NOTE: Common routers such as Linksys, D-Link, Cisco, and Belkin offer specific walk through instructions on the companies' websites to achieve the appropriate router security as described above.

Best Practices

Create passwords that are sufficiently long and complex to include; upper and lowercase letters, numbers, and symbols.

Consider a multi-password phrase that does not consist of dictionary-based words. An example would be ILuvF00tb@77 from the phrase "I love football."

Use a cable to directly connect any stationary computers / devices to your home network to limit vulnerabilities presentedby wirelessly connected devices

Turn off your wireless network when you will not be using it for an extended period of time.

If you have guest-access set up for your network, ensure that it is also password protected.

If possible, turn on automatic updates for your network device's firmware. If they are not offered, periodically check for firmware updates on the network devices' website(s) and manually download and install them.

If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button usually located on the back of the router.

Position the router away from windows and as far into the interior of your house as possible to limit the range of the WiFi signal outside your home.

Accessing Your Router

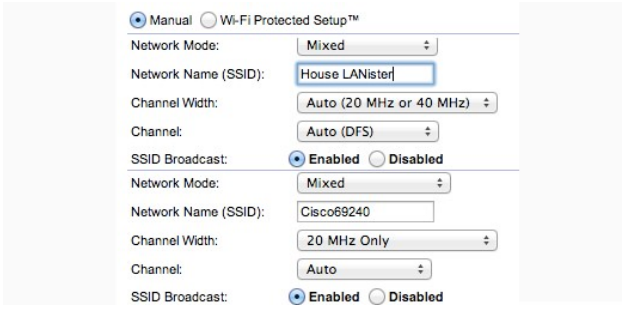
In order to change your WPA2 password you will need to access your router. In order to access your router, you must enter the appropriate IP address, username, and password. If you do not have this information, your Internet Provider should be able to provide it to you. **This information is also usually found on you're the back of your wireless router**.

It is **important** to understand that when your internet is being set up by your Internet Provider, they are not required to set it up using WPA2 (see the chart to the left). Recommend you ensure they set it up for you and provide the IP address for the Router's settings. That way, once they leave you can change the user name and password.

When changing your username and password for the WIFI, it is important to consider the following: choose a username that does not include you or your family members' names; creating a password that is long and complex. Lastly, it is important to change any Guest account password to something other than your Admin/family account password.

#

Creating a Unique SSID



#

When creating a name for your Wi-Fi (your SSID), it is important to consider who will be seeing it and what information it may give away about you and your family. For instance, if you decide to give it the family name (last name and perhaps number of family members), then anyone within range will be able to see your last name and likely piece together what the numbers represent. Alternately, if you name your SSID "FBI Van," that may call attention to your specific network and entice nefarious individuals into attempting to hack into it. It is recommended that you chose a name for your SSID that is generic in nature, providing no information about your family, address, date of birth, etc.

Disabling the SSID Broadcast

If you would like to hide your SSID so that it does not broadcast to the public, you can do so by scrolling down from where you created your SSID name till you find what's pictured above. Remember, that while it is nice to be able to disable the broadcasting of your SSID, it is important to note that it can be easily unhidden should an individual request to find "hidden Wi-Fis".

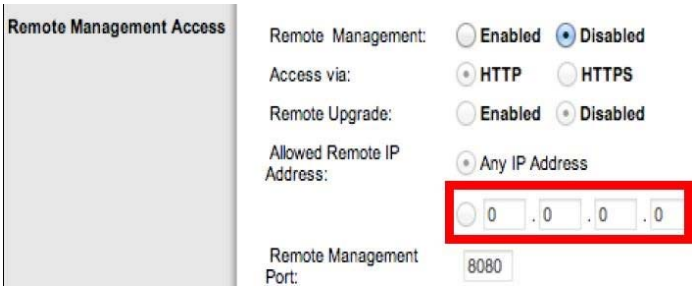
If you have smaller children in your home who have devices like the Leapfrog or Vtech games, and you disable your SSID broadcasting your child's device will not be able to find your network and connect to the internet. In order for those devices to connect, you will need to go back into your router settings and re-Enable the broadcasting of your SSID.

#

Router Firewall

The next two settings are usually found in “Router Settings” but you may have to look around a bit to find them. A firewall is a layer of security between your home network and the Internet. Since a router is the main connection from a home network to the Internet, the firewall function is merged into the router. Every home network should have a firewall to protect its privacy. A firewall does not secure against every kind of attack. For example, you still need to run a virus-checker on all your computers.

Remote Access

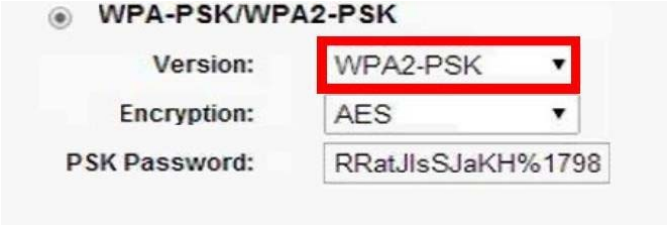


Check that the Remote Management IP Address is set to 0.0.0.0 to ensure that remote access is disabled. This will help to ensure that others cannot access your router remotely and without your permission.

Enabling HTTPS

HTTPS is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit. HTTPS enables encrypted communication and secure connection while on the internet. It is used by websites to provide enhanced security for customers OR financial transactions OR where PII is shared. Enabling HTTPS on your servers is a critical step in providing security for your web pages. It is recommended that you enable HTTPS in order to further protect you and your family while navigating the internet.

Encryption



Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select WPA2-PSK and also AES (a cryptographic cipher that is responsible for a large amount of the information security that you enjoy on a daily basis) for encryption. The PSK password should be long and examples, but different from the administrative router access password.

Wireless MAC Filtering

MAC address filtering allows you to define a list of devices’ MAC addresses so that only those devices can access your Wi-Fi. In order to do so, follow these steps: Add the MAC address of each device you want to authorize access to your network. Next, enter the MAC address and a brief description of the connected device for filtering. Finally, enable MAC address filtering to ensure that only approved computers and devices can connect to your router. Click the ‘Add’ button when done entering authorized devices.