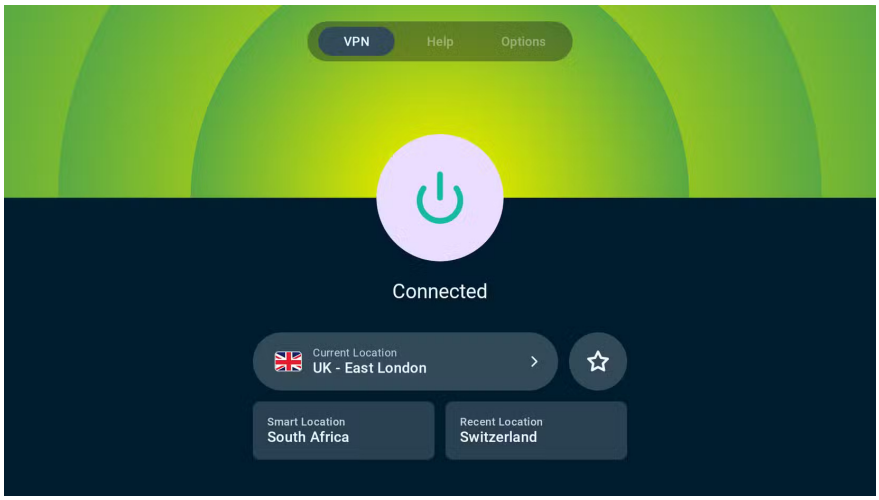
Safety rules when using public WiFi

Many people have been confidently using WiFi networks in airports, cafes and hotels for years, but only if they follow the following safety rules.

Public WiFi isn't going away, and neither are its risks. People have been confidently using WiFi networks in airports, cafes, and hotels for years, but only if they follow these safety rules.

6. Always enable VPN



A virtual private network (VPN) creates an encrypted tunnel between your device and the Internet . Encrypting your traffic prevents unauthorized parties from monitoring your activity or stealing sensitive information.

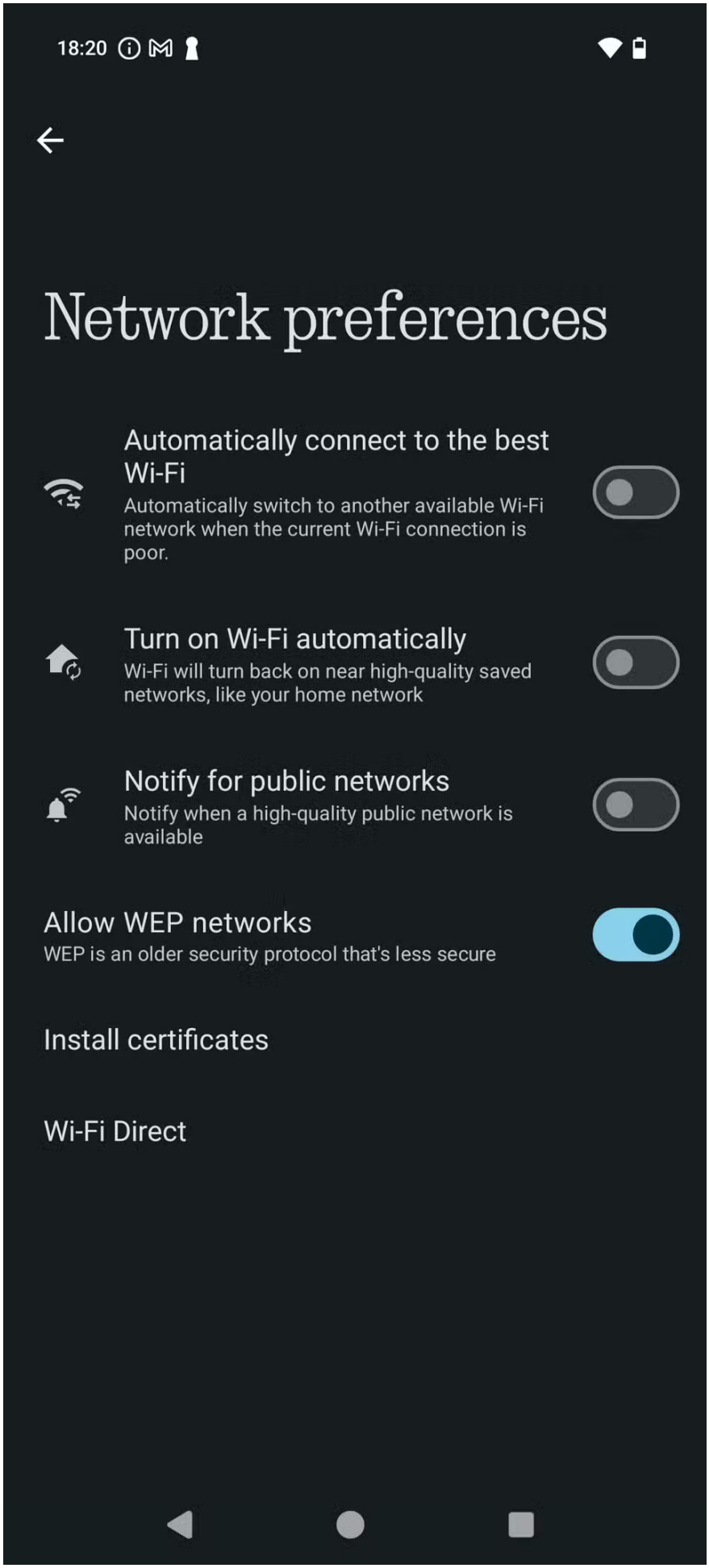
Since premium VPNs are often extremely cheap for multi-year subscriptions, it's worth getting one to avoid any potential issues. Many VPN providers, such as NordVPN and CyberGhost , offer apps with auto-connect features. Enabling these apps ensures that your device connects securely as soon as it detects a public network. This proactive step significantly reduces your risk of being attacked, especially if you travel frequently.

