

# How to Be Safe When Using WiFi

Taking precautions to protect your privacy when accessing the Internet through wireless networks or public Wi-Fi hotspots is absolutely necessary. Hackers and identity thieves commonly use unsecured and vulnerable Wi-Fi networks to access...

Method 1 of 5:

## Turning on Firewall

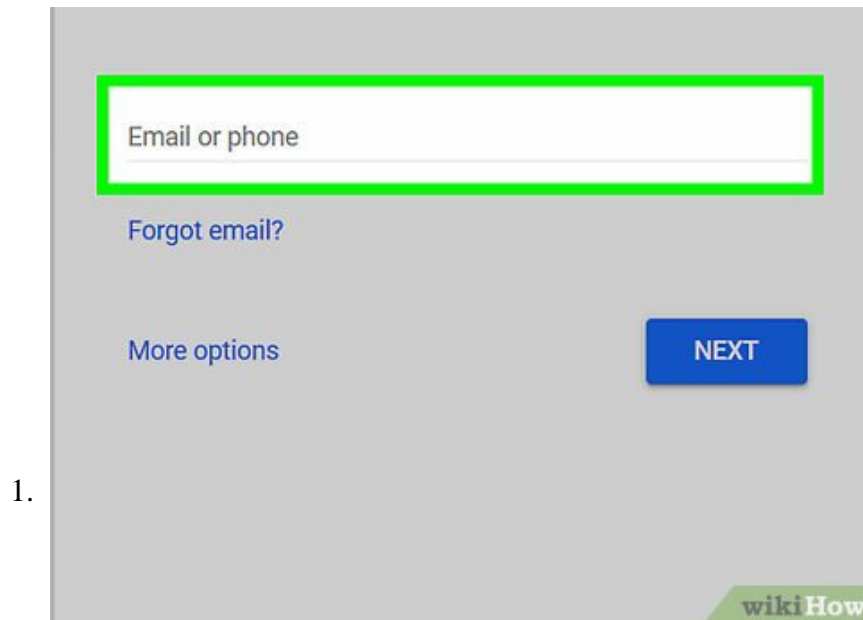


**Enable your firewall.** If your computer is running Windows 7, Windows Vista, or Windows XP, your firewall is turned on by default. To turn on the firewall on Mac OS X, navigate to System Preferences>Security>Firewall and click the 'Start' button.

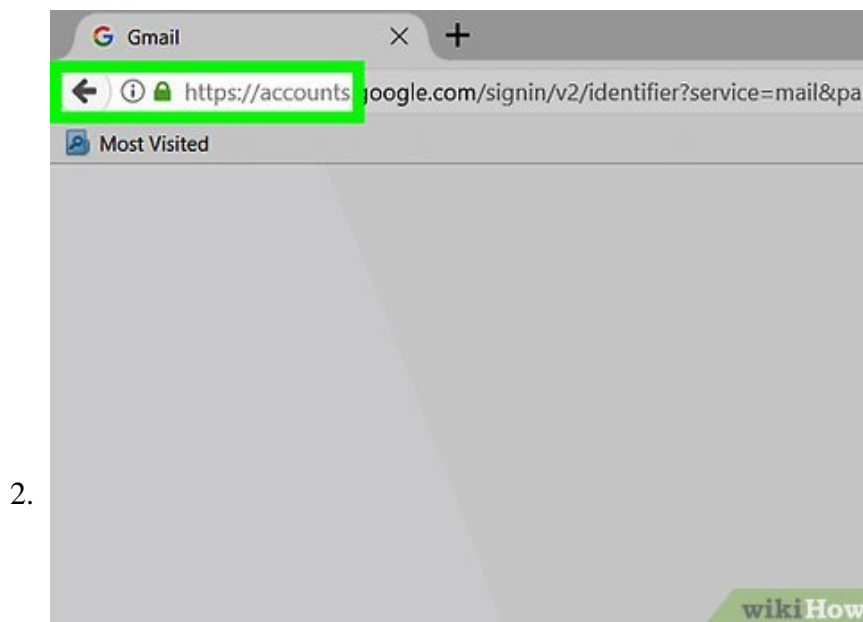
1. To turn the Windows firewall on and off and manage preferences, navigate to Start>Run> type 'Firewall.cpl' and click 'OK' or press Enter.

