Wireless

This information is presented as general purpose suggestions and the effects may differ on each device or based upon specific updates done to each device. The County of York assumes no liability to unintended results this may have on your specific device and will not assist in any issues that may arise from implementing these tips. This is not an all-inclusive list of all software options available, simply a partial list of some options for the reader to further research for what might work best for them.

Using wireless communication, you will be at a higher risk than if you were physically connected. If you are physically connected, it is almost like having a private conversation with the other person. While you are connected wirelessly, you are essentially having that conversation and everyone else connected to that wireless signal is in the room with you and can potentially eavesdrop on the conversation. Luckily most of these instances are crimes of opportunity and by following the recommendations below you can greatly reduce your risk or at least understand the risks you are taking.

Wireless Safety at Home

In most homes their "Wireless Access Point" (WAP) is integrated into their router (a box that connects directly to the wall or into your modem that is connected to your wall). It will be the device usually with one or several antennae sticking out of it. On the router or WAP there will usually be a sticker with default login information.

Configuring your wireless access point

1. **Connect to your device -** Each device's menu is a little different and I strongly recommend visiting the manufacturer's website for the user's manual. Once you get to the settings they are pretty common, which is what I will discuss here. From a device connected to the access point open a browser and go to http://192.168.0.1 (if that doesn't open try http://192.168.1.1, if that doesn't work see your specific device's user's manual).
2. **Update your device –** There should be a section in the menu to update the device or the firmware. Usually you just click a button to update it. This should be done at least once a year. This device is considered an IT security device and most companies will regularly publish critical security updates. Without these updates hackers have been known to find easy ways into your network from the other side of the world without you having any idea.
3. **Update the device password –** While most devices will not allow, by default, remote login from the internet, it is still a very good idea to change the password to access this device. This should be different than the password you use for your wireless access. If you decide to allow someone access to your home network you don't necessarily want them to have access to this security device.
4. **Wireless Settings –** There is usually one section in the device that will focus purely on the wireless settings.

a. **SSID -** It will ask for a “SSID”, this will be the name of your wireless network. You want to change this from the default to something unique, failure to do so will put any devices that “trust” your network at risk of anyone else using this default name.

b. **Broadcast** – You will also be asked if you want to broadcast your SSID. It is recommended not to broadcast so that people looking for wireless network will not easily see yours. However this will also mean that when you setup a device (cell phone, etc.) you will need to correctly type in the SSID and password (otherwise you can select your SSID and just need to type in your password).

c. **WPA2** – It will also ask what type of encryption. Choose WPA2-PSK (WPA2 Pre-Shared Key). It should be noted that as of Oct 2017 there is a major security vulnerability with WPA2 but the details are outside the scope of this and the bottom line is this is still the most secure encryption option available to a normal end-user.

d. **Set WPA2 password** – This should be a complex unique password that will be needed to allow devices to connect to your network. Please see related document for tips on making a secure password.

5. **Access to your network** – Be extremely cautious when you give out your WPA2 password. While many people feel pressured when someone is visiting and they are asked by the guest for internet access to give it out please be very cautious. While this person may be very trustworthy you should think, if this person has a virus on their phone or device you will be letting them circumvent all of your network security (your router which is your first line of defense). Children’s tablets and phones tend to be very susceptible. Some modern routers also have an option for a “Guest Wi-Fi” specifically designed to allow guests access to only the Internet. See your specific router’s documentation to if this is available for your hardware.
6. **Be cautious taking advice from the Internet** – Many articles (especially with gaming) will have you go into your router and make custom tweaks to improve performance or allow networking directly between you and someone else. Be very cautious taking these at face value. Some are directly misleading and will purposefully make your network extremely vulnerable and others, while they will make the game work, were created by someone who didn’t understand the impact of doing a port forward to a machine. In most cases doing a “port forward” is bypassing your network router security and exposing your PC (or device) directly to the entire Internet (a very bad idea).

Wireless Safety on other Networks

When you connect to wireless networks your device can be attacked from several sources that you usually don’t have to worry about. Open Wi-Fi is extremely popular due to its convenience and the tips below will reduce your risk but understand that overall you are still greatly increasing your risk by using it.

1. **Avoid Unknown SSIDs** – If you connect to a SSID (wireless network) that is configured by a hacker you are giving them access to essentially all of your communications. This is a very bad idea. If you see an open Wi-Fi with no password, while it may be tempting to jump on and use it, if it has been compromised you are sure to regret it.

2. **Avoid sensitive browsing** – Many restaurants, hotels, and service centers offer free open Wi-Fi. The biggest danger is other users connected to it eavesdropping on your conversation. While banking websites are further encrypted, with some time and effort a hacker can decrypt the transmission or perform a man-in-the-middle attack. Bottom line is if you need to login to a website, turn off Wi-Fi and use your cellular minutes. When done and you log out of the website then you can reconnect to the free Wi-Fi for your normal surfing.
3. **Turn off sharing** – You might purposefully share documents between your devices while on your home network. If you do you need to make sure they are unshared when you leave your home, otherwise these are open invitations for a hacker to also gain access. On a Windows system make sure you choose “Public” network when you connect to a network you don’t control.
4. **VPNs** – The short answer is do not use an Internet based VPN. Many people online recommend using a VPNs or Virtual Private Networks to eliminate the risk of using an unsafe network. At face value this is 100% correct and is what many corporations and governments use to protect communication. A VPN creates a highly encrypted tunnel between your device and some other device on the Internet. For a business this is usually their router (a little simplistic but valid for this example) at their main office. They control this device and the non-VPN traffic then leaves their trusted main office network. However for the normal end-user the problem is where to connect the VPN to. Most online articles say put in value X which is their router. The problem with this is all of your traffic is being sent to that company which can see it unencrypted. You’ve taken the risk of a hacker connected to the local Wi-Fi spot while you’re connected and now sent it to a random place out on the Internet that is gladly inviting you to send them all of your traffic. To me this is jumping out of the hot water and into the blazing bonfire.