These safe alternatives to public Wi-Fi help protect your data

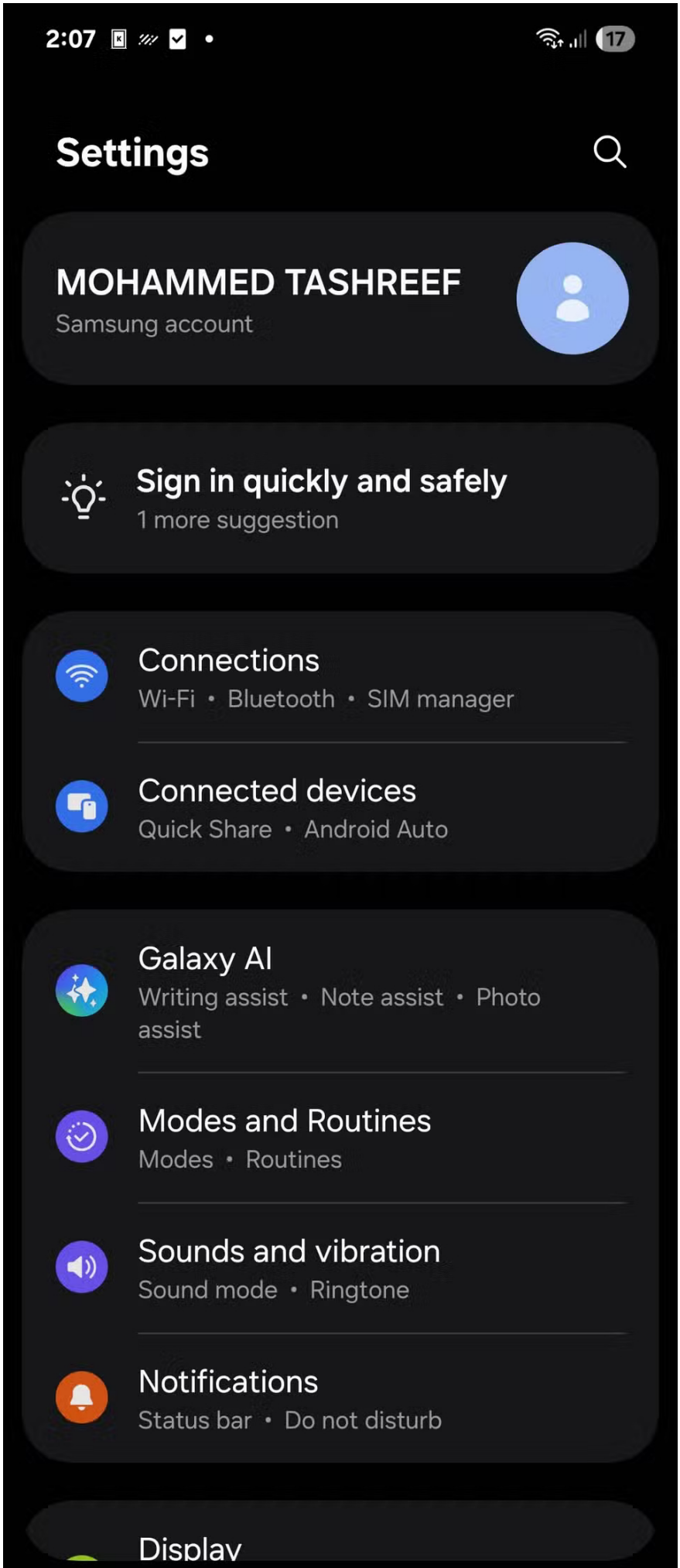
Whether you're working at a coffee shop or checking email at the airport, these more secure alternatives will keep your data secure without sacrificing your connection.