Method 2 of 5:

## Protect Sensitive Information



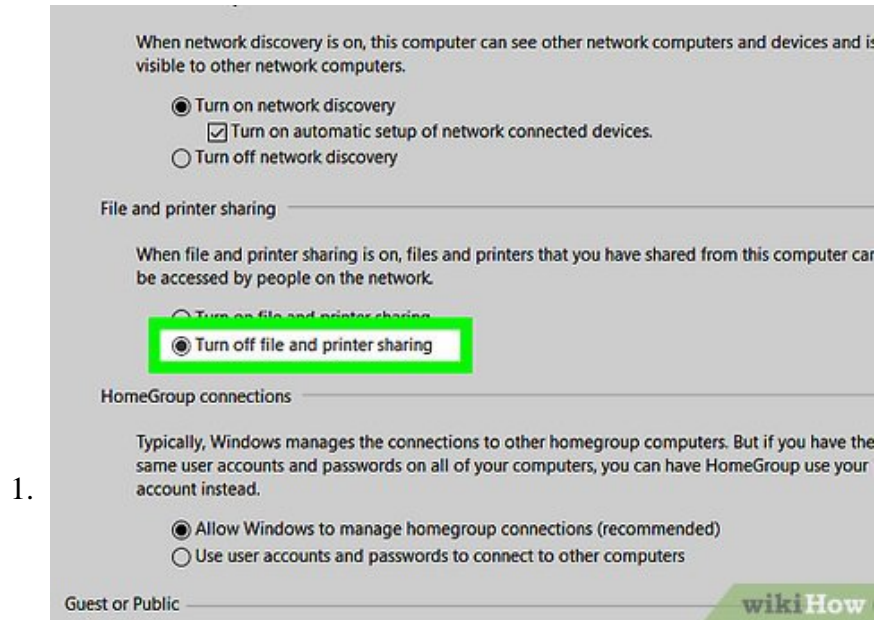
**Avoiding online tasks that require you to enter your sensitive, personal information such as credit card numbers or passwords is best practice when on a Wi-Fi network.**



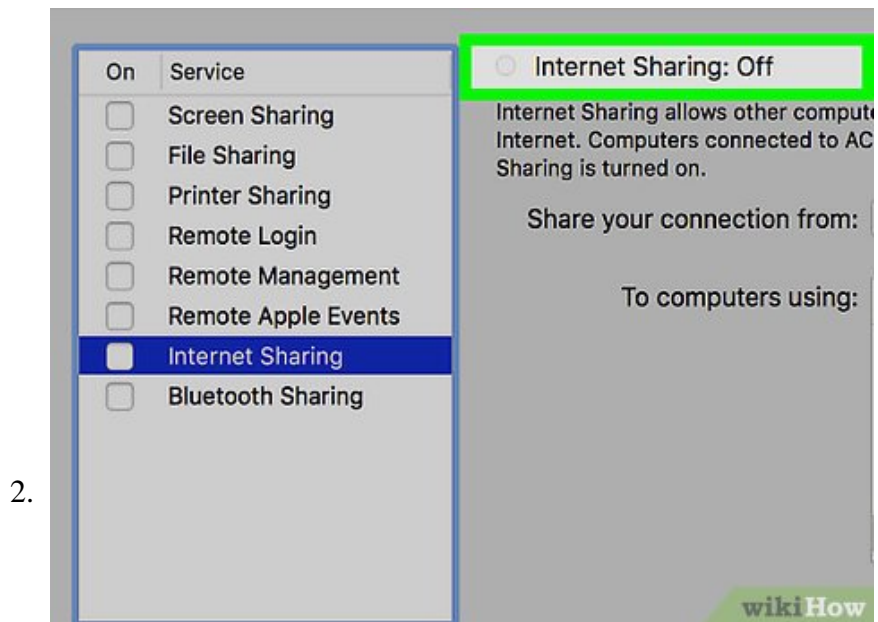
If you must enter this type of data when on a public network, ensure the website asking for the information uses 'https' before their URL in your browser's address bar. The key is the 's' in 'https' lets you know the connection is secure -- even if someone hacks a https:// session, the information they access will be encrypted. **If the 's' is not present, do not enter your private information.**

Method 3 of 5:

