Threat Modeling

"A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called threat modeling. Once you have a threat model, you can conduct a risk analysis."
- EFF

1. What do I want to protect?

2. Who do I want to protect it from?

3. How bad are the consequences if I fail?

4. How likely is it that I will need to protect it?

5. How much trouble am I willing to go through to try to prevent potential consequences?

What are my *assets*?

Who are my *adversaries*?

What are the *threats* of my adversaries?

What is the *risk* of ___ happening?

Bike Courier Marijuana Delivery Person

Assets:

Adversaries:

Threats:

Bike Courier Marijuana Delivery Person

Assets: Bicycle, Inventory, Identity, Identity of Employer, Money

Adversaries: Law enforcement, bicycle thieves, reckless drivers

Threats: Wiretapping, arrest, steal bicycle, run over with car, DEA sting

Sex Work Provider in NYC

Assets: *Photos, legal id, address, social media accts, email, communications, texts, bank acct, payment legers, contacts*

Adversaries: *Cops, stalkers, family, exes, journalists, careless ppl, catfish, trolls, anti sex work ideologues, algorithms*

Threats: *Location tracking spyware, doxxing, blackmail, report police, steal photos, intercept, falsified charge reason/arrest reason, reporting status as sex work provider to 'vanilla' job*