



Wi-Fi Security

Configure and Secure Your Wireless Network

Wireless networking (also known as *Wi-Fi*) is one of the fastest growing areas in computer and networking technology. Never before has it been so cheap and easy to network a home, school, or small business. However, as painless as purchasing and installing the hardware is, it remains fairly difficult to secure a wireless network. In order to effectively lock down a Wi-Fi network so that outsiders cannot steal bandwidth or intercept network traffic, a few extra steps need to be taken after the equipment is set up.

This collection of resources should help readers to:

- Make informed decisions about purchasing networking hardware
- Install a wireless network
- Properly configure and secure that wireless network

Books

Briere, D., Bruce, W., & Hurley, P. (2003). *Wireless home networking for dummies*: John Wiley & Sons, Inc.

Since its inception, the *For Dummies* series of books has been very popular with readers who need basic coverage of a topic. From the time I borrowed *DOS For Dummies* from my mother back in the late '80s, I have believed in the mission of the series - providing easy to follow entry-level technical instruction to readers for about half the price of what most technical books cost.

The book itself seems cheaply produced, having thin pages, a fairly stock layout, and sometimes low-quality illustrations and photographs. For the price this lack of polish is acceptable, though [Absolute Beginner's Guide To Wi-Fi Wireless Networking](#) (2004) by Que Publishing is actually cheaper, and contains none of these quality deficits.

Wireless Home Networking For Dummies provides a good introduction to the ins and outs of wireless networking. Setting up and securing a network at home or at a small business is covered in depth. Choosing hardware and supporting various platforms and security methodologies also get decent coverage.

Davis, H. (2004). *Absolute beginner's guide to wi-fi wireless networking*. Indianapolis: Que Publishing.

Because I have experience with Wireless Networking, it is difficult to judge whether this book is written appropriately or contains enough information to provide true beginners with the information they need to be successful setting up a wireless network. However, the book contains a wealth of information for a technical book that costs less than \$20.

The layout is very attractive, full of large, clear, and illustrative photographs and diagrams. The typography and use of graphics have a youthful, "hip" feel. This may turn off some mature and/or technical readers, but I don't think those people are this book's target readers.

The *Absolute Beginner's Guide* series by Que Publishing seems to be a direct rival of the *For Dummies* series by John Wiley & Sons. The list price of this book is 3 dollars cheaper than the otherwise very similar [Wireless Home Networking For Dummies](#) (2003).

This book covers the wireless standards, gives good tips about purchasing hardware, and explains deploying and securing wireless networks. The text is vendor and platform neutral, covering equally the various networking equipment manufacturers and Macs, Windows PCs, and PDAs. Much attention is given to finding and getting connected to wireless hotspots outside of home and work. The book also explores the "culture" of wireless networking, giving fair treatment to non-standard wireless hardware, war-driving, war-chalking, and other fun and interesting aspects of wireless networking.

Outmesguine, M. (2003). *Wi-fi toys: 15 cool wireless projects for home, office, and entertainment*. Indianapolis: Wiley Publishing, Inc.

This is the ultimate Wi-Fi geek's handbook. No information for beginners can be found in this book, but there are a number of good avenues to travel down if you're comfortable with wireless networks and basic tool use. If I had a lot of time and a little more money, I'd do almost every project in this book, starting with the wireless digital photo frame.

Ross, J. (2003). *The book of wi-fi: Install, configure, and use 802.11b wireless networking*. San Francisco: No Starch Press.

I've been a fan of No Starch Press for some time. This publisher's *The Book of JavaScript* by Dave Thau (who wrote the [JavaScript tutorials on Webmonkey](#)), is one of my favorite books. It can't be assumed that because a publisher produced one high-quality book that its other books will be just as valuable. In this case, however, with *The Book Of Wi-Fi*, I believe the publisher has outdone itself. The book deserves a place on the bookshelf of any wireless networking guru (or wannabe guru).

The book strives to present a complete picture of wireless networking without being too bloated or over-technical. The author writes in a friendly and accessible fashion. While many books cover Wi-Fi for the Windows and Mac platforms, this book goes a step further by giving equal share to the Linux operating system. Since getting Wi-Fi working in Linux can be a little challenging, it's good that at least one book addresses this topic - and in this case the topic is addressed well.

The Book of Wi-Fi has two flaws that I can see:

1. It covers some highly technical areas. Though written for a general audience and mostly easy to read, those completely new to wireless networking won't find a good starting point with this book. Those readers would be better off with [Wireless Home Networking For Dummies](#) (2003) or a similar title.
2. The book is very focused on 802.11b. Since much of the Wi-Fi world is moving toward 802.11g and beyond, the narrow focus of this book, while covering the lowest common denominator and therefore not alienating potential readers, is lacking in currency to a certain degree.

Online Resources

Exploiting and protecting 802.11b wireless networks. Retrieved July 30, 2005, from <http://www.extremetech.com/article2/0,1697,1152933,00.asp>

This page is an excellent tutorial about securing wireless networks. However, readers unfamiliar with all of the Wi-Fi acronyms (AP, SSID, WEP, etc.) will want to stay away from this one.

