



# 10 WAYS TO SECURE YOUR SMALL BUSINESS NETWORK

---

## 10 WAYS TO SECURE YOUR SMALL BUSINESS NETWORK

---

Maintaining a secure small business or home network isn't easy, and even for an old hand in IT, it still takes time and energy to keep things locked down. Here are 10 of the most critical steps you can take to keep your data from ending up elsewhere, and none of them take much time or effort to accomplish.

**1. Use encryption on your wireless access points (AP).** Many site surveys have found half or more of all wireless networks are wide open, ripe for anyone to gather all the traffic and perhaps record your sensitive information by sitting in a nearby parked car. Some people mess around with locking down MAC addresses, but that gets unwieldy and a better solution would be to use WPA2 encryption. WPA2 is far better than other encryption methods that are more easily broken into.

**2. If you have a wireless network, make sure to hide your SSID** (service set identifier), or at least change its name to something common. All wireless routers should have obscure IDs when they announce themselves to the world. Rather than put in any real information that can make it clear who owns the router or that can divulge your location or business name, such as "Acme Systems, here on the 4th floor" or the product name like "Netgear," use something innocuous like "wireless" or "router1" that doesn't give away anything really critical. In my last apartment, I had neighbors who used their apartment numbers for their IDs, making it real easy to figure out who's router was where.

**3. If your router (wired or wireless) has a Web management interface, disable access from the outside network.** And change the admin default password now. Most routers have the ability to do both quite easily. You don't want anyone else coming in and changing your settings or reading your log files.

**4. Make sure all of your PCs use antivirus software and if you're using Windows, add antispyware protection.** This seems obvious, but it bears restating. And while you are at it, check to make sure that all of your antivirus subscriptions are current. Anything out of date isn't doing you any good. In my support travels, I've found that this is a very common lapse among my neighbors.

**5. If you are running a Web server on your LAN, put it on a DMZ.** If your router doesn't have a DMZ, get a new router. Better yet, move to a collocation facility where someone who knows what he is doing can manage it. Having your own local Web server sounds like a good idea, but is a real security sinkhole, and many cable networks have made it harder to host your own from your home network anyway. So why worry? Only allow VPN based access to your webmail.

**6. Speaking of Web servers on the Internet,** if you have them, you should scan regularly for exploits. There are many sites that can do this, two of my favorites are SPIynamics.com and Qualys.com. Also, make sure to keep track of your domain registry and change all of your access passwords regularly.

If you update your Web content, don't use FTP or Microsoft's Web page creation tool, FrontPage; instead, find more-secure methods that don't send your access passwords in the clear. You can learn about other ways to protect your Web site at OWASP.org.

7. **Use a VPN (virtual private network)** for access back to your local LAN or your remote Web server. There are many to choose from, such ones from SonicWall and Fortinet, which are designed for small business owners.

8. **Disable file/print sharing on everything other than your file server.** And if you don't have a file server, buy one now. You don't need it on each desktop, and that just causes more vulnerabilities. This is particularly important for laptop users: You don't want to be broadcasting your entire file system to everyone around you at the airport or hotel, which is something that I often see when I travel and check for open network shares.

9. **Use whole disk encryption on all laptops that will ever leave home.** You never know when someone will steal your data or break into your car or hotel room and lift the laptop. I like PGP Disk, but there are others that cost next to nothing and provide plenty of protection. If you are in the habit of carrying around USB thumb drives with your data, then use one of the more modern U3 drives that work with Windows and are at least password-protected to keep your data away from others.

10. **Start doing regular off-site backups now.** At least start with making copies of your key customer and business data, and then make sure you cover your personal files, such as family photos and the like. Now is the time to cook up something simple. Burn DVDs and take them home, or make use of one of the online storage vendors such as eVault and Amazon.com's S3. They cost less than \$100 a year (Amazon's less than \$10 a year) and can save your data in case of fire, theft or just carelessness. If you have two PCs in two different locations, sign up for Microsoft's Foldershare.com free service to synchronize your data.

Now, there are plenty of other security options that will buy you peace of mind and make it harder for hackers, but these 10 items are easy to implement, don't cost much in terms of your time and money, and will have big security payoffs. Try to attempt one item each week and you'll sleep better at night.

*David Strom is a writer, editor, public speaker, blogging coach and consultant. He is a former editor in chief of Network Computing and Tom's Hardware and has his own blog at <http://strominator.com>. He can be reached at [david@strom.com](mailto:david@strom.com).*