



Securing Your Wireless Network

- Basically 12 steps to securing your wireless network
- Let's get started!
- Document everything you do! (that way you can undo or re-do each step if needed)!!!



Step One

- Read through this procedure and collect all required documentation (manuals, etc.), and specifics for each device that is to connect to your wireless network
- This includes: Device Name, location, IP address, MAC address, for Router, DNS server IP addresses
- *Network Inventory List — (image1)*
- *Check your Router — (image2/3)*



Step Two

- Change the login and password for your wireless router
- *Even Microsoft knows about your router (image4)*



Step Three

- Change the SSID of your network to something other than the default and cannot be identified to you, like your last name or address.
- Use something like "h0me", or "My_Dog"
- Remember to record your changes!



Step Four

- Turn off broadcasting the SSID of your Network so it is NOT visible.
- Why not make it more difficult for others to access your network?
- Record your changes!



Step Five

- Turn on or activate **Wireless Encryption**
- **WEP** minimum but really need to use **WPA** or **WPA2**
- A **firmware upgrade** might be required or **replace your router** and/or **wireless adapters**
- **Record all changes, passkeys, etc.**



Step Six

- ♦ Eliminate unwanted network guests by enabling MAC Address filtering
- ♦ Only devices with filtered MAC addresses will be allowed to connect
- ♦ *Verizon Router example (image5)*



Step Seven

- Use command “ipconfig /all” and record the MAC address and IP address of each device that connects to your network wirelessly
- Be sure to record the MAC address and identify each computer whose MAC address you record



Step Eight

- ♦ Assign fixed IP addresses to all your wireless devices (you may use the current IP address but make it permanent)
- ♦ Turn off DHCP
- ♦ Assigning a “fixed” IP address is dependent on your version of Windows, use help for assistance



Step Nine

- Install and activate firewall software on each pc and the router
- Choose any firewall software you want; I use the free firewall from PCTools
<http://www.pctools.com/>



Step Ten

- Remember, wireless broadcasts everywhere - like tv or radio stations
- Centralize physical placement of router in your house to minimize signal leakage outside your house



Step Eleven

Your password is the first line of defense for your computer and network
- select a good one



Step Twelve

Visit www.grc.com/ and use the “shields up” utility to access if outsiders can see (and attack) your computer/network

Router view of my network (image 6)



That's All Folks!...

Thank you!