



# EC Group

a division of Electronic City, Inc.

## Securing Your Wireless

### SPAM

It is estimated that 95% of all email is considered spam. How much productivity is lost by your employees dealing with spam?

### WEB MONITORING

Cyberslacking in the workplace can lead to productivity loss, financial loss and legal liability.

The average employee spends 2.5 hours per day cyberslacking.

### VIRUS PROTECTION

Experts say that approximately 200 new computer viruses get introduced to the internet every month.

### DISASTER PREVENTION

How long would your business survive without a server, a workstation, data, phones or line of business application?

### IT BUDGET

Do you know how much you're *REALLY* spending on IT? We can help you identify leaks in your IT budget and stop them.

### CALL US TODAY!

520.622.1173

### VISIT US ON THE WEB @

WWW.ECGRP.COM

With over 50% of people admitting to having used someone else's wireless internet without permission, how can you stop your neighbors from stealing your Wi-Fi connection? Securing your wireless network is just a matter of following a few simple tips:

- **Use encryption** - Wireless routers give you the option of encrypting your data, so bank details and passwords can't be intercepted. Wi-Fi Protected Access (WPA and WPA2) is a much stronger encryption system for securing your communications than WEP, which can be easily cracked by hackers.
- **Use a password** - Set up a password for your wireless internet connection. Choose a strong password for securing your network - don't use the one that came with your Wi-Fi router or a dictionary word that is easy to guess or crack.
- **Don't broadcast the name of your wireless network** - The name of your wireless network, known as the SSID, should not be broadcast to passers by. In addition, choose an obscure hard-to-guess SSID name to make life harder for Wi-Fi hackers. SSIDs such as 'home', 'wireless' or 'internet' are not good choices.
- **Use MAC address filtering** - Wi-Fi routers and access points normally have the ability to prevent unknown wireless devices from connecting to the network. This works by comparing the MAC address of the device trying to connect to the Wi-Fi router with a list held by the router. Unfortunately, this feature is normally turned off when the router is shipped because it requires some effort to set up properly. By enabling this feature, and only telling the router the MAC address of wireless devices in your household, you'll be securing your wireless network against neighbors stealing your internet connection. Securing your wireless network using MAC address filtering is not a total solution as it is possible for a determined hacker to clone MAC addresses and connect to your Wi-Fi network, but this measure should still be taken to reduce the risks.
- **Restrict internet access to certain hours** - Some wireless routers allow you to restrict internet access to certain times of the day. For instance, if you know you will not need to access the internet from home between 9-5, Monday to Friday, then schedule your router to disable access between those hours.
- **Make sure your computers are properly secured** - Check you have up-to-date anti-virus, security patches, and client firewall software, this will help to protect your wireless network by stopping malware-based connection to your Wi-Fi.

**Call EC Group today if you need assistance with securing your wireless.**



4555 E. Broadway Blvd. Tucson, AZ 85711

Ph: 520.622.1173

Fax: 520.628.1214

Making Technology Make Sense

Hardware, Service and Support for more than 35 Years