online sos

onlinesos.org

Threat Modeling

First

- **Consider your intangible assets. Who/what do you want to protect?**
  - *Write down any assets from the list below and/or others, in order of priority*
    - Yourself, your spouse, children, family, friends, colleagues
    - Personal privacy
    - Personal control over identity
    - Access to free flow of information
    - Separation of online personas
    - Integrity and trust you or organization has built
- **Then consider your tangible assets. What do you want to protect?**
  - *Write down any assets from the list below and/or others, in order of priority*
    - Physical assets like car, laptop, phone
    - Photographs or video - on phone, laptop, in the cloud
    - Private documents, like financial statements and client reports
    - Online accounts
    - Contact lists of sources, partners, clients
    - Communication with editors, activists, and/or colleagues
    - Time-sensitive research and data
    - Draft documents and articles, sometimes involving collaborators
- **Who do you want to protect it from?**
  - *List these individuals next to listed assets*
    - Abusive partner or ex-partner
    - Criminals (burglars)
    - Cybercriminals (hackers)
    - Online abusers (trolls)
    - Other abusers (in the workplace, at home, etc)
    - Government agencies
    - Individuals looking to discredit you (partner's ex-spouse, online adversary, etc)
    - Individuals looking to get access to information you have
    - Roommates or guests in your home

Then

- ❏ **Determine how likely it is that you will need to protect the assets you listed**
  — Consider and write down:

  - ❏ Severity of threat to assets you listed (high, moderate, low)
  - ❏ Capabilities of adversaries (highly capable of carrying out threat, etc)
  - ❏ Trustworthiness of individuals (highly trustworthy, less trustworthy, etc)

- ❏ **Determine how bad the consequences will be if you fail**
  — Answer the following questions to determine consequences:

  - ❏ Do you have any intangible assets that are at risk? At home? At work?
  - ❏ Do you have any tangible assets that are irreplaceable?
  - ❏ Do you have time and/or money to replace assets?
  - ❏ Do you have insurance to cover stolen goods?
  - ❏ Do you have protection and/or support from your employer in the face of threat?

Next

❏ **What are you willing to do to prevent or reduce these consequences?**
— Consider: Amount of money you are willing to spend on the following:

❏ Physical security (lock, security box, security system, safes, etc.)
❏ Digital security (subscriptions to info-scrubbing services, etc.)
❏ Emotional and mental health (counseling sessions, yoga classes, etc.)
❏ Legal (hiring a lawyer, getting consultations, going to court, etc.)

— Consider: Amount of time you are willing to spend on the following:
❏ Physical security (installing locks or security systems, etc.)
❏ Digital security (installing password managers, 2FA, etc.)
❏ Emotional and mental health (attending counseling, break from internet)

— Consider: Risks you are willing to take on the following:
❏ Your health/wellbeing (mental, physical, emotional)
❏ Your relationships (partner, parents, friends/acquaintances)
❏ Physical possessions (laptop, car, phone)
❏ Employment
❏ Clients
❏ Other forms of credibility (audience/readers, company reputation)

What are the outcomes you want, based on measures you are willing to take? *May include: Security of digital devices and passwords, job security, physical safety, legal recourse against online abuser(s)*

Consider
● If you have been harassed online, start by identifying the type of harassment you are facing
● To help determine who is threatening you and/or your assets, answer these questions:
    ○ Would anyone want to stop you in your activities? If so, who?
    ○ Does anyone want to know what you do? If so, who?
    ○ Have you had any reasons to worry about your online activities or your devices?
● To assess specific, active risks, answer the following questions:
    ○ What is the specific text/content of abuse (threat made in email, etc)?
    ○ What is the volume of the abuse (multiple messages, tweets, emails)?
    ○ What is/are the sources of the abuse? (Twitter account, email account)?
    ○ What is the timeline of the abuse? (How long has it lasted, is it ongoing, etc?)