WIFI SECURITY

Best Practices

- Create passwords that are sufficiently long and complex, and that 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.”
- Turn off your wireless network when you will not be using it for an extended period.
- 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 devices’ 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.

Wireless Router	Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identification (SSID)	Public name of a wireless network.
Pre-Shared Key (PSK)	Authentication mechanism that mandates a password. Adds additional security to wireless networks.
Hypertext Transfer Protocol Secure (HTTPS)	Uses various encryption protocols to add additional security to HTTP.
Media Access Control (MAC) Address	Unique, individual identifier assigned to computers and devices.

WiFi Security Level	Level of Security	Explanation
WEP	Low	Old encryption protocol. No longer considered a standard. Highest risk next to an “open” network
WPA	Low-Moderate	Old encryption protocol. Better than WEP but should not be used when more modern encryption is available.
WPA2	Moderate-High	WPA2-PSK (AES) is the most secure option which uses the latest wifi encryption.
WPA3	High	Approved and replacing WPA2 as the new and more secure option for wifi security. Not available on all devices.

WIFI SECURITY

Accessing Your Router

To change your password, log on to the router online. To do so, enter the appropriate IP address, username, and password. If you do not have this information, contact your Internet Provider.

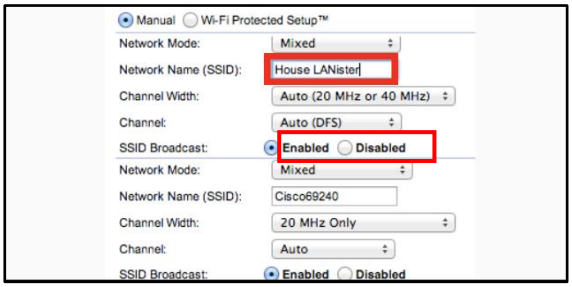
It is **important** to understand that when your internet is set up by the Internet Provider, they are not required to set it up using WPA2. It is recommended that you ask that your internet be set up with WPA2 and acquire the username and password at the time of service.

When setting or changing your username and password, it is important to use a strong password unrelated to any personal or family attributes.

Lastly, it is important to create a “Guest Account” and password separate from the “Admin”/”Family” account and password.

Creating a Unique Service Set Identifier (SSID)

When creating a name for your wifi (SSID,) it is important to consider who will be seeing it. For instance, if you decide on the family last name and 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 network and invite nefarious activities. It is recommended that you choose a name for your SSID that is generic in nature. If you would like to hide your SSID so that it does not broadcast to the public, simply select “Disabled” from the “SSID Broadcast” section. Note that while it is nice to be able to disable the broadcasting of your SSID, it can be “unhidden” by any individual requesting “hidden wifis.”



Firewall/Internet Protocol

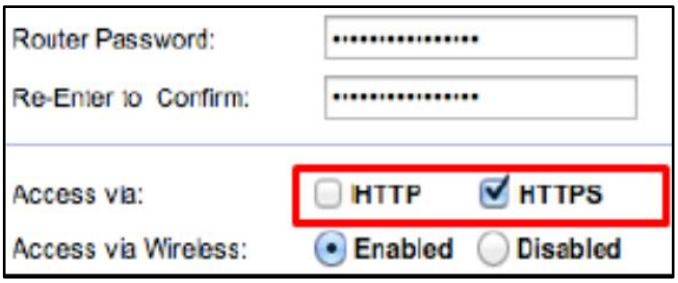
Internet Protocol (IP) is the infrastructure protocol that provides an identification and location system for computers on networks and routes traffic on the Internet. IPv4 is slowly being replaced with IPv6. It is important to understand that if you are running a VPN on your system, IPv6 may not be supported. Check the VPN provider’s website to see if both versions are supported. You can also visit a “What is my IP address?” site that pulls both IPv4 and IPv6 to check if you are properly covered. If IPv6 is not covered, you can choose to disable it through settings.

Children’s Learning Devices: If you have children who play with devices like Leapfrog or Vtech games and you disable your SSID broadcasting, these devices will not be able to locate your wifi network.

WIFI SECURITY

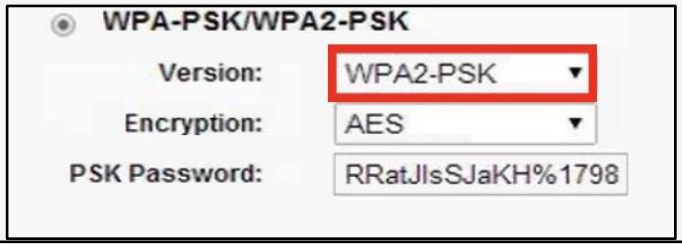
Enabling Hypertext Transfer Protocol Secure (HTTPs)

HTTPS is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data while in transit. HTTPS enables encrypted communication and secure connection while on the Internet. It is used by websites to provide enhanced security for customers' financial transactions or where personally identifiable information (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 AES (a crypto-graphic cipher that is responsible for a large amount of the information security that you enjoy daily) for encryption. The PSK password should be long and complex, but different from the administrative router-access password.



MAC Address Filtering

MAC address filtering allows you to define a list of devices' MAC addresses so that only those devices can access your wifi. In order to do so, follow the steps below:
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.