HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #148
February 23rd, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

WiFi Router Security

A Wi-Fi router is our window to the Internet. However, it is also a gateway for hackers and cybercriminals to hack our computer/laptops and smart home systems. Having an open wireless network can be a security risk as it may allow anyone who is close enough to your router to access your network.

To make your Wi-Fi router cyber attack proof follow these tips and you'll be well ahead of most home Wi-Fi users. While you will never be 100 percent secure against sophisticated cyber attacks and crafty social engineering schemes but this tips will help you keep your Wi-Fi routers safe from run-of-the-mill hackers.

5 Ways to Secure Your Wi-Fi Router

#1 Change Your Router Admin Username and Password

By default, every Wi-Fi router comes with a generic username and password which is easily available on the Internet and can be easily used against you. As soon as you first connect your Wi-Fi router to the Internet change them both. Immediately! (We are not talking about the passworded to join your WiFi network, this is a different password and many people don't realize this.) If you are a forgetful person and can't remember usernames/passwords, you should jot down the new Wi-Fi username and password in your diary or notebook because you can't reset usernames/passwords in a router. The only way out is to reset a router to its factory settings with the original default password which again should be changed immediately.

#2 Change the Network Name

Like username and password, every WiFi router comes with a default network name called the SSID. The service set identifier (SSID) is the name that's broadcast from your Wi-Fi so that you and other people (those whom you have allowed) to connect to the Internet. Most of us keep the SSID public using the default network name/SSID which gives a clue to hackers and cybercriminals that you are security-blind and an easy target. Also, if possible keep changing the SSID. It helps protect against someone who you had given emergency access just that once.

#3 Activate Encryption

Encryption is perhaps one of the best tools to protect your WiFi router from hack attacks and protect your PC/laptop and smart devices. It's the single most important thing you must do to lock down your wireless network.

Navigate to your router's settings and look for security options. You can access manuals of various routers online. In the settings panel, turn on WPA2 Personal or WPA2-PSK. Set the encryption type to AES. Avoid TKIP option. Next, you will need to set your password. Keep a different password from the one you have kept for Wi-Fi router admin settings. Make this password hard to guess by using a mix of upper- and lowercase letters, numbers, and special characters.

#4 EnableFirewalls

Enabling a Firewall makes the job for hackers that much harder. In addition to the PC/laptop firewalls, your Wi-Fi router has a firewall built in that should protect your internal network against outside attacks. Activate it if it's not automatic. Some Wi-Fi router have SPI (stateful packet inspection) while others have NAT (network address translation).

#5 Update Router Firmware

Updating a software or firmware should be a habit. Just like with your PC/ laptop/smartphone operating system and browsers and other software are to be updated against latest cybersecurity threats from time to time, routers manufacturers release security patches against flaws and exploits. The updates for your WiFi routers are called firmware updates. Go into your router settings every month or so and do a quick check to see if you need an update, then run their upgrade.

This Week's Cyber Alerts:

Alert Issued 2/22/18 **Tot-Monitoring Camera Lets Miscreants Watch 10,000s of Kids Online**

Alert Issued 2/21/18 **Telugu 'Text Bomb' Will Crash Your iPhone in Secondsâ€"Here's How to Fix It**

Alert Issued 2/21/18 **Hackers Could Break into Tinder Accounts with Just a Phone Number**

Alert Issued 2/20/18 **43 Percent of Online Login Attempts Malicious**

Alert Issued 2/19/18 **Fraudulent Online Vehicle Sales**

Alert Issued 2/17/18 **120k FedEx Customer Files Spill from AWS S3 Silo**

Alert Issued 2/15/18 **Skype Can't Fix a Nasty Security Bug without a Massive Code Rewrite**

Alert Issued 2/14/18 **Microsoft to add Windows Defender Advanced Threat Protection support for Windows 7**

Alert Issued 2/13/18 **Killing Passwords in Windows 10 S is one of 7 big changes in Windows 10**

Alert Issued 2/12/18 **This Phishing Trick steals your Email and then Fools your Friends into Downloading Malware**

Thank you for subscribing to our email and I hope the information we have shared will make your online life a little easier.