BC Society of Transition Houses

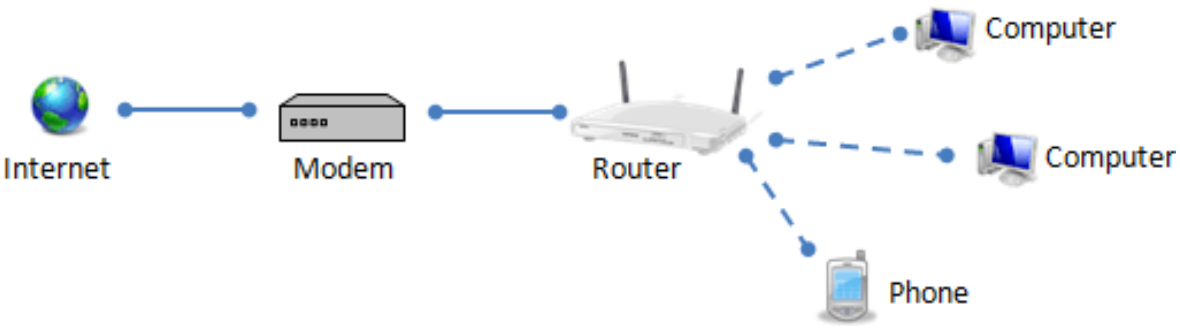
Securing Your Home Wi-Fi Network

One of the first things people ask when they visit your home is: "What's the Wi-Fi password?" Home Wi-Fi is no longer a luxury but almost a necessity for many households. So many home devices: computer, laptop, smartphones, tablets, smart TV, printer, home cameras, and for some households, even lightbulbs and refrigerator connect to the internet! The hub of all this connection is the router – the thing that connects all your Wi-Fi-enabled devices to each other on a home network and to the internet. To ensure that your devices are secure and safe from hackers, it's important that your home router is secure. That's how you'll increase the security of your home Wi-Fi network and all the devices connected to the router.

Note: You do not have to use Wi-Fi to access the internet. You can still use an Ethernet cable if your device is not Wi-Fi enabled only.

WHAT IS A ROUTER?

A router is the access point for your Wi-Fi-enabled devices. Whether you have DSL, ADSL, cable, or old-fashioned dialup, (and some versions of NBN), in order for you to connect to the internet, you need a modem and a router. (Sometimes, the modem and router are combined into one device.) The modem is generally provided by your Internet provider and it's what allows you to connect to the Internet. The router (which can be a separate device or built into the modem) is what connects your Wi-Fi-enabled devices to the modem, and thereby the Internet.



All the devices that are connected to your router forms a network. This is what allows your devices to "talk" to each other – for example, if you have a Wi-Fi printer, you can print wirelessly if the device you're printing from and your printer are all on the same network.

BC Society of Transition Houses

WHAT IS THE SECURITY RISK?

Because all your devices are connected to the router, if someone were to gain access to your router, that person may be able to monitor the internet traffic from your devices, limit your devices' access to the router (and the Internet), or perhaps even gain access to your devices. If your router is very insecure, someone with the right skills can even hack your router, take it over, or set it up so that when you connect to the internet, you're connecting to fake websites – where whoever built the fake website can steal your information when you enter personal data (such as username, passwords, credit card information, etc.) into those fake websites.

WHAT CAN I DO?

- ***Put a passcode on your Wi-Fi network***
  The first thing you should do is put a password on your Wi-Fi network. When you set up your Wi-Fi network, you're asked to create a name for your network (SSID) and offered the opportunity to create a password for the network. If someone wanted to join your Wi-Fi network, they would need to know the password to join.

  In addition to password protecting the network, choose a network name that isn't personally identifiable, such as "Ae374-jid" versus something that is identifiable, such as "John&KatesWiFi." The purpose is to unknown devices to connect to your home network.

- ***Change the log-in credentials to your router***
  In most cases, to log into your router, you were given a website URL that contains a series of numbers and dots. To sign into your router, you connect your computer to the router, enter the URL address into a web browser, and sign in with a username and password. We recommend changing the default sign-in to something that's unique to you. This way, other people can't log into your router simply because they know the default log-in credentials. (Granted, for someone to do that, they would either have to be physically connected to your router or they would have to know specific information about your router to access it remotely. Still, it's best practice to change the default credentials.)

- ***Create a guest Wi-Fi network***
  If you want your guests to be able to use your Wi-Fi, consider creating a secondary Wi-Fi network just for them. The guest network will have a separate network name (SSID) and password. This will prevent your guests' devices from being able to access or "speak to" your Wi-Fi connected devices. For example, if they are on a different network, they will be unable to wirelessly connect and print to your Wi-Fi printer, since the printer is on a different network.

Limiting devices (that's not yours) from connecting your home network will increase your security.

- ***Select strong encryption***
  Your router is the gatekeeper between you and the Internet. When you set up your router, select WPA2 as your encryption. This is the strongest encryption available to protect your internet traffic. With WPA2 encryption turned on, each time you visit the internet your visit is encrypted making it more difficult for hackers or eavesdropper from seeing the data (username, password, credit card information, or other sensitive data) you're sending over the internet.

- ***Turn off remote management***
  Some routers allow you the ability to access it remotely. Turn this off, especially if you don't think you will need to manage your router remotely and are worried that someone might exploit this ability to access your router. Find this feature under the router settings and turn off the setting that allows remote access or management.

- ***Download firmware patches***
  As new security threats are discovered, companies will develop patches or updates to devices to protect it from those security threats. Check your manufacturer's website to see if there are firmware updates for your router. If you have an older router, be sure to update the router firmware before you set it up or buy a newer one that will have the latest encryption tools and protections.

  Don't forget that security patches are not just for your router. Your Wi-Fi-enabled devices also need to be updated. When your phone or computer suggests that you update the operating system, it's sometimes because the update includes security patches. If you have an older device that is no longer getting updates from the manufacturers (and is no longer being protected from the latest security threats), consider buying a newer device.

- ***Limit devices from connecting to your network with Mac address filtering***
  If you really don't want any other device to connect to your network, you could set up Mac address filtering on the router. Every device that has the ability to connect to the internet has a unique Mac address, which is a series of letters and numbers. You can set up your router to only allow certain Mac addresses to connect. This does mean that you will have to find the Mac addresses of all your internet-enabled devices and enter those into your router. This also means that when you have guests visiting (or purchase a new device that needs to be connected to the internet), you'd have to manually add the Mac addresses of those devices to your router.

- ***Practice good security habits***
  Your device security, internet security, and personal information security is more than just making sure your router is secure. Router security is one piece of this complex system. There are other things that you can do to protect your information and increase your security.

  - Make sure you practice good internet privacy and security habits, such as not visiting virus- infected websites or falling victim to phishing schemes and scams. Check out our online safety and privacy guides.
  - Ensure that your devices are secure by reviewing settings and running security software. Check out our handout on computer and laptop security and privacy. Even your smartphones have settings that can increase the security and privacy. Check out our iPhone and Android guide.
  - If you're using public Wi-Fi, there are additional steps you can take to increase privacy and security. Check out our guide on using public Wi-Fi.

Adapted from and in cooperation with the WESNET Safety Net Australia project at the Women's Services Network, Australia