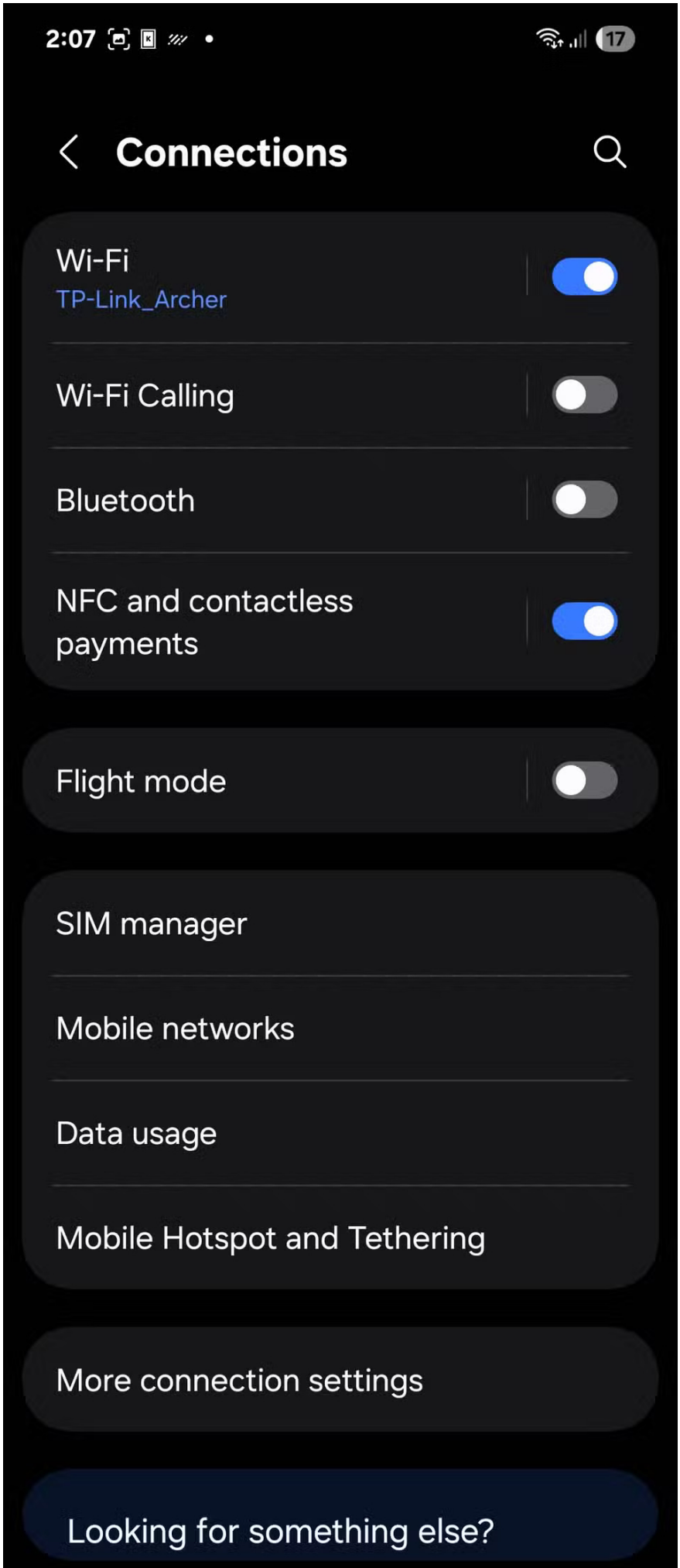
Public Wi-Fi is everywhere, but when the network isn't yours, you're never sure what's going on there. Whether you're working in a coffee shop or checking email at the airport, these safer alternatives will keep your data safe without sacrificing your connection.