Securing your wireless network. (July 1, 2004). Retrieved July 30, 2005, from <http://www.quepublishing.com/articles/article.asp?p=339052>

Unlike many online tutorials about securing Wi-Fi networks, this page does a good job of starting from the beginning - explaining the difference between default (insecure) wireless networks and those that are properly configured and secured. This tutorial also includes lot of helpful screenshots of the various configurations screens a Windows user may encounter.

Securing your wireless network. Retrieved July 30, 2005, from http://www.practicallynetworked.com/support/wireless_secure.htm

This Webpage is a great intro to securing an existing wireless network. However, because it is short and dense, and uses more buzzwords that it defines, it may not a good resource for the technically uninitiated. Includes several good links to other tutorials including a good explanation of when and how to use WEP.

Flickenger, R. (2001, July 5, 2001). Antenna on the cheap (er, chip). Retrieved August 4, 2005, from <http://www.oreillynet.com/cs/weblog/view/wlg/448>

This page doesn't have much to do with wireless security, though creators of antennas such as the classic Pringle's® can antenna may be able to exploit your wireless network from a considerable distance. If you are ready to start hacking your wireless connection, consider making a long-range antenna out of a recycled food container. If not, a [commercial version](#) is available. Some *cantenna* experts feel the potato chip can is not an optimal size and diameter, and recommend [soup or coffee cans](#) instead.

Appendix A: Wi-Fi Vendors

- 3Com - <http://www.3com.com>
- Apple - <http://www.apple.com/airport/>
- Belkin - <http://www.belkin.com>
- Cisco - <http://www.cisco.com>
- D-Link - <http://www.dlink.com>
- Linksys - <http://www.linksys.com>
- Netgear - <http://www.netgear.com>
- US Robotoics - <http://www.usr.com>
- And several hundred smaller companies and OEMs (Original Equipment Manufactures)

D-Link, *Linksys*, and *Netgear* are the brands you are most likely to see on the shelf at your local Office Depot, Fry's, or Best Buy. Many wireless users have a favorite (or least favorite) company among these vendors. However, the hardware inside the equipment distributed by all of these companies comes from a fairly small list of chipset manufacturers, so you are likely evaluating very similar products when comparing the models of these various brands.

In my experience, a faulty product has less to do with the quality control of a particular vendor, and more to do with an overall potential lack of quality that comes with inexpensive, mass-produced products. Reading user-contributed online reviews (such as those at amazon.com or epinions.com) seems to confirm this belief.

Appendix B - Wi-Fi Glossary

802.11 - A group of networking standards established by the Institute of Electrical and Electronics Engineers (IEEE). There are several versions of 802.11, the most popular of which are 802.11b, 802.11a, and 802.11g. The standards differ by the theoretical speed can be achieved and which spectrum the standard uses.

Access Point - A wireless access point is similar to the base-station of a cordless phone, except that a base-station generally only communicates with one phone, whereas an access point can distribute network traffic to many wireless clients (in many cases up to 255).

AP - [Access Point](#)

Broadband - A generic term for a fast Internet connection. Generally, to be considered broadband, a connection must be faster than dial-up (e.g. 56k modem). [DSL](#), cable, satellite, and fiber-optic are all examples of broadband connections which may be available to a home user.

DSL - Typically, a wireless access point shares a [broadband](#) connection, such as DSL, among several users.

Encryption - In order to protect wireless traffic from being intercepted and viewed by others, it should be encrypted

ESSID (see [SSID](#))

Hotspot - A hotspot is a public wireless access point. Some hotspots are free, but most require some kind of subscription or per-use payment. Hotspots are found at hotels, airports, coffee shops, conventional halls, bookstores, and many other places.

PDA - *Personal Digital Assistant*. Any of a variety of handheld computers, many of which are able to connect to wireless networks.

Router - A device that accepts and redistributes network traffic. Most off-the-shelf wireless [access points](#) are also routers, allowing a [broadband](#) connection to be shared among several wireless users.

SSID - *Service Set Identifier*. The SSID is the broadcasted name of a wireless network.

WEP - *Wireless Equivalency Protocol*. WEP was the original method for [encrypting 802.11b](#) wireless traffic. The protocol has a fundamental flaw in that it can be *cracked* (decrypted) by anybody using any one of several freely downloadable tools. [WPA](#) is a newer, and much more secure method of encrypting wireless traffic. Older wireless hardware does not support WPA, so in most cases it is recommended that WEP be used, as weak encryption is better than none.

Wi-Fi - *Wireless Fidelity*. Wi-Fi is a nickname for wireless networking. Also, products reviewed and approved by the [Wi-Fi alliance](#), are guaranteed a higher likelihood of interoperability.

Wireless Networking - Connecting to a network and/or the Internet without wires. Wireless networking generally means being connected to an [access point](#), but may also refer to connecting to the networks used by mobile phones.

WiMAX - Based on the 802.16 standard, WiMAX is a wireless technology of future that potentially will provide a 30 mile wireless network accessible to hundreds of homes and/or businesses.

WPA - *Wi-Fi Protected Access*. A newer and more secure [encryption](#) and access-control system for [802.11](#). Meant to replace [WEP](#).

The Wi-Fi Alliance provides a more complete [listing of wireless terms](#).