Public Wi-Fi convenient, but risky

November 10 2011, By Salvador Rodriguez

It seems you can surf the Internet and check your email from virtually anywhere these days - in coffee shops, hotel lobbies, airport terminals and airplane cabins.

More places are making it easier to turn on your laptop or tablet computer and connect to the Internet through free public Wi-Fi hot spots .

But much like leaving your diary on a park bench, connecting to the Internet using a public Wi-Fi allows anyone with the right software to see what you are doing.

Worse, you risk being hit with malware and other virulent programs that can turn your computer into botnets controlled by hackers to attack websites.

Here are some tips to protect your computer from digital eavesdroppers and malicious hackers:

Before leaving home:

-Enable SSL connections: One of the most effective ways you can to protect your Web surfing is to use secure connections. As you probably have noticed whenever you log into your bank's website, your browser displays a lock icon or adjusts the URL bar. This is your browser indicating that you are visiting the website over a Secure Sockets Layer, or SSL, connection. An SSL connection encrypts the information

exchanged between you and your bank, keeping others out.

SSL connections are usually enabled for bank websites and other sites that hold sensitive information, but they can be costly for large companies, which is why many don't have them turned on automatically. But you can enable an SSL connection easily on many of your most used sites:

-Gmail: Most people have a Gmail account nowadays for their email, and it's always important to make sure your emails are safe. To enable an SSL connection for your Gmail account, click on the gear icon at the top right of the page, click Mail Settings, select Always Use HTTPS, and save.

-Twitter: Go to your settings, scroll to the bottom of the Account tab, check the box for Always Use HTTPS and save.

-Facebook: Some people stay logged on to Facebook throughout the day, so making sure your connection is secure can go a long way. To switch on the SSL connection, go to Account Settings and click the Security tab. Once there, edit Secure Browsing and check the box that offers browsing on a secure connection. Unfortunately for heavy Facebook app users, you will have to disable this when you run programs such as "FarmVille."

-Disable sharing: People often enable sharing to connect with printers and other devices wirelessly. As useful as this can be at home, leaving sharing on in public areas is like leaving your door unlocked in a bad neighborhood. Here's how to turn it off:

For Macs, launch your system preferences and click on the Sharing icon. Uncheck all of the boxes to disable sharing. To turn them back on, simply check whatever you're going to use.

For PCs, Windows will ask you if you are connecting to a home, work or public network when you connect to a new WiFi network. If you select public, Windows will disable sharing for you. If you'd like to do this yourself on Windows XP and 7, click the Start button and launch the Control Panel.

Here is where the method changes depending on your version of Windows. For Windows XP, click on Network Connections and right-click Local Area Connection. Click Properties and from there uncheck the box that offers file and printer sharing and then click OK. Check it to enable file and printer sharing again. For Windows 7, click Network and Sharing Center, and select Change Advanced Sharing Settings on the left. Click on the arrow of the network you'd like to disable sharing on, select Turn Off File and Printer Sharing, and save.

-Turn off Wi-Fi: One more precaution you can take is to turn off your Wi-Fi before heading out to avoid having your computer latch on to an unsafe network on its own.

For Macs, click the WiFi icon on the top right corner called Airport. Select Turn Airport Off.

For PCs, right-click the wireless icon on the task bar and turn it off.

Once you're there:

-Turn on WiFi: Follow the same steps to turn your WiFi on when you arrive at your destination and select the desired network.

-Log in using a VPN: If you can log into a virtual private network, your online experience will be that much safer. Most companies give employees with network access at the office a way to log into the company VPN from outside. Enabling the company VPN will encrypt

your browsing and work as a shield.

If you don't work for a company or have access to the company VPN, you can buy a VPN account with a third party.

This will give you that same protection and encrypt your activity. Prices range from $8 to $10 a month.

Once you leave:

-Turn off Wi-Fi: Should you go to another public spot, this will prevent the computer from automatically connecting to an unsecured network.