

Staying Safe on Public WiFi

Free WiFi in cafes, airports, or other public spaces can put your data at risk. Attackers exploit open networks to steal information or spread malware, making public WiFi inherently insecure.



How Attacks Happen



Fake Hotspots

Criminals can set up WiFi networks that appear legitimate, tricking users into connecting. Once connected, attackers can intercept your data.

Tip: Use a VPN to encrypt your connection and stay secure on public networks.



Traffic Sniffing

On open WiFi, hackers can monitor unencrypted traffic, capturing passwords, emails, and other sensitive information.

Tip: Avoid logging into sensitive accounts while on public WiFi.



Malware Distribution

Some public networks can be used to push malware to connected devices, compromising security without users noticing.

Tip: Stick to mobile/cellular data when possible and avoid auto-connecting to unknown networks.



Prevent Auto-Reconnection

Devices often reconnect automatically to previously used networks, which could be malicious.

Tip: Forget public networks after use to prevent unintended connections.