## **Disable Sharing**



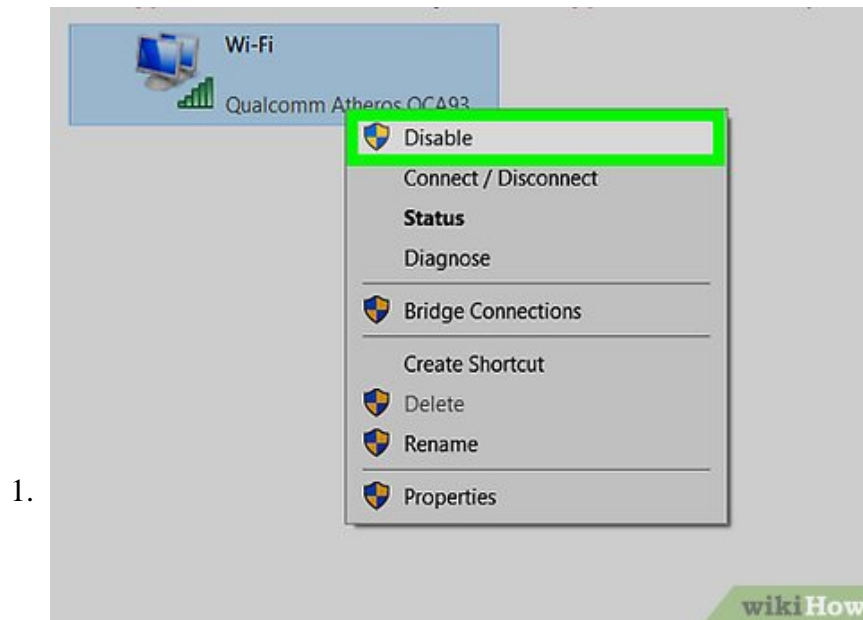
**Turn off sharing settings on Windows.** Navigate to Start >> Control Panel >> Network and Internet >> Network and Sharing Center. Select 'Homegroup and Sharing Options' followed by 'Change Advanced Sharing Settings'. From within the Change Advanced Sharing Settings dialog you can disable printer and file sharing as well as Public folder sharing and network discovery.



**Turn off sharing settings on Mac OS X.** Click the Apple menu in the upper left corner of the screen followed by 'System Preferences' from the context menu. Select sharing from the System Preferences window and uncheck all of the sharing options that are currently enabled to disable them.

Method 4 of 5:

## Turn Off Wi-Fi When Not in Use

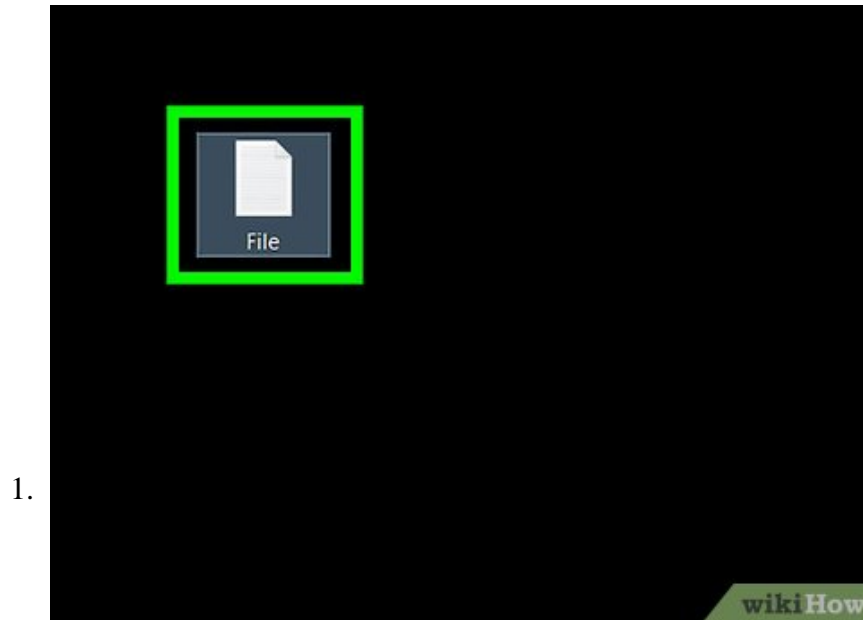


**Most modern PCs and mobile devices will automatically connect to a wireless network when it's in range.** However, if you are not currently using the internet but your device is on, its best to turn off your Wi-Fi adapter.

