FCC Consumer Tip Sheet

Wi-Fi Networks and Consumer Privacy

Background

Wi-Fi networks are powerful, valuable tools in our modern communications and information society, enabling users to connect wirelessly to the Internet by extending broadband service in your own home, or by connecting to "hot spots" in public spaces, like airports, coffee shops, and hotels. In using these networks, however, it is important to understand that information being transmitted over them can potentially be intercepted if the networks are not secure. Consumers should be aware of whether they are using a secure (encrypted) or unsecure (unencrypted) network, and should be especially cautious about using unsecured networks – whether those networks are in their homes or in public spaces – to send sensitive information.

How do I secure my personal Wi-Fi network?

Protect your sensitive information:

- *Turn on encryption*: Encrypted information is encoded information that cannot be easily deciphered if intercepted. Today, encrypting information transmitted on your Wi-Fi network is as easy as activating the encryption feature on your wireless router. Check the instructions that came with your router for information on how to do so. If your computer and router will support it, WPA2 is the most effective encryption standard for Wi-Fi.

Prevent others from accessing your network:

- *Activate the router firewall*: Both in the actual and virtual world, a firewall is a barrier intended to confine or restrict a hazard. As with encryption, constructing a firewall on your Wi-Fi network is as simple as activating that feature on your wireless router.

- *Change the router default password*: The password for your router is the key to administering device settings on your router. Many wireless routers come with default passwords that others may know or be able to figure out easily. Change the password to your router to a unique combination of letter, numbers, and symbols that only you know in order to ensure that you will be the only one who holds the keys to your router.

What about public Wi-Fi networks?

Since consumers do not themselves administer public Wi-Fi networks, they have much less control over the security of the information transmitted. *For that reason, consumers are at risk when they transmit sensitive information – such as credit card numbers and passwords – over public Wi-Fi networks*. If you happen to use a public Wi-Fi network, remember the following additional tips.

Only log in or send personal data to fully encrypted sites:

- To determine if a website is encrypted, look for *https* at the beginning of a site's web address (the "s" is for "secure") and a lock icon at the bottom or top of your browser window. Make sure that *https* appears the entire time you're logged in -- some sites use encryption only for the sign-in page, but if any part of your session isn't encrypted, you could be at risk.

Turn on your personal firewall:

- Many computers come with operating systems (e.g., Windows 7) that have a built-in firewall that's turned on by default. You can configure the firewall to provide better protection when you're using a public Wi-Fi network.

Turn off your wireless network when you're not using it:

- If you're in a public Wi-Fi area but not using the Internet, disable your wireless connection by either removing your external Wi-Fi card or clicking on your internal Wi-Fi connection.

Use an encrypted VPN (Virtual Private Network) from your computing device

- VPNs are often used by businesses and organizations to afford a safe and secure mechanism for mobile travelers to communicate. VPN software provides an encrypted pathway allowing an end user to connect to a business or organizational enterprise network.

For More Information

For information about other Wi-Fi issues, visit onguardonline.gov. You can also contact the FCC's Consumer Center at 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY; fax to 1-866-418-0232; or write to:

Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, D.C. 20554