



# Reasons Not To Use Public Wi-Fi Networks

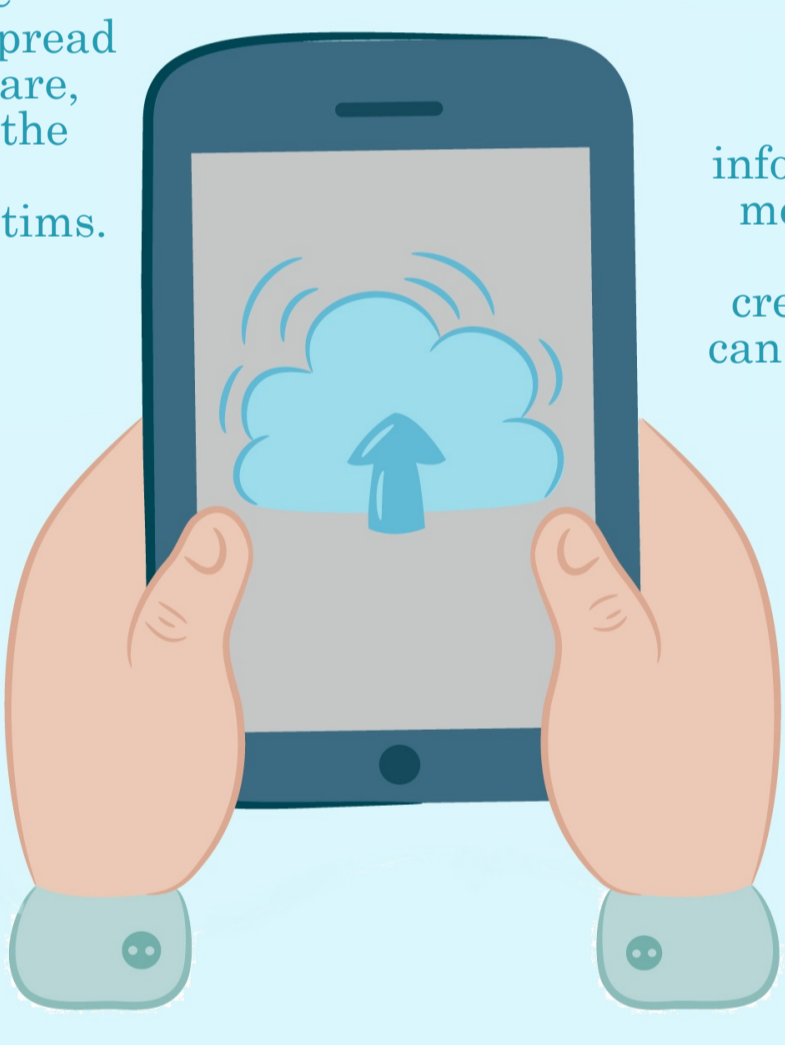
Public Wi-Fi networks that provide free internet access can be found at places like coffee shops, malls or hotels. However, these networks are not as secure & it is extremely important to be cautious while accessing them.

Most common threat while using Public Wi-Fi is Man-In-The-Middle attack. In these attacks, hackers may intercept the user data using techniques like eavesdropping.

A network needs to be encrypted for it to be secure, which is quite expensive. Public Wi-Fi networks often lack encryption and so lack the ability to protect your data.

Hackers may use public Wi-Fi to spread all sorts of malware, trojans etc. over the systems of unsuspecting victims.

Your personal information, i.e. social media accounts, chat messages, login credentials (banking) can be easily stolen by hackers.



## Ways To Protect Yourself While Using Public Wi-Fi

Visit websites that have HTTPS in their URL

Use a VPN to make Public Wi-Fi connections private on your device.

Don't make online transactions while using public Wi-Fi.

Implement two factor authentication for your personal accounts.



[www.centextech.com](http://www.centextech.com)  
Centex Technologies



13355 Noel Road,  
Suite # 1100, Dallas, TX 75240  
Phone: (972) 375 - 9654

501 N. 4th Street,  
Killeen, TX - 76541  
Phone: (254) 213 - 4740

1201 Peachtree St NE,  
Suite 200, Atlanta, GA 30361  
Phone: (404) 994 - 5074

Image Source: Designed by Freepik