Securing Your Home Wifi ver-1.0

We are spending more time in our homes these days and this might not change anytime soon. We are now relying heavily on our home internet to work and transmit sensitive information.

This is a good time to review our internet access and put in place safety and privacy measures. We can start by revisiting our wifi router and put in place safety configurations.

20200515 | @BlocSheep@mastodon.social

SheepWreck

Consider that most of our wifi routers come with our internet subscription and we might have limited to no access in configuring these devices. Also, some wifi routers have limited settings so some of the items below might not be available on your devices.

A. Secure administration and maintenance.

1. Backup your wifi router configuration file. This will allow you to restore your wifi router to the previous working state. Make sure that your backup file is working by changing a few settings and then restoring the backup file.

2. Make sure you use a very strong admin password for the wifi router.

3. Check for updates or upgrades to your wifi router firmware. If available, it is generally a good idea to update or upgrade.

B. Secure wifi configuration.

1. Make sure you use a very strong wifi password.

2. Choose WPA2 only for your wifi security, but make sure that devices that connect to your wifi support WPA2.

3. Make sure that the name of your wifi or SSID is not associated to you, and your household. Don't use your name, surname and the like as your wifi name or SSID.

4. If available, hide your wifi name or SSID. Make sure that all of your devices can connect to a hidden wifi. You can determine this by actual testing.

5. Select the auto channel frequency of your wifi. This helps in ensuring that your wifi is accessible when there is a high concentration of wifi routers in your vicinity.

6. If available, choose 5Ghz only as the radio frequency of your wifi. Make sure that devices that connect to your wifi support 5Ghz. This limits the number of devices that can attempt unauthorised connection to your wifi.

7. If available, limit the transmit (TX) power of your wifi to cover only locations that you want to have internet access. Adjusting the TX power ensures that your wifi is not accessible, for example, along the street outside of your house. You can determine this by actual testing.

8. If available, configure and activate the guest wifi. This is useful in cases where your visitors request for internet access. A guest wifi should have a different wifi name or SSID and password from your main wifi.

C. Limiting the number of connected devices.

1. Configure your wifi router to limit the number of device connections. This is done by assigning a limited range of IP addresses that the wifi router can provide to connected devices, This feature is usually found in the LAN Settings of your wifi router.

2. Assign specific IP addresses to devices connecting to your wifi router. You need to get the MAC addresses of the devices in order to assign IP addresses. This is commonly referred to as Static IP Address Binding. This works in conjunction with point 1 above. Doing both limits the the number of connections to your wifi router and also limits the connection to only authorised devices

D. Securing your internet traffic.

1. Configure your wifi router to provide Secure DNS servers. You can add/change this in the LAN Settings of your wifi router. You can use DNS Server IP addresses 9.9.9.9/49.112.112.112 from https://quad9.net, or 1.1.1.1/1.0.0.1 from https://www.cloudflare.com. This DNS servers are recommended for their focus on privacy and security.

2. If available, configure your wifi router VPN client. This will require a VPN subscription. When configured, data traffic of devices connected to your wifi router passes through the VPN service. This helps if you don't want your internet service provider to see what sites you are accessing on the internet.

Once everything is working, make sure you backup your configuration file. This ensures that your working wifi router configuration will be available for restoration if anything goes wrong.