Online Privacy Checklist –

What can you do to maintain your online safety & autonomy?

1. Take stock of your online presence

- ❏ Check haveibeenpwned.com to see if your account credentials have been included in any past breaches. Prioritize changing these credentials in step 2.
- ❏ Open an incognito browser window and Google yourself.
  - ❏ Take note of anything you want to be removed from your search results (you will find public data websites with your address, phone number, etc.)
  - ❏ Are your social media accounts showing up in Google searches? Are your profiles public?
  - ❏ Consider what public information might be online about you, such as professional licensure, website registration (WHOIS), voter registration, corporate or nonprofit filings, real estate records..

2. Secure your accounts

- ❏ Change your most important passwords so they are unique and longer than 12 characters. Use passphrases to get to 12.
  - ❏ BONUS POINTS: Download & start using a password manager to store all your new, unique passwords.
- ❏ Secure your important accounts with two-factor authentication.
  - ❏ BONUS POINTS: Set up the Authy app (https://authy.com/) as your second factor of authentication.
- ❏ Be on high alert for phishing emails.
  - ❏ BONUS POINTS: Take the google phishing quiz to practice spotting the phish https://phishingquiz.withgoogle.com/

3. Make your harassment prevention & response plans

- ❏ Remember your Google results? Complete the information removal process (https://tinyurl.com/nytInfoRemoval) for the sites you found with your data.
- ❏ Set up Google Alerts for your name, number, & address.
- ❏ Explore and tighten your social media privacy settings using this guide from the New York Times: https://tinyurl.com/nytPrivacyGuide
- ❏ Consider using an alternative address & number.
    - ❏ Purchase a commercial mail receiving agency box (like a UPS box) so you have an address to use besides your home address
    - ❏ Get a free Google Voice or affordable Twilio number to use.
- ❏ Talk with your loved ones & friends about your increased risk profile, and recruit them:
    - ❏ As supporters to help you deal with trolls if you are targeted.
    - ❏ To consider the information they post publicly about you.
- ❏ Make a response plan before you need one.
    - ❏ Identify a safe place to go or a friend to come over if you feel unsafe at home.
    - ❏ Learn how to document threats to save as evidence.
    - ❏ Enlist colleagues, friends, & loved ones as a community safety team to help you deal with future attacks.

Resource library:

- Protection from Online Harassment Guide by Renee Bracey Sherman (abortion storyteller!): https://onlinesafety.feministfrequency.com/en/
- DIY Feminist Cybersecurity Guide: https://hackblossom.org/cybersecurity/
- Personal Data Removal Workbook: https://inteltechniques.com/data/workbook.pdf
- C.A. Goldberg Incident Tracking Sheet and Tips for Documenting Harassment: https://www.cagoldberglaw.com/incident-tracking-chart/