PRIVACY 101: ASSESSING YOUR RISK

WHAT IS A RISK ASSESSMENT?

Risk assessments, also known as "threat models," are how we understand our specific privacy and security needs.

A SECURITY MINDSET

A security mindset is an important part of a risk assessment. It means asking questions like:

- What data trail am I creating?
- What data am I being asked for?
- Who can see my data? How will they use it?
- Is the data relevant to completing the task?
- Can I skip optional fields and minimize the data I'm sharing?
- Am I putting people I care about at risk with my data sharing choices?
- How might my life situation and risk assessment change in the future?

RISK ASSESSMENT FRAMEWORK

What do I want to protect?

Ex: My identity while protesting.

Who do I want to protect it from?

Ex: Bad actors who may wish to share my info without my consent or otherwise harm me.

What bad things can happen if I don't protect my data?

Ex: An online harassment campaign against me.

How likely are these consequences?

Ex: This has happened to people I know.

How much work am I willing to do to protect myself?

Ex: I'm willing to cover my face, hair, and other identifying features.

Risk Assessment Framework	Example: I want to avoid identity theft or fraud when I go online.	Practice your own risk assessment here:
What do I want to protect?	My browsing and search history. The personal information required for job applications.	
Who am I protecting it from?	Scammers and identity thieves. Malware or computer viruses.	
What bad things can happen if I don't protect my data?	Financial harm and credit score impacts.	
How likely are these consequences?	I know others who have been scammed, and I get lots of spam emails, calls, and text messages.	
How am I willing to protect myself?	I'll make sure my passwords are unique and strong, and I'll try some password managers to find out which one works for me. I'll use a privacy-forward browser. I'll delete apps I haven't used lately. I won't click on suspicious links in my emails or texts.	