

How to secure wireless networks

How to lock down a wireless network

The following steps will only take a few minutes each, but will make a big difference. The results will fend off all but the most determined and skillful crackers.

Change the default password

Almost all wireless devices can be managed via a web interface that can be accessed by simply typing its IP address in a browser's address field. While the admin interface is password protected, the default password set by the manufacturer is always the same. Any wireless network sniffer program will easily discover the manufacturer of the wireless device because it willingly broadcasts that information. Anybody can download the manual from the manufacturer's website, and get the default password to that manufacturer's devices in seconds. As a result, an intruder can type in the default IP address of the wireless gateway to get to the admin interface, and try the default password to log in and access the device settings. Knowing the manufacturer of the device gives the intruder the additional benefit of being able to employ cracks or exploit vulnerabilities specific to that manufacturer.

Disable SSID Broadcast

The SSID is the name of the wireless network. In order to connect to a wireless network, its name needs to be known. By default, wireless gateways happily broadcast the SSID to be picked up by any wireless network device for easy configuration. Hiding the SSID by disabling SSID broadcast will make it much harder for an intruder because he will have to start guessing. It has to be mentioned that while most wireless gateway devices offer the option to disable SSID broadcast, some devices require a firmware upgrade, and some devices do not offer that option at all.

Change the SSID

Disabling SSID broadcast doesn't help much if the SSID remains the manufacturer's default, which is just as easily found in the manual as the default admin password. The SSID should be changed to a custom phrase that is difficult to guess. The use of non-dictionary words as well as numbers and special characters for the new SSID is encouraged.

Enable encryption

Wireless devices support the wireless encryption protocol (WEP) with either 64-bit or 128-bit encryption. 64-bit encryption has been proven to be very weak and easily broken, 128-bit encryption is recommended because it is a lot more difficult to break (though far from impossible). Some devices might require a firmware upgrade to support 128-bit encryption. Encryption works by entering the encryption key on the wireless gateway as well as on the PC with the wireless card. All transmitted data is encrypted for the transfer between the two devices. If the encryption key does not match, the wireless gateway will not communicate. Enabling encryption will usually discourage the casual lazy cracker and send him off to find an easier target.

Disable DHCP

Most gateway devices by default have DHCP enabled. This means that any new host on a network that makes its presence known and broadcasts a request for an IP address and TCP/IP configuration information will be automatically provided this information without questioning. This is very convenient for the legitimate user because it means real plug-and-play (minus the "plug" part since it's wireless). However, it also makes it very easy for the intruder to connect to a wireless network. By simply setting his laptop to use DHCP it will immediately receive all TCP/IP configuration information he needs to connect to the network.

While it is an inconvenience and requires more maintenance from the legitimate user, disabling DHCP and manually assigning static IP addresses creates another hurdle for the intruder. It requires him to manually configure his laptop with what he thinks are the

correct TCP/IP properties to be able to connect to the network.

Change the default subnet

Disabling DHCP doesn't help much if the subnet remains the manufacturer's default, which is just easily found in the manual as the default admin password or SSID. Most devices use the common default subnet of 192.168.0.0 with a subnet mask of 255.255.255.0. The subnet should be changed to another private subnet. There are a number of non-routable IP address ranges that are reserved exclusively for use on private networks. These ranges are 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255 - plenty to choose from. This will prevent the intruder from assigning himself a static IP address and TCP/IP configuration information based on the manufacturer's default subnet.

Use MAC address filtering

Each network adapter has a unique hardware address also called MAC address. The first half of the MAC address identifies the manufacturer of the network adapter, the second half identifies the network adapter. This hardware address is unique (more or less) for each network card. Most wireless gateway devices support MAC address filtering. The way this works is that the legitimate user creates a list and enters only the MAC addresses for network cards that he is aware of and that he wants to be able to access the wireless network. Any network adapter with a MAC address that doesn't match a MAC address in the approved list will be automatically denied access. Only machines with an authorized MAC address are allowed to participate in the network. MAC addresses can be spoofed by a savvy intruder, but using MAC filtering is another good deterrent.

Practice safe computing

Even though the network is private and hidden behind a gateway device with a firewall, common sense precautions still need to be used, including but not limited to:

- Use safe passwords for all user accounts. Use non-dictionary words, include numbers, special characters, upper and lower case letters. Use passwords longer than 8 characters. Change passwords every month.
- Password-protect any network shares
- Require a user login for all computers, disable the guest account
- Install Antivirus software on all computers and keep it current
- Install software firewalls on all computers
- Monitor log files such as event logs, firewall logs, antivirus logs, etc. for unusual activity

Conclusion

As documented in this article, there are many very valid reasons why all wireless networks should be secured. It is extremely easy to do so with not much effort and little time. Armed with this knowledge, it would be foolish not to take the necessary precautions and secure that wireless network. A few minutes of reading the manual and a few minutes of changing settings could prevent a boatload of trouble in the future