Online Harassment Self-Defense Resources

- **PEN America Online Harassment Field Manual**: https://onlineharassmentfieldmanual.pen.org/
- **HeartMob:** https://iheartmob.org/
- **Trollbusters:** http://www.troll-busters.com/
- **ADAA – Guide to Affordable Mental Health Care**: https://adaa.org/finding-help/treatment/low-cost-treatment
- **PEN America – Online Harassment Field Manual – Advice from a Psychologist:** https://onlineharassmentfieldmanual.pen.org/advice-from-a-psychologist/
- **Reporters Committee for Freedom of the Press - Legal Assistance Hotline:** https://www.rcfp.org/legal-hotline/
- **Cyber Civil Rights – Pro-Bono Legal Project:** https://www.cybercivilrights.org/professionals-helping-victims/

Cyber Security Resources

- **Citizen Lab – Security Planner**: https://securityplanner.org/
- **Access Now – Digital Security Helpline:** https://www.accessnow.org/help

Cyber Security Tools & Tips -- PHASE I

***SEE: PEN America – Online Harassment Field Manual – Cyber Security Section:** https://onlineharassmentfieldmanual.pen.org/prepare/

- **Keep Software and Mobile Apps Updated!**

- **Get Password Manager**
  TIP: Get browser extension & mobile app, which can automatically generate secure passwords and autofill them.
  - LastPass (free): https://www.lastpass.com/
  - DashLane (free): https://www.dashlane.com/
  - 1Password (free for journalists): https://1password.com/for-journalism/

- **Practice Password Hygiene**
  TIP: Pick a random phrase OR pick your favorite song lyric or book title, pick first letter of each word, capitalize few of letters, then add few numbers or punctuation
  - At least 16 characters (eg: correcthorsebatterystaple)
  - One-to-one rule: different password for EVERY account
  - Invent security questions (avoid Google-able answers, like mother's maiden name)

- **Set up Two-Factor Authentication (2FA)** – on professional and personal accounts
  TIP: This is one of the best things you can do to protect yourself online – better to use an authenticator app, NOT text message.
  - **What is 2FA?** Whenever there is an attempted login to your account from an unrecognized device, you must authenticate it using a one-time-use code (delivered via app or text message).
  - Start with your core accounts (email, Twitter, Facebook, Instagram, etc.)
    - List of accounts and platforms that support 2FA: https://twofactorauth.org/

- **Watch out for SIM Jacking --** for more, see VICE: https://bit.ly/2ZmWSkv

- **What is it?** Hackers call your mobile provider pretending to be you, explain you've "lost" your SIM card, and then request that your phone traffic be routed to a new SIM card (in the hacker's hands).
- **What to do:** call your mobile provider and ask that a PIN be placed on your account, which can be used to verify your identity before any changes are made in future.

- **Set up Virtual Phone Number (for public-facing use)**
  - Google Voice: https://voice.google.com/about

- **Watch out for Data Breaches**
  - Check to see if any of your emails were part of a data breach: https://haveibeenpwned.com/
  - Set up an alert to see if your emails are part of future data breaches (see "Notify me" tab): https://haveibeenpwned.com/
  - If YES, change password ASAP on that account and never use that password again.

- **Protect your Data from Doxing**
  - **What is it?** Publishing private, sensitive info (home address, cell, SSN#, etc.)**.** Data brokers collect and sell information about you to companies, individuals, or other data brokers, which can facilitate doxing.
    - **HARD, FREE WAY –** opt out of each data broker site manually:
      - Stopdamamining.me: https://www.stopdatamining.me/opt-out-list/
      - Big Ass Data Broker Opt-Out List: fpf.training/databrokers
    - **EASY, PAID WAY:** Pay for a data scrubber subscription:
      - Delete.ME: https://abine.com/deleteme/
      - Privacy Duck: https://www.privacyduck.com/ (discount code: FAMILY)
  - **Google Alerts** - set one up for your name, cell, home address, and any other sensitive info: https://support.google.com/websearch/answer/4815696?hl=en
  - **Remove person info from your professional bios** (partner's name, home city, etc.)

- **DO NOT grant 3rd party apps access to your accounts**
  - **What is it?** Avoid signing into other accounts directly via Google, Facebook, or Twitter and don't allow apps to access your contacts and emails to post as you on your feeds.

