Sentrly — Public Wi-Fi Safety Checklist

Use airport, café and hotel Wi-Fi without leaking credentials.

Before you connect

- ■ Confirm the exact network name with staff.
  Fake hotspots use names like 'Starbucks_Free' to lure you in.
- ■ Turn on your VPN before joining.
  Joining first means a window where DNS, captive portal and updates run in clear.
- ■ Set 'public' or 'untrusted' as the network type when prompted.
  Most operating systems block file sharing and discovery on public networks.

While connected

- ■ Avoid logging into accounts you don't have 2FA on.
  If credentials leak, 2FA is the difference between an attempted login and a real one.
- ■ Skip banking and password-manager logins on shared computers entirely.
  Shared computers are out of your control — and may be keylogging.
- ■ Watch for HTTPS downgrade warnings; if a site falls back to HTTP, walk away.
  Captive portals occasionally interfere; persistent issues are a red flag.
- ■ Don't accept extra TLS certificates unless your IT department asked you to.
  Self-signed certs on coffee-shop Wi-Fi are how interception attacks start.

After you disconnect

- ■ Forget the network if you don't plan to reuse it.
  Stops your device auto-rejoining a spoofed copy elsewhere.
- ■ Review login history on the accounts you used.
  Catch unfamiliar locations early — most providers show recent logins in account settings.