Secure Routers and Configuration for Home or Small Business Networks

Introduction: Even if you have a modem/router for your Internet connection (e.g. cable modem, DSL modem, etc.), you still *must* add an additional router to your network for security reasons. Although the modem/router supplied by your Internet provider works fine for providing Internet access, adding an additional router provides a critical layer of security.

However, the average consumer-grade "home router" you may purchase at a big-box store is just not secure. (This includes routers made by LinkSys, DLink, Belkin, Netgear, ASUS, etc.) (See "**News Articles**" below for examples if you need convincing.) These insecure routers can be hacked/hijacked and used to read all your Internet traffic, distribute malware, infect your machine with ransomware, or be used as part of a bot-army to attack other networks. Don't be a part of this nonsense or allow all your information to be stolen. If you are concerned about cybersecurity for your home or small business environment, I encourage you to pay a little extra and purchase a "small business router" (as opposed to a cheap home router) **and** follow the simple advice below. (If you don't purchase a small business router, at least follow the other steps listed below and purchase a more secure router when it is time to upgrade.)

Note: I am not claiming that if you follow the steps here you absolutely will not get hacked, especially if you are a high-value target and have a motivated, well-funded organization out to steal your information. But I am saying that following the advice here will make your router much more likely to remain secure and make the "effort of compromising your device" a cost high enough to keep out all but the most determined and motivated attackers. (Why spend hours breaking into your house when your neighbor's backdoor is unlocked?)

If you are concerned about the security of your home or small-business network, then do the following:

1) **Buy A Secure Router**: Purchase a Small- or Medium-sized Business (SMB) Router. Most consumer-grade "home routers" purchased at big-box stores are not secure! See my list of suggestions below.
   a) Note: If you already have one of these cheaper routers and are not able to purchase a better one, then at least follow the rest of the steps in this list! (If you are really concerned about security or have highly sensitive data, then just upgrade now!)
2) **Change router password!** Change all default passwords on your router when you initially set it up, i.e. administrator password. (If you did not do that initially, it is critical that you change them now!)
3) **Turn off remote access features:** Unless you are intentionally configuring secure remote access to your router/network, you should turn off all remote access to your router from the Internet. If you do allow remote access, make sure it is only through an encrypted connection (VPN), with a very strong password, with 2FA enabled.
4) **Disable UPnP**: Turn off the Universal Plug-and-Play (UPnP) option (if offered by your router).
5) **Firmware Update**: Periodically/regularly update the router's firmware. (Do this when you first set it up and then a couple times each year.) This is important to patch vulnerabilities as they are regularly discovered and exploited by hackers.
   a) Turn on the auto-update feature if available.
   b) Make sure to carefully follow the directions on your router for updating the firmware. It is very simple and straightforward to update, but the directions need to be followed or you can brick your router (i.e. permanently break it; turn it into a brick!).

6) **Wi-Fi Configuration**: If you purchase a router with Wi-Fi capabilities, make sure to configure it for security (or turn off Wi-Fi if you don't use that feature).
   a) **Use WPA3 or WPA2**: If you use Wi-Fi, then turn on WPA2-Personal (WPA2-PSK) or WPA3-Personal (WPA3-SAE) with a complex (but memorable) password. (You will only use this password the first time a new user/device attaches to the Wi-Fi network.)
   b) **Disable WPS**: Wi-Fi Protected Setup (WPS) is not really "protected!" If you are especially concerned about sensitive information you own or transmit, and believe you may be targeted by hackers, then make sure to disable WPS on the Wi-Fi setup. This technology is known to have vulnerabilities that can be exploited by motivated hackers.
   c) Although not likely in this day and age, if you don't need Wi-Fi (or don't want that function combined with your router), you can purchase a small business router without Wi-Fi and add a separate Wi-Fi access point later.

Some Routers that are "More-Secure" that I Might Suggest:

(These can all be purchased from Amazon or other online retailers.)

