WIRED

<< Back to Article
COMMENTARY

Security Matters

Commentary by Bruce Schneier

Steal This Wi-Fi

Bruce Schneier 01.10.08 | 12:00 AM

Whenever I talk or write about my own security setup, the one thing that surprises people -- and attracts the most criticism -- is the fact that I run an open wireless network at home. There's no password. There's no encryption. Anyone with wireless capability who can see my network can use it to access the internet.

To me, it's basic politeness. Providing internet access to guests is kind of like providing heat and electricity, or a hot cup of tea. But to some observers, it's both wrong and dangerous.

I'm told that uninvited strangers may sit in their cars in front of my house, and use my network to send spam, eavesdrop on my passwords, and upload and download everything from pirated movies to child pornography. As a result, I risk all sorts of bad things happening to me, from seeing my IP address blacklisted to having the police crash through my door.

While this is technically true, I don't think it's much of a risk. I can count five open wireless networks in coffee shops within a mile of my house, and any potential spammer is far more likely to sit in a warm room with a cup of coffee and a scone than in a cold car outside my house. And yes, if someone did commit a crime using my network the police might visit, but what better defense is there than the fact that I have an open wireless network? If I enabled wireless security on my network and someone hacked it, I would have a far harder time proving my innocence.

This is not to say that the new wireless security protocol, WPA, isn't very good. It is. But there are going to be security flaws in it; there always are.

I spoke to several lawyers about this, and in their lawyerly way they outlined several other risks with leaving your network open.

While none thought you could be successfully prosecuted just because someone else

used your network to commit a crime, any investigation could be time-consuming and expensive. You might have your computer equipment seized, and if you have any contraband of your own on your machine, it could be a delicate situation. Also, prosecutors aren't always the most technically savvy bunch, and you might end up being charged despite your innocence. The lawyers I spoke with say most defense attorneys will advise you to reach a plea agreement rather than risk going to trial on child-pornography charges.

In a less far-fetched scenario, the Recording Industry Association of America is known to sue copyright infringers based on nothing more than an IP address. The accused's chance of winning is higher than in a criminal case, because in civil litigation the burden of proof is lower. And again, lawyers argue that even if you win it's not worth the risk or expense, and that you should settle and pay a few thousand dollars.

I remain unconvinced of this threat, though. The RIAA has conducted about 26,000 lawsuits, and there are more than 15 million music downloaders. Mark Mulligan of Jupiter Research said it best: "If you're a file sharer, you know that the likelihood of you being caught is very similar to that of being hit by an asteroid."

I'm also unmoved by those who say I'm putting my own data at risk, because hackers might park in front of my house, log on to my open network and eavesdrop on my internet traffic or break into my computers. This is true, but my computers are much more at risk when I use them on wireless networks in airports, coffee shops and other public places. If I configure my computer to be secure regardless of the network it's on, then it simply doesn't matter. And if my computer isn't secure on a public network, securing my own network isn't going to reduce my risk very much.

Yes, computer security is hard. But if your computers leave your house, you have to solve it anyway. And any solution will apply to your desktop machines as well.

Finally, critics say someone might steal bandwidth from me. Despite isolated court rulings that this is illegal, my feeling is that they're welcome to it. I really don't mind if neighbors use my wireless network when they need it, and I've heard several stories of people who have been rescued from connectivity emergencies by open wireless networks in the neighborhood.

Similarly, I appreciate an open network when I am otherwise without bandwidth. If someone were using my network to the point that it affected my own traffic or if some neighbor kid was dinking around, I might want to do something about it; but as long as we're all polite, why should this concern me? Pay it forward, I say.

Certainly this does concern ISPs. Running an open wireless network will often violate your terms of service. But despite the occasional cease-and-desist letter and providers

getting pissy at people who exceed some secret bandwidth limit, this isn't a big risk either. The worst that will happen to you is that you'll have to find a new ISP.

A company called Fon has an interesting approach to this problem. Fon wireless access points have two wireless networks: a secure one for you, and an open one for everyone else. You can configure your open network in either "Bill" or "Linus" mode: In the former, people pay you to use your network, and you have to pay to use any other Fon wireless network. In Linus mode, anyone can use your network, and you can use any other Fon wireless network for free. It's a really clever idea.

Security is always a trade-off. I know people who rarely lock their front door, who drive in the rain (and, while using a cellphone) and who talk to strangers. In my opinion, securing my wireless network isn't worth it. And I appreciate everyone else who keeps an open wireless network, including all the coffee shops, bars and libraries I have visited in the past, the Dayton International Airport where I started writing this and the Four Points Sheraton where I finished. You all make the world a better place.

Bruce Schneier is CTO of BT Counterpane and author of* Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. You can read more of his writings on his website.