



Protecting Against Physical and Digital Targeting: Location Sharing

- Malicious actors (such as criminals, terrorists, and foreign intelligence officers) use social media sites to gather information that can be used to hurt you, rob you, or compromise your online accounts.
- Location sharing is the easiest way for malicious actors to find you in real life. Sharing your current location, travel plans, or daily pattern of movement can make you easy to find.
- Don't share your location unless you decide it's worth the risk.

If you announce details of your travel to a high-threat environment, you may be putting yourself at additional risk of **physical targeting**

Thieves have been known to rob homes after the owner posted a status that they would be out of town

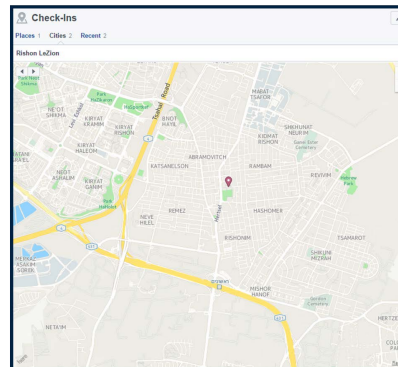


Most photos include hints about your location. Even though Fred didn't explicitly say where he is, it would be easy to guess

A malicious actor could easily find his **current location** or realize that he is away from home



When you tag your current location, a malicious actor or **foreign intelligence** officer can track you down, or establish your pattern of behavior



If you tag yourself somewhere that you visit often, malicious actors can **predict** that you will be there again



On Twitter, if this **pin** is highlighted, your location will be automatically attached to your tweets. Click the pin to turn location sharing off

- ## Protect Yourself
- Never "check in" at home or work
 - Avoid announcing current/future travel plans
 - Consider waiting until you've left a location to "check in," and avoid revealing what businesses/locations you frequently visit