

# Wireless Network Disclaimer

The Computer Wizard  
www.thecomputerwizard.biz  
3131 Custer Rd #175  
Plano, TX 75075  
972.781.0011

The current crop of wireless networking products operate in the 2.4GHz frequency range. As a result, they are compromised by 2.4GHz cordless phones and numerous other environmental conditions. Many manufacturers produce 5GHz systems, which circumvent the problem of interference by cordless phones.

Things to consider when selecting and installing wireless network components:

1: **Antenna Style**... Internet Gateways and Routers with external antennae (preferably two) are more reliable than the units that have internal antennae. NICs also work better with external antennae, as the wave propagation is superior and the signal can escape the metal chassis of the computer. The USB interface seems to work the best overall, as it can be placed some distance (2 - 6 feet) from the computer itself, improving wave propagation and allowing you to adjust the location until you have optimum performance.

2: **Objects That Interfere With Wireless Signals**...

- Large-screen TVs will interfere with the signal if they are near the line-of-sight path between the gateway and the remote computer.
- Large masses of metal such as AC ductwork, fireplaces, vents and fire-floors will deplete the wireless signal.
- Brick walls, likewise interfere with wireless wave propagation.
- Cell phones and microwave ovens, when in use, can damage the integrity of the wireless signal.
- Other wireless networks close by.
- Cordless phones (yours or your neighbor's.)

3: **Multiple Access Points**... Some higher-end systems support 'repeaters' or multiple Access Points. By distributing two or three of these throughout your home or office you can get around the signal strength problems that may be caused by either distance or loss due to objects described under item 2 above. Multiple Access Points will not, however solve interference problems caused by 2.4GHz cordless phones.

4: **Security**... Anyone near you (neighbors or someone in a passing car) can access your home network if you use a wireless network without encryption. Don't think it can't happen to you. Just as there are people who write viruses, 'key' cars and TP houses, there are individuals with nothing better to do than cruise neighborhoods with a wireless network card and a laptop computer looking for something to vandalize.

Remember... "Your mileage may vary." Every wireless installation is different. With exactly the same set of components in a different building, entirely different results may occur. Your installation may work perfectly one day and disconnect everyone the next - or randomly disconnect only one or more users. There are no guarantees that any consultant can make regarding wireless networking, as there are too many variables to consider - and the end-user can do things that negatively impact wireless performance.

For instance:

Moving a Wireless Access Point or USB NIC only a few inches may render the system non-functional in some installations.

Adding a cordless phone - or using one in close proximity to a wireless computer or Access Point can knock all - or some computers off-line.

Power glitches can lock up the Wireless Access Point on some models and require a reset before wireless operation is restored.

A neighbor may add a wireless network or cordless phone that will interfere with your previously-solid wireless network.

Wireless networking is incredibly convenient - especially if you use a laptop in your home and need it connected to the rest of the world. But will it work? We have installations that work flawlessly. And we have some that are a 'moving target', where it works most of the time, but has to be 'rebooted' periodically to stabilize. Remember... Just because it worked yesterday doesn't mean it will work tomorrow.

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

The Computer Wizard  
3131 Custer Rd #175  
Plano, TX 75075  
972.781.0011