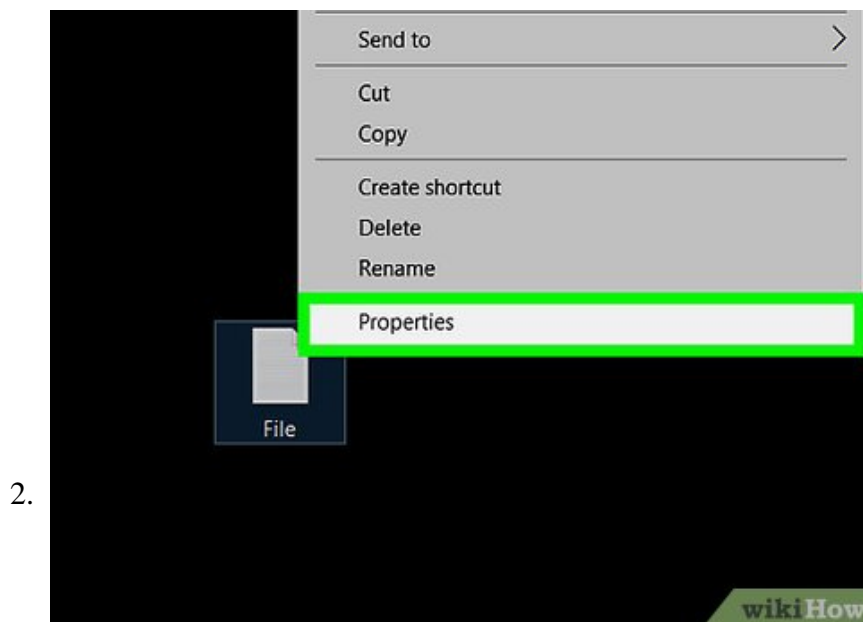
1. If your device has an internal Wi-Fi adapter, you can access Network Connections on Windows by clicking Start, typing 'ncpa.cpl' and pressing Enter on your keyboard. Note: The process of disabling your Wi-Fi card will vary from device to device. Consult your manufacturer documentation to learn more.
2. On Mac OS X, click the Apple menu in the upper left corner followed by 'System Preferences'>'Network'>'Turn Airport Off'.
3. If you have an external Wi-Fi card you can simply remove it from your device.

Method 5 of 5:

## Encrypt Sensitive Files

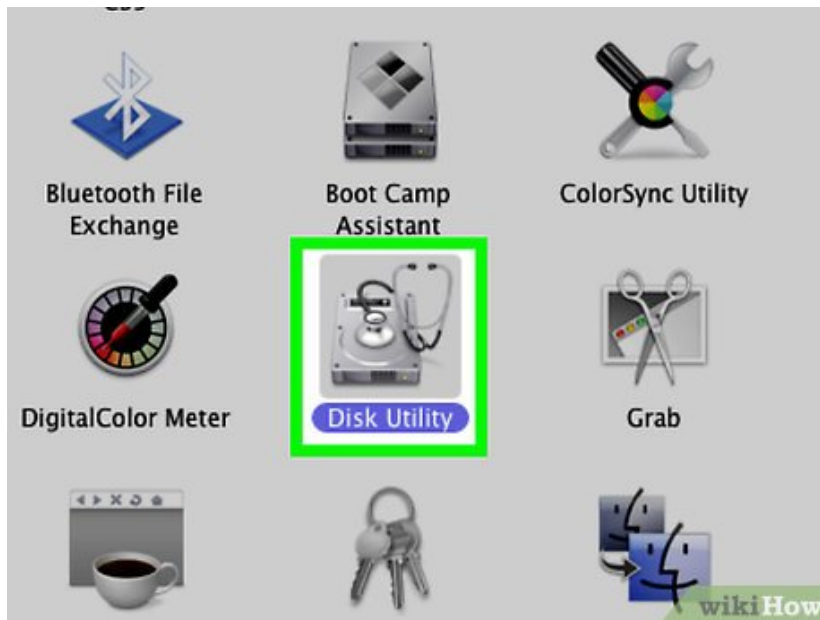


**Encrypting important private files and folders is a great method of keeping them from prying eyes that may have been able to access your machine through a Wi-Fi network.**



**On Windows, right-click the file or folder you want to encrypt, select 'Properties' from the context menu.**

1. Select the 'General' tab from within the Properties dialog, followed by 'Advanced'.
2. In the 'Advanced dialog select 'Encrypt contents to secure data' followed by 'OK'.



**On Mac OS X, you can encrypt files by creating a virtual password-protected drive to store sensitive files and folders.**

1. Open the Finder and navigate to Applications>Utilities> and double-click Disk Utility.
2. From within Disk Utility, select File>Blank Disk Image.
3. Enter a name in the 'Save As:' field and select '128-bit AES encryption (recommended)' from the 'Encryption' drop down menu. You can also browse to select a specific location to save the new disk image.
4. Click the 'Create' button.
5. Enter a password and verify a password for the disk image and click 'OK'. A new '.dmg' disk image will be created. Double-click it to open it as a virtual drive. You can now simply drag and drop files and folders onto the virtual, password-protected drive to keep them protected when on a Wi-Fi network.

You finished reading the article "**How to Be Safe When Using WiFi**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.