Security when working with Wi-Fi Hotspot

In this article we will share some tips to help protect your email, documents and computers safely using Wi-Fi hotspots.

Network administration **- Unlike regular Wi-Fi networks, public hotspots are not secure with wireless encryption. So in this article we will share some tips to help protect your email, documents and computers safely using Wi-Fi hotspots.**

As you probably know, there are some security issues during the use of public Wi-Fi networks, such as hotspots at cafes, restaurants, hotels and other public places.
Wi-Fi is clearly not developed for public access. Rather, hotspot providers such as T-Mobile, do not use wireless encryption (WPA / WPA2) on hotspots. This Wi-Fi encryption is impractical for hotspots when its original purpose is to be used only as private networks in the home or business. Add to that the sharing aspect on public Wi-Fi networks; You definitely won't want to share files with strangers.

In this article, we will show you how to protect your computer and communication while using Wi-Fi hotspots. Although wireless networking technology is not designed for public use, it is still safe if the hotspot provider and user comply with the following precautions:

Make browsing and email safe

Just like when surfing the web at home or work, you should follow basic Internet security measures when using hotspots. This is because many of the Internet protocols and services that we use on a daily basis are inherently insecure.

Logging and communication for services such as HTTP, POP3 / SMTP email, IMAP email, Telnet command line access, FTP file transfer are not only encrypted but also sent and received as documents "pure" version.

At home and at work, the communication of these text services can be encrypted and protected to prevent internal Wi-Fi eavesdroppers by using WPA or WPA2 encryption.

However, most hotspots do not use this encryption. Therefore you should follow the actions introduced in the sections below.

Use HTTPS / SSL for sensitive users and login

Make sure that the Web sites you log in with use Secure Socket Layer (SSL) encryption. URL starts with *https* instead of *http* . In addition, the browser needs to display a lock icon, blue address bar, or other notification (security measure).

Secure POP3 / SMTP / IMAP Email connections with SSL

If you use email clients, such as Outlook or Thunderbird with POP3, IMAP, or SMTP protocols, it should be used with SSL encryption.

After all, you still depend on your email server and service. If this type of encryption is supported, you can set up on the email client. If the server does not support, see if you can access your mail via the web (using HTTPS / SSL), at least when using public networks.

Use SSH instead of Telnet

If you have to remotely connect to a computer or a server when you are in a public network, use a secure remote access protocol like SSH.

Use SFTP / SCP instead of FTP

Although it may be easier to use FTP for downloading and uploading files to the server, the cost of the ease is insecure. Similar to other plain text protocols, Wi-Fi eavesdroppers can capture the log data as well as the transferred data of FTP connections.

Instead, to be safe, you should use SL encryption with FTP connections, which must be supported by the server and client. You can also look for another solution that is using the SCP protocol.

See page 2

Encrypt communications

Since most hotspots do not use WPA or WPA2 encryption to secure communication between computers and wireless access points (or wireless routers), you should use something to provide encryption. this.
If you use a clear text protocol as described above, local Wi-Fi eavesdroppers can't see the communication. You can use this type of encryption using Virtual Private Network (VPN) technology.

Traditional VPN solutions are designed to provide secure remote access to corporate networks. Because VPN connections are encrypted from the user's client, all connections to the network or server, any traffic when used on the hotspot will be protected from eavesdroppers.

If your employees do not provide VPN access, you can set up your server using the Professional version of Windows.

There are also VPN solutions specifically designed for hotspot security. They do not have the ability to access files remotely, but they can still create a tunnel for Internet traffic through a transmission system, so your hotspot traffic can be safe.

A free solution that you can try is AnchorFree's Hotspot Shield.

Protect computers and shared files

Wireless networks were originally designed with the intention of being used exclusively, within the home or businesses, where users were completely trusted. Although file and printer sharing is one of the obvious benefits of Wi-Fi, it is one of the dangers in public hotspots, where users are not trusted. Some hotspots set up using hotspot gateways block sharing, but many hotspots are implemented using regular Wi-Fi devices. You can ensure your computer and documents are safe by following these precautions:

Sort Hotspot is Public in Vista or Windows 7

When you first connect to wireless networks in Windows Vista and Windows 7, you will see a prompt to classify the network type as Public or Private (Work or Home). Windows then selects the appropriate network and

firewall settings, such as disabling the file sharing and printer sharing feature when connecting to a public network.

If you need to change the network classification, or network type after the initial configuration in the first connection, visit the Network and Sharing Center.

Disable file and printer sharing in Windows XP

If you're still using Windows XP, you'll have to disable this sharing feature yourself. To do that, access the **Network Connections** window by right-clicking on the network status icon in the system tray or **Start> Connect To> Show all connections** .

Then double-click the connection you are using, uncheck the option F **ile and Printer Sharing for Microsoft Networks** and click **OK** . When you return home or go to the office, you can activate the sharing option again to work normally.

Activate Windows Firewall

Connecting to hotspots also means opening your computer to general intrusion attempts from internal hotspots or Internet hackers.

Therefore, you should ensure that you have enabled Windows Firewall or some other firewall program when accessing the public network.

Things to remember

There are many methods that can protect data and privacy when accessing Wi-Fi hotspots. Remember, try to protect your services independently.

Also consider using a VPN service to encrypt Internet communications to avoid eavesdroppers and to make sure that you don't share them with other hotspots.