A HACKER'S SECURITY GUIDE // INFOGRAPHIC 08/08

AWAY FROM HOME: PUBLIC WI-FI, CONNECTIONS, AND TRAVEL

Coffee shops, airports, and hotels are shared territory: networks you don't control and exposed devices. The right habits for each scenario.

>> THREE SCENARIOS, ONE RULE

CAFÉ / MALL

- × No online banking or shopping on third-party Wi-Fi unless you trust the network and its provider
- » When in doubt, use your mobile data
- » Never leave your device alone, not even for a minute

AIRPORT

- × Public USB charging ports: they can sync your data
- » Your own charger in a wall outlet, or charge-only mode with protection
- » Verify the exact name of the official network before connecting

HOTEL

- × Don't leave devices in plain sight in the room
- » Use the safe for whatever you don't carry with you
- » Sessions signed out and device locked at all times

>> BEFORE YOU TRAVEL: DEVICE CHECKLIST

1. **Full backup**
   If the device gets lost or stolen, your information still exists.
2. **Disk encryption enabled**
   An advanced security measure: without your key, the device's contents are unreadable.
3. **Find-my-device turned on**
   Tracking, locking, and remote wipe available from another device.
4. **Travel light on data**
   Carry only what you need on the device: what isn't there can't be stolen.

>> IN ANY PUBLIC PLACE

→ Prying eyes

A privacy filter on your screen, and care when typing passwords around other people: don't make it obvious.

→ Physical safekeeping

Stealing the device itself is still the most common attack. On you or under lock and key, no exceptions.

THE SHARED-TERRITORY RULE

On networks you don't control, behave as if someone were watching. Sometimes someone is.