

Re: using wireless internet without security

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2006-12/msg00078.html>

- *From:* comphelp@xxxxxxxxxx (Todd H.)
 - *Date:* 08 Dec 2006 09:24:38 -0600
-

"Erik" <erikbach-fjerndette-@xxxxxxxxxxxxx> writes:

Some families in my neighbourhood are using wireless internet without any security.

I know that using security (password or Mac-address filtering) is often advisable

MAC filtering is very easily bypassed by anyone other than casual snoopers. The same can be said of WEP encryption which can be broken in minutes using freely available tools.

, but I would like to know better what risks are involved by having an open wireless network:

1) Can virus spread across a wireless network between computers which are only sharing the internet connection?

Absolutely, but that's an issue orthogonal to the whole wireless equation, and more a risk of putting a group of computer on the same network.

However, if you lack a hardware firewall or home office router today, you'll be adding no additional risk of network based piece of malware spreading to you from the internet right now. If you have a "software firewall" or are using windows firewall on your machine already, and if you configure it not to trust computers on your local area network, you'll be in as good a shape as you are against internet based attacks today.

2) Is it possible for users sharing an internet connection to gain access to files on other computers sharing the connection?

Re: using wireless internet without security

Absolutely. With similar caveats above though. The difference between an internet based threat and one of a local area network is often in how the packet filter software ("software firewall") is configured. Many of these programs trust the computers on your LAN implicitly, which if file sharing is being used, would leave them open to a neighbor jumping on the open access point.

Other more worrisome things, however, would be johnny neighbor jumping on the open access point, running script kiddie attacks against government networks, then men in black start knocking on the front door inquiring about the illegal hacking activity originating from that internet connection.

If you want to frighten the neighbors into action, that's the threat that's most compelling. And add that with directional antennas, the attacker could be up to a mile away.

WPA security with a strong, random, long passphrase is what they should implement. Don't bother with WEP or MAC based filtering, and SSID hiding tends to cause the legitimate owner more headache in getting legit computers configured than it provides in any obscurity.

Best Regards,

—

Todd H.

<http://www.toddh.net/>

.