

Protecting Your Wireless Network

Make your wireless network a little harder to break into than the next firm's.

Wireless networks are very useful since they provide almost ubiquitous access to the Internet and thus your office network. But wireless access also brings with it security issues that could compromise the data on your laptop and, by virtue of that access your entire network. Here are five steps that you can take to protect your wireless access - at the office or at home:

1. Is wireless access really needed?

If you are in the office where there are plenty of network jacks, then use a land line instead of wireless. This offers the most protection against remote snooping and eliminates the wireless issue altogether. Some firms need to provide wireless access for clients so that they can gain access to the Internet and thus their own business data. That is where the next suggestion applies.

2. Implement wireless on a separate subnet.

A subnet is a separate network which is located on the same network but isolated from the main network for communication purposes. A wireless network should be set up on a separate subnet with no information that would allow information on the wireless subnet to be routed to the wired network. By using two unique and different networks, the traffic from the wireless network can be directed to the Internet only, while the traffic on the wired network can flow as it normally does.

3. Use WPA rather than WEP security.

WEP security was the first form of security provided with wireless networks. It consists of a difficult to remember series of digits and letters of two distinct lengths. WEP security can be defeated in mere minutes nowadays and is no better than having no wireless security at all. Most devices released over the past 4 years can handle a higher form of security called WPA. When setting up a wireless network, use WPA (or WPA2) security. This provides better protection for your wireless network. More complex wireless networks offer very sophisticated wireless protection schemes that are much more complex than WPA. These do require that the same protocols be loaded onto the laptop computers that connect to them.

4. Be specific around who has wireless access.

Each computer has a network card with a unique address, called a MAC address. Wireless routers can be programmed to only accept connections from computers with specific MAC addresses. While this requires some management as computers are replaced, this system will allow only those laptops that you designate to access the wireless network.

5. Turn off wireless SSID broadcasting.

Each wireless network has a name, called an SSID. When you scan for available networks, the SSID will show up in the list of available networks. Wireless users can then use that information to connect to the wireless network. If the SSID or wireless name is not broadcast, then the user would have to know the exact name of the wireless network in order to connect to it.

6. Connect via VPN.

If wireless access must be used, connect to the wireless and then use a secure VPN to connect to the office. The VPN tunnel will secure the traffic going to and from your firm, limiting the potential for compromising your data.

While wireless is great for a lot of applications, such as email, Internet and remote access, caution should be used when using simple database programs which can be more susceptible to the drops in communications that can occur from time to time when using communications.

Wireless access can be secure if configured correctly. Notwithstanding, it is not yet something that would completely replace a wired network in terms of the ability to secure the network and provide high speed access to applications.

Charles Bennett is the Principal Consultant of Triella, a technology consulting company specializing in providing technology audits, planning advice, project management and other CIO related services to small and medium sized firms. Triella is a BlackBerry Alliance Partner. Charles can be reached at cbennett@triella.com or 647.426.1004. For additional articles, go to <http://www.triella.com/publications.html>.

© 2008, by Triella Corp. All rights reserved. Reproduction with credit is permitted.