1) **Orbi Wi-Fi Router: (Wireless, with a couple Wired connections.)**
   a) Most homes today use wireless networking almost exclusively, and rarely use a wired/cabled connection (or maybe use one or two). If this fits your situation, I highly recommend the Orbi family of wireless routers.
      i) Easy to Use: The router's features are easy to configure via an intuitive app on your smartphone.
      ii) Extend WiFi Network: They make it easy to add "satellite" routers (besides the main one) to extend the range of wi-fi access in your home or business; that no matter how large of home you have, the wi-fi can be available everywhere.
      iii) Security: I strongly suggest paying the yearly subscription for their NETGEAR Armor (network security software). This makes sure your router can scan your internet traffic looking for the malware. It also provides you with good antivirus software you can install on all your computers (currently BitDefender).
      iv) Security with Split Networks: Allows you to create a Home Wi-Fi network and a secondary one for your Smart-Home Devices (e.g. TV, electrical outlets, lights, refrigerator, etc.). It is smart to separate out the wireless network your computers and smartphones connect to, vs. other wireless devices.
      v) Child-Protection: The router allows you to activate Parental Controls that can be set to provide age-appropriate content, can set times of day to be active/inactive, and can monitor internet and app usage.
2) **Peplink Routers (Excellent for Small Businesses & Home Offices)**:
   a) If you need Wi-Fi and a powerful router with some security features, the Pepwave SOHO (Small Office, Home Office) router is an excellent choice. It has fast Wi-Fi and wired options.
   See: www.peplink.com/products/soho-routers/
   (You can purchase it at Amazon or at the Peplink store: https://estore.peplink.com/)
   b) If you don't need Wi-Fi, consider a router for the Small Branch Office or Small Business on this page: www.peplink.com/products/balance/model-comparison/
3) **Ibuquiti Routers (Dream Machine Pro) & WiFi Access Points:**
   a) If you want the ultimate security in an advanced firewall and business-grade security appliance for your home or business, then the Ibiquiti Dream Machine Pro is for you! However, this solution

would requires a tech savvy person to implement. This is more expensive and can be complicated, but it is powerful and offers strong security. (Feel free to reach out to me if you want help designing or installing this solution.)

i) The Dream Machine Pro: (https://store.ui.com/us/en/products/udm-pro) does not have built-in WiFi; they are a separate purchase. (See WiFi products: https://store.ui.com/us/en/category/all-wifi) There are a wide-array of Security Cameras that can be integrated into this solution.

News Articles:

Although some of these news articles are a little older, the problem still exists!

1) "Your router's security stinks: Here's how to fix it." www.tomsguide.com/us/home-router-security,news-19245.html (Jan. 2023)
2) "Don't use your home Wi-Fi before fixing these security risks" cyberguy.com/security/dont-use-home-wi-fi-before-fixing-security-risks/ (Sept. 2025)
3) "Sanctioned Bulletproof Host Tied to DNS Hijacking" https://www.databreachtoday.com/sanctioned-bulletproof-host-tied-to-dns-hijacking-a-30723 (Feb. 2026)
   "Routers - especially small office or home office routers - are a perennial hacking target given that the vast majority of their owners tend not to install updates." "The FBI in May 2025 admonished SOHO [Small Office-Home Office] router owners to upgrade any unsupported device, or to at least disable remote management."
4) "Cyber Criminal Proxy Services Exploiting End of Life Routers" (May 2025) www.ic3.gov/PSA/2025/PSA250507
5) "Is Your Router Insecure (and Does Your Router Maker Care)?" Jan. 2017, www.pcmag.com/news/351109/is-your-router-insecure-and-does-your-router-maker-care
6) "Oft-forgotten, why the humble router remains one of the most insecure devices in your home," March 2017, www.cbc.ca/news/technology/routers-cia-wikileaks-cyber-security-insecure-1.4017033

Note on Network Design for Small Businesses: If you are a SMB using wired Ethernet (with network cables), you do not need to purchase a router with enough ports for all computers; you can always plug a network switch into the router to give you more ports. Then, plug the cables from the computers into the switch. If you need help with configuring your network, contact a techie friend, hire someone with networking knowledge, or do online research if you just need a little extra guidance.