- **Separate Personal & Professional Online** -- for more, see PEN: https://bit.ly/2L4x8El

  TIP: Be strategic about which platforms you use for which purposes. If you're using a platform for personal reasons (eg, sharing photos with friends and family), tighten your privacy settings (see links below). If you're using a platform publicly/professionally, you may decide to have the settings set to public – in that case, do not include sensitive personal info and images (family member's names and photos, home address, cell, etc.).
  - Google's Privacy Settings: https://safety.google/privacy/
  - Facebook's Privacy Settings: https://www.facebook.com/settings?tab=privacy
  - Twitter's Privacy Settings: https://twitter.com/settings/safety
  - Instagram's Privacy Settings: https://help.instagram.com/196883487377501
  - LinkedIn's Privacy Settings: https://www.linkedin.com/help/linkedin/answer/66

SPECIFIC Cyber Security Tools & Tips -- PHASE II

- **Be deliberate about granting mobile apps permissions (to contacts, location, etc.)**
  - Google and all kinds of mobile apps are tracking you ALL time. You can turn that off – for more, see Guardian: https://bit.ly/2B7oMtX

- **Encrypted Calls & SMS (for sensitive communication)**
  - Signal: https://signal.org/ - RECOMMENDED
  - Wire: https://wire.com/en/
  - WhatsApp: https://www.whatsapp.com/ - More ubiquitous but less secure than Signal -- owned by Facebook and recently had security breach; still better than no encryption.

- **Encrypted Emails (for international travel or sensitive communications)**
  - For Gmail - get "Mailvelope" extension: https://www.mailvelope.com/en
  - Protonmail: https://protonmail.com/

    Tip: Protonmail is easy to download and use, but if you want to be extra secure, follow the guidelines in "Protonmail like a Pro": https://freedom.press/training/protonmail-pro/

- **Encrypted Browsing (for international travel or insecure internet connections)**
  - Protect your privacy while browsing: VPNs
    - **What is VPN?** A Virtual Private Network lets you access the web safely and privately by routing your connection through servers owned by that service, which can make it appear as if you're browsing from a different location.
      - **Tip #1: NOT ALL VPNs ARE CREATED EQUAL. SOME WILL SELL YOUR DATA, SO ONLY USE TRUSTED VPNs (which cost $$)**
      - **Tip #2: VPNs do not make you anonymous (which requires hiding your IP address). For that, use Tor (see below).**
      - **Recommended VPNs -- see Wirecutter:** https://thewirecutter.com/reviews/best-vpn-service/

  - Browse Anonymously: Tor (The onion router) https://www.torproject.org/
    - **What is Tor?** Tor protects your identity online—namely your IP address—by encrypting your traffic in at least three layers and bouncing it through a chain of volunteer computers around the world, which makes it very difficult for anyone to trace your connection from origin to destination; however, it can be slow to use.
    - **How to use Tor?** https://www.techradar.com/how-to/how-to-protect-your-privacy-online-with-tor-browser

- **Secure Document Exchange:**
  - For individuals: GlobaLeaks https://www.globaleaks.org/
  - For organizations with IT support (more technical): Secure Drop https://securedrop.org/overview/

- DIY Cyber Community

    - Find your people: allies (bigger group via social channels) + rapid response team (smaller group via WhatsApp group, email list, etc.)
        - Friends and family
        - Colleagues
        - Professional Associations
        - Interest/Identity Groups
        - Classmates or Alumni Groups
        - Fans and followers

    - Tell them what's happening: who, when, where, what (screenshots can help)

    - Request support (be clear and specific)
        - *Sample Message: SOS—Publishing an article about reproductive rights today. Last time I wrote on this topic, people doxed my home address and bombarded me with racial slurs. Anyone willing to get on the article's comments section at 12pm EST to set the tone of the thread? Anything constructive and respectful will help!*

- Join Existing Cyber Community: https://iheartmob.org/

- Deploy Allies

    - **CRITICAL FIRST STEPS**
        - Always check in with the target of abuse - acknowledge & offer specific ideas: "I am sorry this is happening to you. I have your back. Would you like me to help you document the abuse you're getting or mobilize others to help you report it?"
        - Assess threat level to yourself as an ally and do cyber security self-check

    - **OPTIONS**
        - Monitor social media channels to give the target break, while documenting and alerting the target to any escalation
        - Block, mute, or document on the target's behalf (need "keys" to their account)
        - Report on the target's behalf
        - Rally a supportive cyber community - or leverage an existing one (like Heartmob)
        - Counterspeech
            - Reclaim negative hashtag attached to the target's name by using that hashtag to spread positive messages
            - Denounce hate and toxic behavior
            - Leverage position of influence, privilege, or power to fact-check a false claim
        - Chime in on a conversation thread right away – if the initial comments are civil and polite, ensuing comments are often less abusive

REMEMBER: Counterspeech can be profoundly empowering and does not have to involve directly communicating with an abuser, BUT: 1) keep in mind that the abuse can escalate and 2) resist engaging in online harassment yourself - not only are you then contributing to the wider problem, but it could have a negative impact on present or future professional opportunities.