Secure Routers for Home or Small- or Medium-sized Businesses

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 will provide a critical extra 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 security 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.

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 what I am saying is that following the advice contained 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.

Note: If you already have one of these cheaper routers and are not able to purchase a better one, then at least follow the other advice on this page to change default passwords, regularly update the router's firmware, configure WiFi security, and upgrade as soon as you are possible. (If you are really concerned about security or have highly sensitive data, then just upgrade now!)

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

1) Purchase a Small- or Medium-sized Business (SMB) Router. See my list of suggestions below.
2) 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 the Universal Plug-and-Play (UPnP) option (if offered by your router).
4) 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 in order to patch vulnerabilities as they are discovered.
   a) 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!).
   b) As an example of a critical need to periodically update your firmware, even one of the small business routers recommended below (Cisco RV110W) came out with a critical fix for a newly discovered vulnerability. Please update your firmware now and set a reminder to update your router once or twice a year. See: tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex
5) If you purchase a router with WiFi capabilities, make sure to configure it for security (or turn off WiFi if you don't use that feature).
   a) If you use WiFi, then turn on WPA2-Personal (WPA2-PSK) with a complex (but memorable) password. (You will only use this password the first time a new user/device attaches to the WiFi network.)

b) If you don't need WiFi (or don't want that function combined with your router), you can purchase a small business router without WiFi and add a separate WiFi access point at a later date.
c) If you are especially concerned about sensitive information you have or transmit, and believe you may be targeted by hackers, then make sure to disable "WPS" on the WiFi setup. This technology is known to have vulnerabilities that can be exploited by motivated hackers.

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

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

1) **Peplink Routers for Small Businesses**:
   a) If you need WiFi and a powerful router, the Pepwave Surf SOHO router is an excellent choice. It has 802.11ac (fastest current WiFi), and Gigabit Ethernet (1,000 Mbps wired).
   See: www.peplink.com/products/pepwave-surf-soho
   - Purchase it at Amazon or here: http://3gstore.com/product/4136_surf-soho-4g-router-with-80211ac.html (The 3G Store offers great technical support, documentation, and configuration videos.)
   b) If you don't need WiFi, consider a router for the Small Branch Office or Small Business on this page: www.peplink.com/products/balance/model-comparison/
      i) The Peplink Balance 20 Dual-WAN Router (BPL-021) would be adequate for any home and for most any small business.
2) **Cisco Small Business Routers**: See this page: www.cisco.com/c/en/us/products/routers/small-business-rv-series-routers/models-comparison.html
   a) If you need a basic router with WiFi capabilities, check out the RV110W. It has 802.11n (WiFi), and Fast Ethernet (100 Mbps wired).
      i) **Update your firmware for this router - February 2019.** See: tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex
   b) Cisco typically builds routers with security in mind AND regularly provides updates for vulnerabilities that are discovered.
3) **ASUS RT-AC66U with Upgraded Firmware**: Another security professional suggests using the ASUS RT-AC66U with a security-hardened firmware upgrade. This configuration takes a bit more work than setting up one of the ones I have suggested above, but he gives very clear directions and his configuration looks solid: http://dfarq.homeip.net/recommended-asus-rt-ac66u-settings (Don't try this unless you are somewhat technically-minded and want to spend time tweaking your hardware.)

News Articles:

1) "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
2) "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
3) "ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk," Feb. 2016, www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put
4) "WikiLeaks, Home Routers and the CIA," March 2017, www.routercheck.com/2017/03/10/wikileaks-home-routers-cia/

5) "Universal Plug and Play" (UPnP) used for hacking into router. arstechnica.com/security/2017/06/advanced-cia-firmware-turns-home-routers-into-covert-listening-posts

Resources for Further Research and Reading:

1) See this page for "What can go wrong if your router gets hacked": routersecurity.org/whatcangowrong.php
2) A great place for researching all items about router insecurity, WiFi insecurity, etc.: www.routercheck.com
3) "Why You Should Invest in a Business-Grade Router": eccitsolutions.com/why-you-should-invest-in-a-business-grade-router
4) "What Separates Business Routers from Consumer Routers": You can read the entire article if you want the details. But at least notice the order of priorities as listed in these headings:
   "Consumer Router Priorities: Speed, Media Streaming, and Security"
   "Business-Class Router Priorities: Security, Remote Access, and Scalability"
   www.pcworld.com/article/256683/what_separates_business_routers_from_consumer_routers_.html
5) If you are interested in more general research on this topic, please see: routersecurity.org

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.