangerous. For example, most anti-virus programs have a safe search option that will vet search results and other websites before you visit them, and if it senses something is wrong, it will prompt you with a warning that could save your life.
Another thing anti-virus software does is that it stops potentially harmful software from immediately downloading. So, if you click on something by accident (something we all know can happen), you will have the chance to halt things in their tracks before the damage gets too great.

Traditionally, anti-virus software has only been needed on PC computers, but Apple devices, as they are now much more popular, are also at risk, and so is your phone. Consider installing some sort of protection to make sure your devices are safe.

You'll also want to check out what kind of protection is on any smart devices you have. It seems almost everything can connect to the internet now, and this increases the risks we face.

Use Parental Controls

While it might not be a very popular decision, you should consider using the parental controls offered by your internet provider as much as possible. These will allow you to control what type of content can be accessed on the internet, which keeps both kids and adults away from sites that could possess harmful content that you could wind up downloading by mistake.

The nice thing is that you can use these controls at your discretion. Sometimes all it takes is a password to override them, and while this might be a tad annoying, having this step in place will help make your internet much more secure.

Here's a detailed guide on how you can most effectively use parental controls so that they increase security but don't strain familial relations.

Educate the Family

All of these tools and tricks are both helpful and necessary for you to make your home WiFi secure, but in the end, our defenses are only as strong as ourselves. All the anti-virus software in the world can't actually stop us from clicking on a link or agreeing to download a piece of bad software.

As a result, it's of utmost importance that we take the time to learn what the threats are and

how to spot them. Email phishing is one of the biggest risks we face, and this tool from Google will help you evaluate how well you spot phishing and if you need to be more vigilant.

Other things you can do include discussing with your family what constitutes safe browsing, and perhaps more importantly, what it means to use social media responsibly. Encourage kids to ask questions and work to create an environment where everyone feels safe to get help, as this is really the best way to keep you home WiFi secure.

Stay Protected

Taking this approach to home cybersecurity will help considerably reduce the extent of the threat we are exposed to by putting so much of our lives online. Of course, however, you need to remain vigilant. Hackers are constantly devising new ways to hurt us, and so it’s important we consistently respond by strengthening our defenses and our abilities in fighting against the many threats we face online.

- Click to share on Facebook (Opens in new window)
- Click to share on Reddit (Opens in new window)
- Click to share on Twitter (Opens in new window)
- Click to share on Pinterest (Opens in new window)
- Click to email this to a friend (Opens in new window)