Why "Free" Wi-Fi Isn't Really Free: The Hidden Risk of Public Internet

Authors: Krishna CV Grandhi, Chandra Lekha

Wi-Fi has become a necessity in today's world. A stable internet is what ensures that you can complete your tasks, studies or the movie you were watching to unwind after a long day. Resultantly, there has been an increased use of 'Public Wi-Fi' networks, which are convenient, easy to access and often free. Reports find that 70% of laptop users and 35% of phone or tablet users are connected to Public Wi-Fi.

However, no service is truly free, and in the case of Public Wi-fi networks, the price is the user's privacy and security. This is because Public Wi-fi networks are often unsecured, making it a hidden treasure for hackers. Some of the most common attacks via Public Wi-Fi networks are:

Man-in-the-Middle Attack

Hackers find the free internet networks which are often unprotected and may be used to gain access into the connected devices. Hackers often spy on these connections, and intercept any data that is being transferred through such connections, leading to hackers finding out a user's sensitive information like banking credentials, passwords, and personal messages.

Fake Hotspots

Devices are hacked by cybercriminals, where they replicate a known connection leading users falsely believing and connecting to the fabricated network created by the hacker following which hackers get complete access to the user's device, leading to a complete compromise of the user's data.

Unencrypted Connections

Public Wi-Fi networks are often unencrypted, meaning that the data is transmitted in plain text, making it vulnerable to cybercriminals to intercept the data by using certain legal or illegal tools.

How to stay safe?

To ensure that users don't fall prey to such attacks, certain precautions may be effective:

1. Using a VPN.

   VPN is an internet service which provides a safe private network over a public network to ensure secure online access. In the case of Public Internet, using VPN can ensure that a user's connection is robust and has iron-clad security.

2. Enabling Two-Factor Authentication.

Strong and unique passwords can be compromised and data stolen by hackers by intercepting Public Wi-Fi networks. Therefore, in order to strengthen device protection, Two-Factor Authentication may be enabled, where even if a hacker secures the password to a user's device, they will not be able to access the user's accounts without the second authentication step. Such two layer authentication steps may include codes or messages sent to the user's smartphone. Two-Factor Authentication essentially adds a second layer of security, keeping the data hidden from attackers.

3. Using Antivirus Software.

Good Antivirus Software does more than blocking viruses; they protect the devices against malware, suspicious downloads, and hacking attempts, providing an extra shield while using public networks.

Public Wi-Fi networks can be convenient and useful if used with the right tools and safety measures. While a Public Wi-Fi systems comes with its own pros and cons, proper utilisation may allow users to reap its benefits and ensure protection of personal data at the same time.

www.csail.org