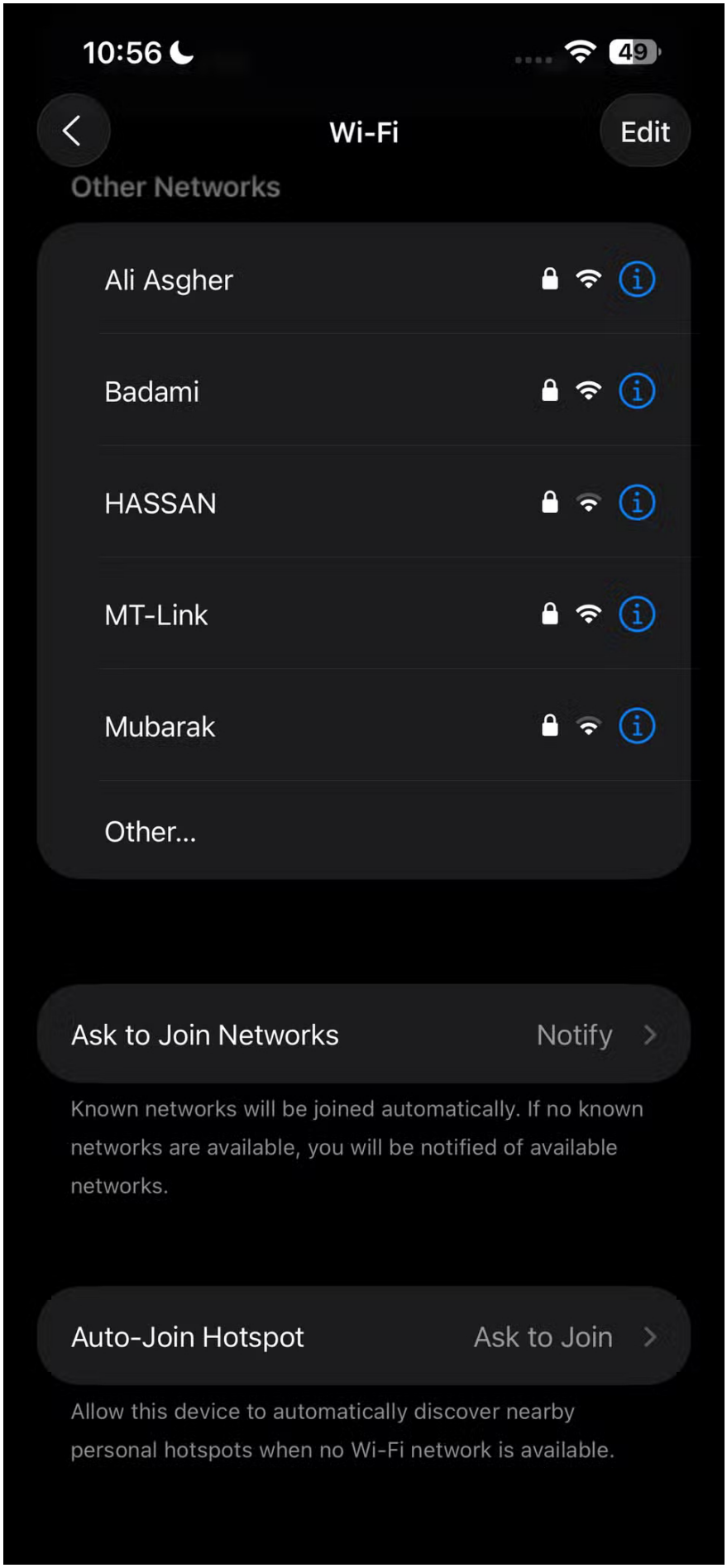
5. Turn off Auto-connect feature

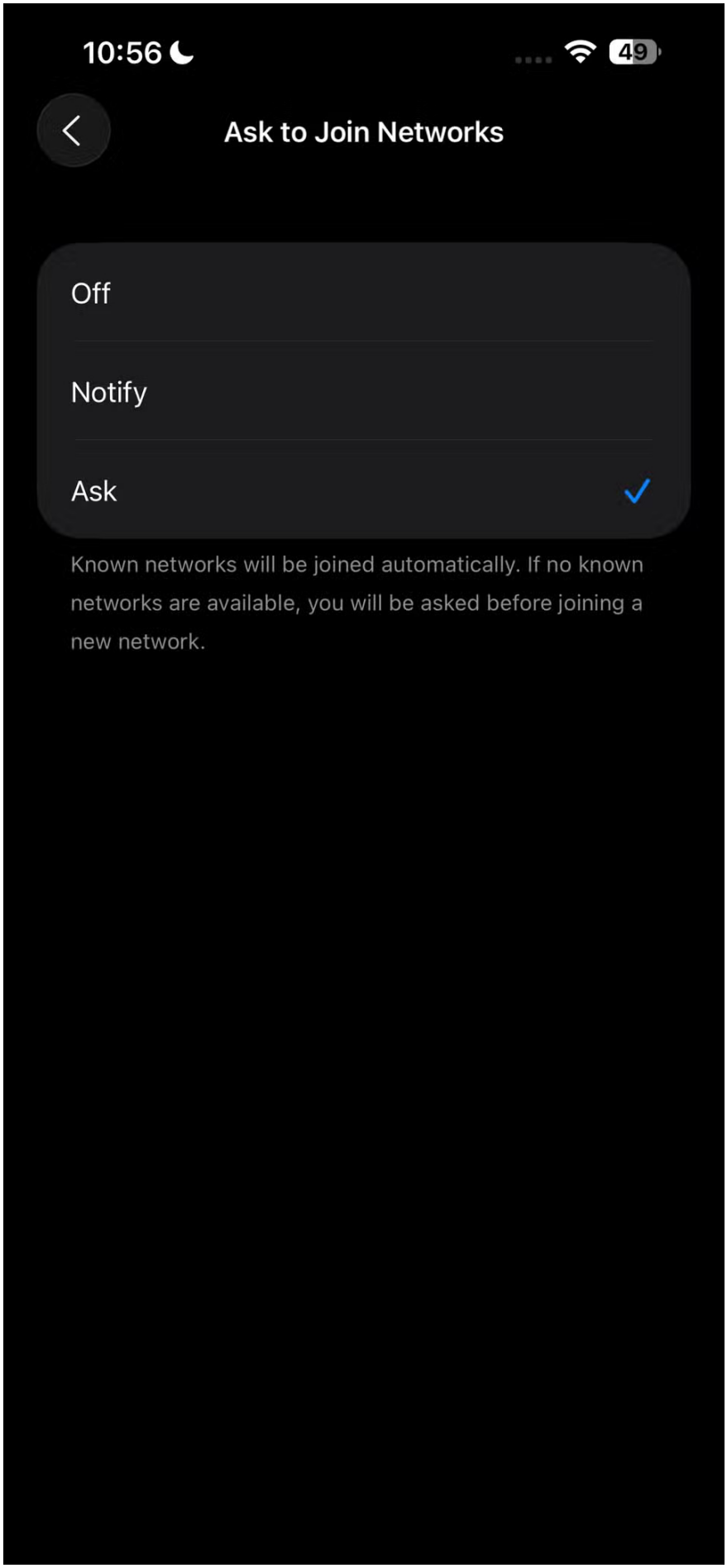
Devices often have settings that allow them to automatically connect to previously used or trusted networks. While convenient, this feature can expose you to security threats, especially in public places.

