

# Checklist for Securing your Home Network



## Choose a Unique SSID

The SSID is the name you see when you connect to wifi. You want to make sure to choose a unique SSID.

## Choose a Unique WiFi Password

Make sure your wifi password is not even close to a password that you've used before. Make it long and unique. Better yet, [use this tool to make it a passphrase](#).

## Update your Wi-Fi Router

Just like your computer and your smartphone, your router needs to be updated. Make it a habit to log into your router once a month to check for updates. It only takes a few minutes.

## Change your Router Username

Many WiFi routers ship with the same default username ("admin") and password ("password"). Most people don't change these! You absolutely should.

## Pick WPA2 Encryption

When you set up your wifi network, you're asked to pick what kind of encryption you want to use. Choose WPA2. Other forms are easy to break. Also, if you're given a choice, always pick AES over TKIP.

## Turn on the Firewall

Some wifi routers come with a firewall built in. Search to see if yours does, and confirm that it's turned on. If not, it may be worth upgrading to one that does.

## Guest Networks

It might not be a bad idea to have your work computer on a separate guest network. Not all wifi routers support this, but many let you create a separate network, with a separate SSID and password.

## Get Notified when Someone Joins your Network

For \$99, a [Fingbox](#) sits on your network, monitors activity, and sends you notifications when unrecognized devices join your WiFi network. Your internet service provider may provide this service free of charge. Give them a call and ask!

## Do you get your WiFi through an ISP?

Many people get their wifi directly from their ISP (e.g., Verizon, Comcast). If that's the case, you may not have control over a lot of the items listed above. Feel free to walk through this list with them and ask which ones they'll handle vs. those that you should handle.