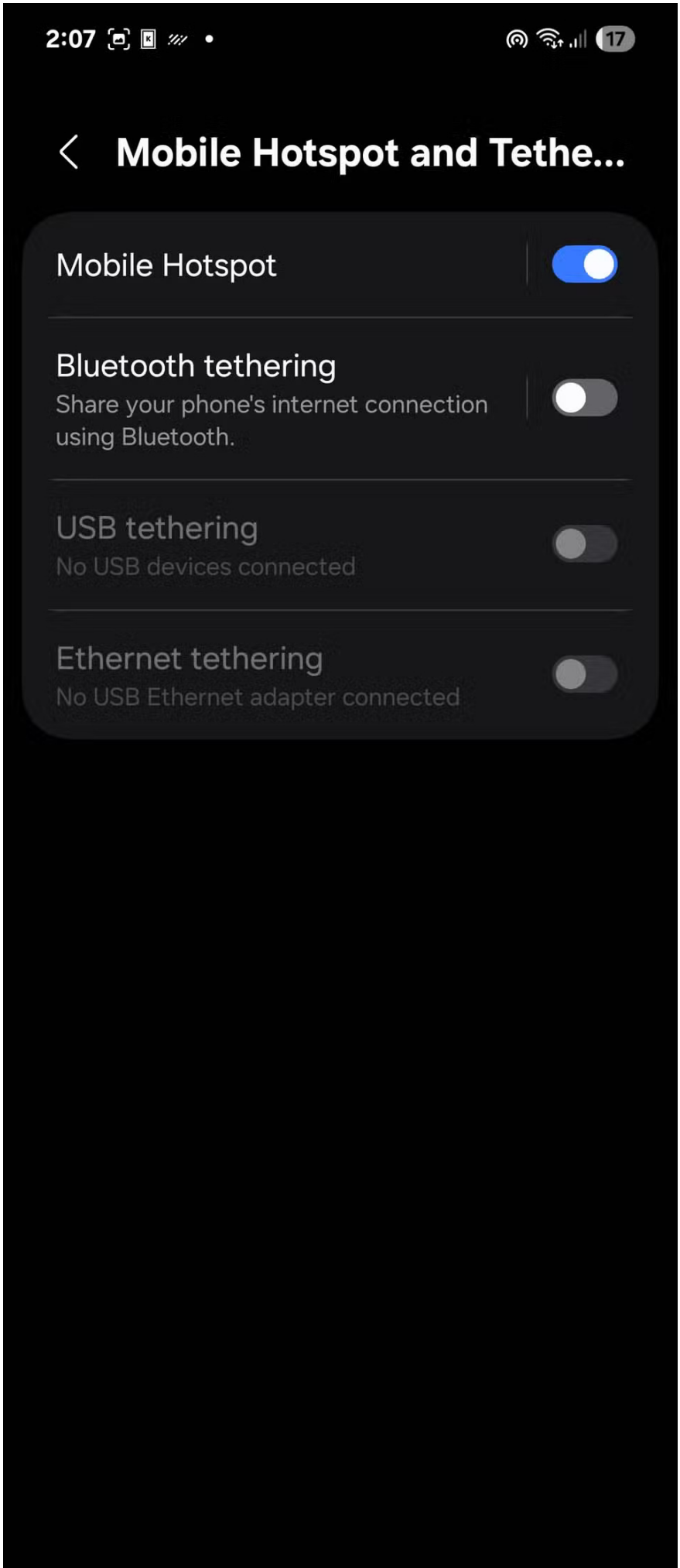
6. Mobile hotspot from phone

A mobile hotspot on your smartphone is the easiest way to avoid the risks of public Wi-Fi. Unlike shared networks, where anyone can snoop on your data, your phone creates a private connection, allowing you to control who has access to it.

Setting it up takes just a few seconds on both Android and iOS. On Android, you'll find it under **Settings > Connections > Mobile Hotspot & Tethering** . For iPhone, go to **Settings > Personal Hotspot** . Before turning it on, make sure to set a strong password that others can't easily guess. Once enabled, your laptop will connect to your phone's network just like any other Wi-Fi, except you know it's secure.


2:07
17
Settings
MOHAMMED TASHREEF
Samsung account
Sign in quickly and safely
1 more suggestion
Connections
Wi-Fi • Bluetooth • SIM manager
Connected devices
Quick Share • Android Auto
Galaxy AI
Writing assist • Note assist • Photo assist
Modes and Routines
Modes • Routines
Sounds and vibration
Sound mode • Ringtone
Notifications
Status bar • Do not disturb
Display


2:07
17
Connections
Wi-Fi
TP-Link_Archer
Wi-Fi Calling
Bluetooth
NFC and contactless payments
Flight mode
SIM manager
Mobile networks
Data usage
Mobile Hotspot and Tethering
More connection settings
Looking for something else?