The idea of malicious hotspots in public places is certainly unsettling and dangerous. There are numerous examples of hackers creating fake hotspots with familiar or trusted names, such as 'Airport_Free' or 'Starbucks_WiFi,' to trick users into automatically connecting, which could give the attacker access to sensitive data.

To prevent this, turn off auto-connect in your WiFi settings. This simple change ensures you're aware of every attempt to connect to a network, giving you control over your security. Regularly check your network settings to make sure auto-connect is still turned off, especially after a software update or device reset.


18:20
Network preferences
Automatically connect to the best Wi-Fi
Automatically switch to another available Wi-Fi network when the current Wi-Fi connection is poor.
Turn on Wi-Fi automatically
Wi-Fi will turn back on near high-quality saved networks, like your home network
Notify for public networks
Notify when a high-quality public network is available
Allow WEP networks
WEP is an older security protocol that's less secure
Install certificates
Wi-Fi Direct


10:56
49
Wi-Fi
Edit
Other Networks
Ali Asgher
Badami
HASSAN
MT-Link
Mubarak
Other...
Ask to Join Networks
Notify
Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.
Auto-Join Hotspot
Ask to Join
Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.


10:56
49
Ask to Join Networks
Off
Notify
Ask
Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Whether or not your device automatically connects to WiFi, take a moment to review each WiFi network you connect to.

4. Confirm network name with staff

Try the easiest security check: Just ask someone who works there. If you're worried about fake WiFi hotspots, ask an employee to confirm that you're connecting to the right one.

Never assume a network is legitimate based on its name alone. Taking the time to verify can prevent potential security breaches and protect your personal information.

3. Use HTTPS-Only mode or always use secure connections

HTTPS-Only mode is one of the important browser security features that everyone should enable. It essentially forces your browser to always use the more secure HTTPS protocol , protecting your data from prying eyes.

In the past, security and privacy enthusiasts have used the EFF's HTTPS Everywhere extension to protect their data. Fortunately, modern browsers now use HTTPS by default; however, you should still enable it to ensure your browser always uses it.

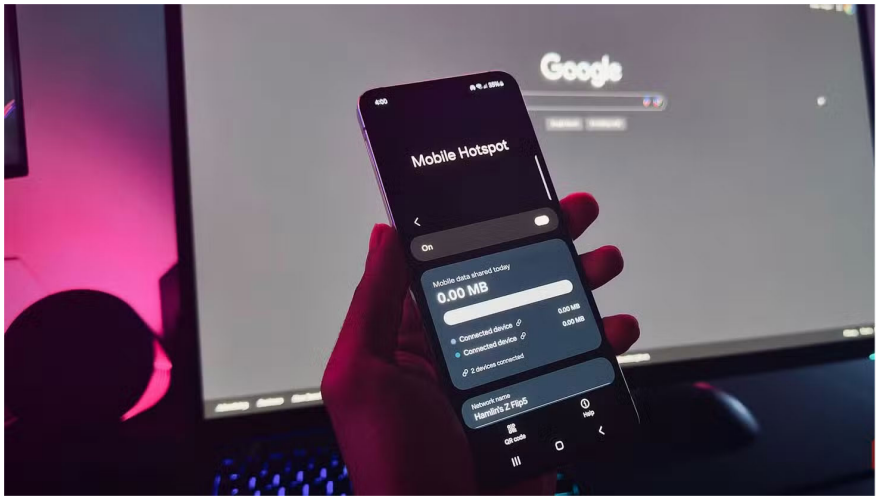
This feature goes by different names depending on the browser you're using. For example, in Google Chrome , you'll need to enable the **"Always Use Secure Connections"** option , while in Firefox, look for HTTPS-Only mode.

2. Turn off Airdrop and Nearby Share

File sharing features like AirDrop (Apple) or Nearby Share (Android), along with Bluetooth , are incredibly convenient when used in trusted environments, but pose significant risks on public WiFi. Enabling these features can inadvertently expose your device to nearby attackers who can exploit open connections or security vulnerabilities.

It's best to turn off these easy sharing features until you need them.

1. Use hotspot on phone



People swear by using smartphone hotspots instead of public WiFi. It's convenient, works almost instantly, and most of the time provides internet speeds comparable to the public WiFi you're using.

But it's not all about convenience. Connecting directly to a hotspot on your smartphone eliminates the risks of public WiFi and keeps your communications on a private network. You can adjust the security protocols on your smartphone and set a strong , unique password to prevent others from accessing it, and that's it!

The most obvious downside to using a hotspot is that it can cut into your monthly data allowance. You should consider what you'll do if you use a hotspot like this; for example, don't download a 4K movie until you get home.