4 TIPS TO KEEP YOUR WIRELESS NETWORK SECURE

Because wireless networks are particularly vulnerable to attacks, security is a primary concern. Wireless networks can be hacked by “war drivers“—who cruise around looking for a wireless signal to exploit. Usually war drivers are just looking for free Internet access, but sometimes they’re looking for confidential information such as credit card numbers.

Although a wireless network can never be totally secure, there are important steps you can take to minimize the risk:

1. Know how far your signal extends.

When you install a wireless network near public areas, it’s very important to know where your signal is going. If it’s easily picked up outside your business—perhaps from a parked car across the street or from the building next door—then you’ve

got a security problem. If you send a strong wireless signal into the coffee house next door to your business, chances are someone is going to try to take advantage of it.

A wireless analyzer can help you map exactly where your access points are sending their signals. This can help you arrange the access points in your network in order to minimize signals in public areas and maximize signals to your users. A wireless analyzer can also spot unauthorized wireless access points attached to your network as well as other wireless networks broadcasting in your area. A wireless analyzer may be a freestanding application or may be part of a wireless management suite. Newer wireless mesh products often feature cloud-based management that includes wireless analysis.

2. Separate your wired network from your wireless network.

To add a layer of security to your wireless network, separate it from your wired network by gathering all your wireless access points into a separate LAN connected to the DMZ port of your firewall. This makes the wireless network accessible, yet safely outside of your main wired LAN. Once you separate the wireless from the wired network, insist that anything that needs to be kept secure stay on the wired network. This includes confidential data such as credit card numbers, sensitive financial data, or corporate secrets of any kind. You can, however, freely use the wireless network for less-sensitive applications such as notebook computers for taking notes at meetings, PCs for temporary workers, computer hookups for trade show booths, and bar-code readers for inventory.

3. Use encryption to lock out unauthorized users.

Any wireless signal, no matter how heavily encrypted, can be broken into eventually. Encryption isn't perfect, but it can go a long way towards discouraging the casual hacker—the trick is to make breaking into your network so difficult that the hackers don't bother. Be sure to use encryption and, rather than easily hacked WEP, use higher-level encryption schemes such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).

4. Have a security plan and implement it. Seriously.

With a wireless network, as in any other network, it's important to have a security plan and then implement it. The biggest security problem with wireless security is that network administrators often fail to take even the simplest of steps to ensure security, do not activate encryption at all, or fail to change the default passwords.

When you fail to take these basic precautions, you leave your wireless network extremely vulnerable to casual hacking.

Yes, a wireless network is less secure than a wired network, but if you pay attention to your wireless network and implement a sensible security plan, you won't find yourself blindsided by its vulnerabilities.

Source: https://bboxblog.wordpress.com/2011/08/30/4-tips-to-keep-your-wireless-network-secure/