SECURITY REPORT CARD

A free 7-point security check of your Wireless Internet Hotspot has revealed the security issues checked below.

_____   _____   _____
Business Name   Grade   Date

☐ **YOU HAVE AN "EVIL TWIN" OR "MAN-IN-THE-MIDDLE"**
PROBLEM: Another wireless network is using your network name. Customers may be tricked into connecting to the "Evil Twin" network where personal data could be stolen.
SOLUTION: Probably innocent if your router is using the default name. Change name.

☐ **BUSINESS COMPUTERS PUBLICLY ACCESSIBLE**
PROBLEM: Your business computers appear to share the same network as your public hotspot. This leaves your private business data exposed to anyone who connects.
SOLUTION: Isolate business computers with a firewall or by creating a private network.

☐ **FIREWALL NOT ENABLED**
PROBLEM: Several recent studies have shown that a computer placed on the Internet without protection is attacked within 4 minutes. Viruses are not good for your business!
SOLUTION: Your router's instruction manual describes how to turn on firewall protection.

☐ **CUSTOMERS' HARD DRIVES EASILY ACCESSIBLE**
PROBLEM: Computers on your network can talk to one another. Some routers even feature one-click access to your customers' hard drives. This is a dangerous condition.
SOLUTION: Create a "VLAN" or inform your customers of the risk to their privacy.

☐ **WIRELESS SIGNAL REACHES WELL BEYOND PREMISES**
PROBLEM: Since anyone in range of your wireless network can connect, confine your signal to an area in your control. Internet connection abuse usually occurs out of sight.
SOLUTION: Reduce your signal strength or implement access control on your network.

☐ **INTERNET AVAILABLE AFTER BUSINESS HOURS**
PROBLEM: A criminal is less likely to commit a crime if he feels watched. Never leave your hotspot unattended. As you lock the doors at night, be sure to lock your Internet.
SOLUTION: Usually you can just unplug your router at night. Some feature scheduling.

☐ **DEFAULT OR NO PASSWORD ON WIRELESS ROUTER**
PROBLEM: Knowing a router password unlocks all kinds of things: your customer's identity, the ability to reroute your Internet connection and the ability to lock _you_ out.
SOLUTION: Your user's manual describes how to set a configuration password.

Act now. Reduce your exposure to and liability for Internet crime by correcting these vulnerabilities.

Did you know...

By providing your customers Internet access, **you are an Internet Service Provider (ISP)** under federal law; a small communications company.

To meet your **legal obligations** and protect your business from **litigation**, you should be taking on many of the functions of a large ISP.

Here are some quick guidelines:
- ❍ Record Who Is Connecting and When
- ❍ Do Not Leave Your Hotspot Unattended
- ❍ Properly Configure Your Equipment
- ❍ Employ an Internet firewall
- ❍ Respond to court orders and subpoenas
- ❍ Post an Acceptable Use Policy

We can help!

Our **Professional Hotspot Management** service will take security worries off your shoulders and take care of all of your responsibilities as an ISP.

But we don't stop there.

We will help you reach more customers by relentlessly promoting your hotspot.

We will be there for you when your hotspot is down or a customer has trouble connecting.

Finally, you'll have access to our exclusive ControlSpot software for proactive customer management and user personalization.

Your wireless Internet hotspot is **attractive to criminals** because it is **anonymous** and **unattended**.

Identity Theft ● SPAM Senders ● Online Predators ● Harassment ● Copyright Infringement ● Terrorism