Wireless Internet Basics

Setting Up a Wi-Fi Network

1. Find the best location for the wireless router.
   - Place the router in a central location, free from obstructions which could cause wireless interference.
2. Turn off the modem.
   - Power off the cable or DSL modem from your Internet service provider before connecting your equipment.
3. Connect the router to the modem.
   - Plug an Ethernet cable into the router's WAN port and then the other end to the modem.
4. Connect your laptop or computer to the router.
   - Plug one end of another Ethernet cable into the router's LAN port and the other end into your computer's Ethernet port.
5. Power up the modem, then router and then computer.
   - Be sure to turn them on in this order.
6. Go to the management webpage for the router.
   - Open a browser and type in the IP address of the router's administration page; this information can be found on a label on the router or in the manual.
7. Change the default administrator password (and username if necessary) for the router.
   - This setting is typically found in a tab or section called administration.
8. Add WPA2 security.
   - This setting is located in the wireless security section, select which type of encryption to use and then enter a passphrase of at least 8 characters.
9. Change the wireless network name (SSID).
   - Specify a name for the SSID (Service Set Identifier) in the wireless network information section.
10. Setup the wireless adapter on the computer.
    - After saving the configuration settings on the router, unplug the cable connecting the computer to the router. The computer may automatically install the drivers or the setup CD which came with the adapter can be used to install it.
11. Connect to the new wireless network.
    - On the computer and other wireless-enabled devices, find the new network you set up and connect to it.

Wireless Internet Basics

Wireless Internet Safety

<u>Home Network Security</u>
A home wireless network allows you to use your computer or devices anywhere in your home and be able to connect to other computers on the network or connect to the Internet. It is extremely important for home wireless networks to be secure. Utilize these tips to protect home wireless networks:
- Do not use default passwords.
- Turn off SSID broadcasting to prevent your wireless device from announcing its availability.
- Change the device's SSID name.
- Encrypt your data.
- Install an anti-malware product on all computers and devices.

<u>Public Network Security</u>
Many public locations offer free access to public wi-fi. Cybercriminals often spy on these networks and intercept data transferred on the connection. Utilize these tips to protect yourself on public wireless networks:
- Be aware of what information you are sharing on the network.
- Treat all wi-fi links with suspicion and do not assume a network is legitimate.
- Try to verify a wi-fi connection is legitimate before connecting to it.
- Use a VPN (virtual private network) when connecting to a public wi-fi network.
- Avoid using websites which require entering certain types of information such as banking information, credit card information, passwords, etc.
- Protect your device against cyberattachks