Wi-Fi Router Protection
Secure your wireless network

By John Allen

Home WiFi networks need to be secure. Insecure networks can easily be hacked into and used for the following illegal purposes:

- Accessing the internet using your internet connection
- Eavesdropping your internet activity, stealing passwords and other private information
- Hijacking your router and changing its settings remotely so that your internet access is redirected to a different server

All the above can occur whether your computer is on or off. Antivirus software and software firewalls cannot prevent it.

This now becomes even more important because there is a new class of virus we will begin seeing soon - Wi-Fi-borne viruses – viruses that can travel over Wi-Fi networks. These target Wi-Fi routers that have not had their default admin passwords changed. Once hackers get into the device, they're able to install new firmware and bring it under their control, thus redirecting where you go on the internet and stealing passwords and otherwise monitoring your internet traffic.

It is very simple via Google for anyone to find out the default admin password for any brand of Wi-Fi Router. Default admin passwords are generally something like "admin" or "Password".

This type of virus is not detected by computer antivirus product. In fact it can infect a router even if the computer is turned off.

To be secure, modem/routers require three strong passwords, and a strong wireless encryption method. You can also stop your router broadcasting your network availability, and turn on its "hardware" firewall.

"Admin" or "System" password

All wireless routers require a password to access settings on the router via your web browser. Some also require a user name. Most modems come with a default user/password, such as admin/admin, some do not have an admin password set at all. Hackers are aware of the default passwords for all the various models, and are able to remotely access your router and hijack it with this information without you knowing it. You should login to your router and change the admin password from the default to a strong password of your choice.

How to change your Wi-Fi Router's default Admin password

You may already have set a new admin password when you initially set the router up.

Make sure that you are changing the Router Admin password – don't change the Internet Account password, or you won't be able to access the internet.

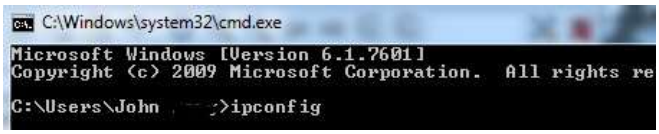
The method varies depending on the brand of router, but the general procedure is:

- Open your web browser
- In the address bar of your browser, type in http:// then the LAN IP Address of your router (for example for my D-Link router it is http://192.168.1.1) – this address will be in your router manual. If you can't find it in the manual, see below how to find it using system commands
- You will then be connected to a user interface of your router

- Then you need to find where to change the Admin or Administrator password – again, your manual should explain this (for my D-Link Router, I go to *Maintenance > Access Controls*)

Make sure that you write down the new Admin login details!

How to find your Wi-Fi Router's LAN IP Address using system commands
(if you can't find it in your router manual)

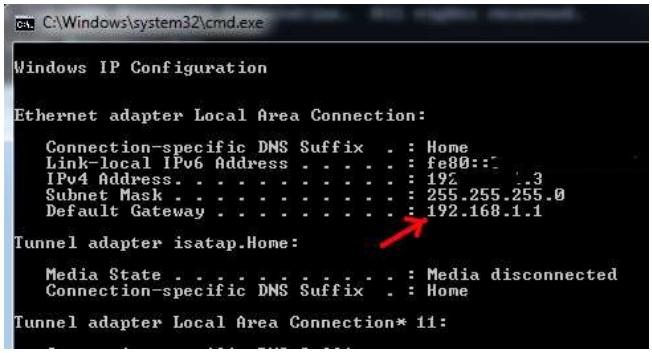


Windows 7/Vista

Click Start, type "cmd" (no quotes), click on *cmd.exe*

Windows 8

Right click in lower left have corner, left click *Command Prompt*



Then for all systems

- Type "ipconfig" (no quotes)
- Under Ethernet adaptor Local Area Connection, you will see Default Gateway – this is the LAN IP address of your router.

Internet password

This is the password associated with your internet user account name, usually associated with your email address. For example, if you are with Bigpond, this is your Bigpond internet account password. This password is set up in the modem/router when you first install it, and may be pre-set by your internet provider.

Wireless Encryption Key (password)

This is the password that you need to enter to connect to the modem/router via WiFi. If you do not need a key to access the WiFi then the network has no encryption and is highly vulnerable to eavesdropping.

Wireless encryption method

You should also check that you have the strongest possible encryption method selected – WPA2 is preferable, WPA is the older and less secure method. You need to check that your computer can also handle the stronger method. If you change the encryption method you may have to remove your old connection from your computer and reconnect.

SSID Broadcast

The SSID (Service Set Identification) is the name of your WiFi network. It is continually broadcast by your router. Anyone with a computer or other WiFi device within receiving distance is aware that you have a WiFi network. You can turn this SSID broadcast off for added security, but this means that anyone connecting to your WiFi for the first time would need to know your SSID as well as your encryption key.

"Hardware" firewall

Routers have a "hardware" firewall facility. This should be turned on as it provides an extra level of protection of your router computer. This is different to the software firewall you would have on your computer. Both firewalls can be safely active and do not interfere with one another. On most routers this firewall is enabled by default

See also the following websites:
http://www.police.qld.gov.au/programs/cscp/eCrime/wireless.htm
http://www.smh.com.au/it-pro/security-it/the-flyby-wifi-hacking-machine-20130524-2k5xg.html