2:07
17
Mobile Hotspot and Tethe...
Mobile Hotspot
Bluetooth tethering
Share your phone's internet connection using Bluetooth.
USB tethering
No USB devices connected
Ethernet tethering
No USB Ethernet adapter connected

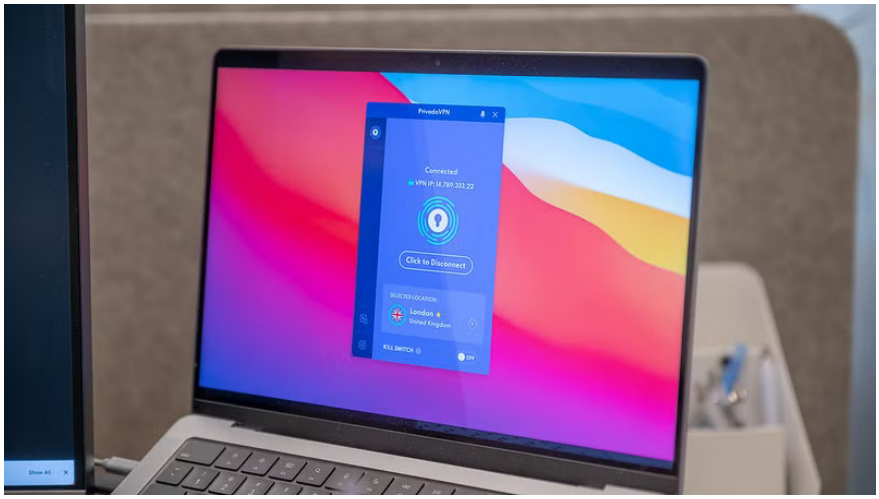
5. Dedicated mobile hotspot devices and travel routers

While a phone hotspot is useful in emergencies, a dedicated mobile hotspot (also known as a MiFi) offers better performance and more security features for those on the go. These compact networking devices can connect more than 15 devices at once and often have all-day battery life on a single charge. However, they require a separate data plan and an extra device to carry.

Travel routers , on the other hand, help you create a secure and convenient network when using public Wi-Fi. For example, the GL.iNet GL-MT300N, which is about the size of a deck of cards, can be configured to run a router-level VPN when connected to a hotel's Wi-Fi. You'll need to subscribe to a separate VPN, and you may have to enter VPN credentials or upload configuration files during setup.

4. VPN on public Wi-Fi

If you absolutely need to use public Wi-Fi, a VPN can add an extra layer of security. It creates an encrypted tunnel for your data, making it unreadable to anyone trying to intercept it. Even if you accidentally connect to a rogue hotspot, your information is still protected.



If you want security and reliable performance, consider a reliable paid option like ExpressVPN or NordVPN . These services typically cost between $3 and $12 per month and offer strong encryption, faster speeds, and a wide range of global servers.

3. Ethernet connection

If you're in a hotel or co-working space, a wired Ethernet connection is one of the most secure and reliable ways to access the Internet. Because you're physically connected to the network, it's much harder for someone to steal your data. That's exactly why many people still choose Ethernet over Wi-Fi whenever possible.

2. USB Tethering

Sometimes the simplest solution is the most effective. USB Tethering allows you to use your phone as a wired Internet connection with just a charging cable. To share your Android phone's Internet connection with your computer , simply connect your phone to your laptop using a cable, then enable USB Tethering sharing in your phone's settings. Since your phone is still charging while sharing mobile data, you don't have to worry about battery drain.

1. Connect securely to public Wi-Fi

While it's true that you won't be hacked just by connecting to public Wi-Fi, the real threat comes from what you do after you're connected. Banking, shopping, or logging into accounts on unsecured networks can put your data at risk. If public Wi-Fi is your only option and there are no other alternatives, there are a few precautions you can take to protect yourself.

If you must use public Wi-Fi, use free Wi-Fi finder apps to identify legitimate networks that have better security measures than random open connections.