digital defense fund

Online Privacy: Controlling Your Data

Last updated 1/20/21

Take care of yourself!

We know digital security can be a scary topic, especially if you've faced online harassment, identity theft, or other online attacks before.

We're here to support you.

Feel free to take a break and remember to drink water, have a snack, and step away if you need to take care of any needs!

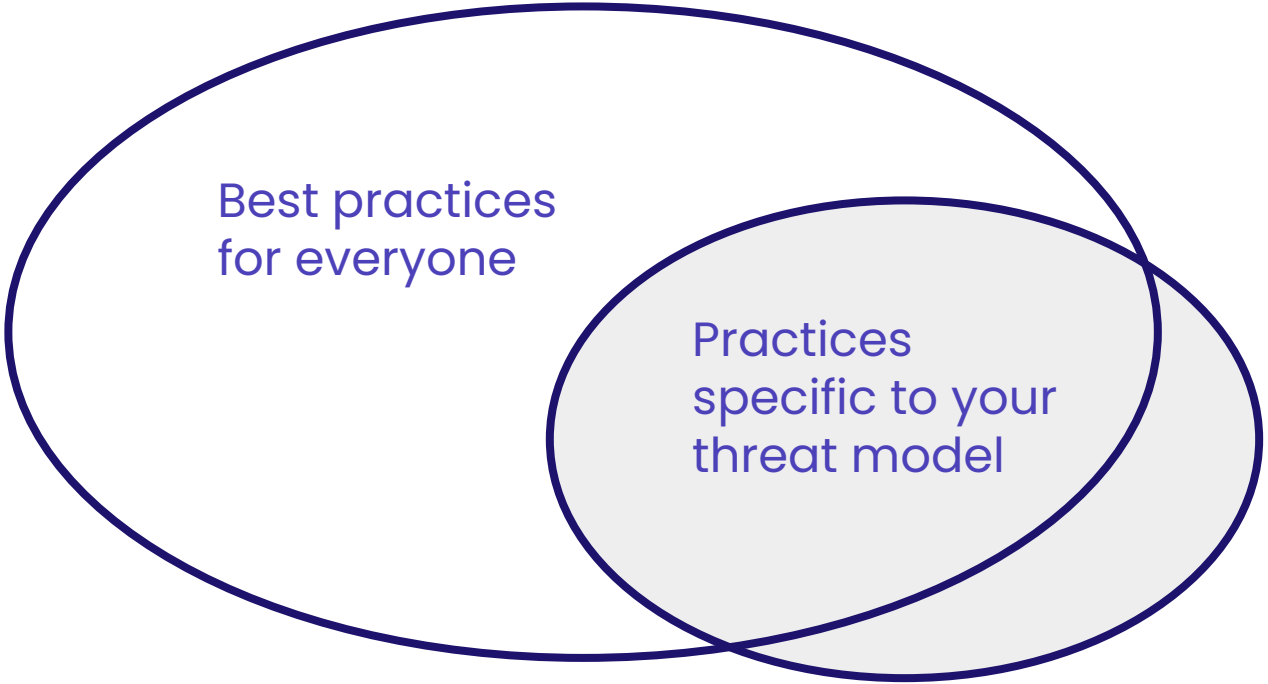
Overview of Common Threats: Privacy & Harassment

Security vs. Privacy

Privacy limits the amount of information about you that people can learn.

Security prevents unauthorized access to your accounts/events.

Threat Modeling: Online Privacy & Doxxing



ddf

Context is key!

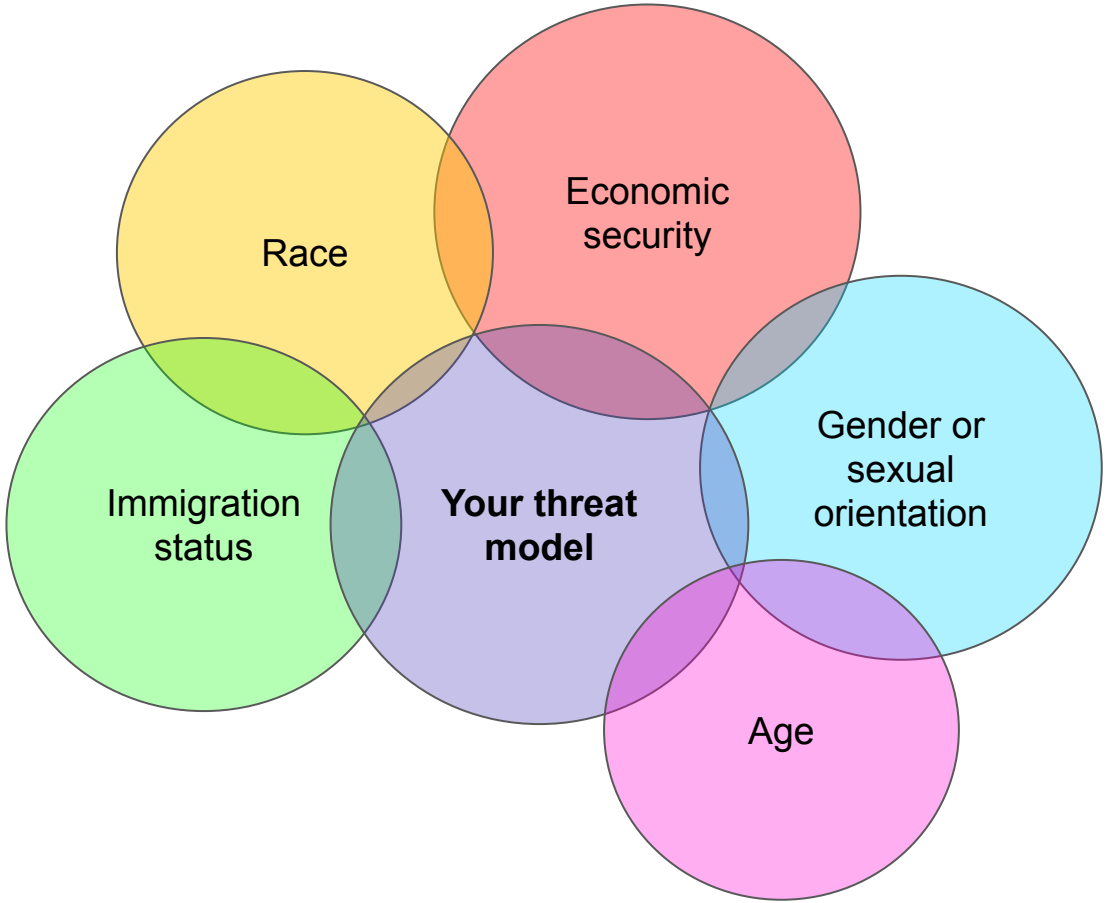
What type of work are you doing?

This affects the type of threat you'll face.

Context is key!

What about your identity affects how you move through the world?

This can affect how severe impact of a threat will be.



Threat modeling helps us ground our fears in reality.

The best way to predict what can happen is by looking at what has happened in the past.

Threat Modeling: Online Harassment

Paths of Escalation

- Taking a threat from one level to the next is called escalation
- Note that as the severity of a threat increases, its likelihood usually decreases

Common escalation paths

Common “escalation paths” that attackers can follow:

1. Get an entire group to start harassing you too
2. Taking attack cross-platform
3. Find your password on a breach list, and attempt to use it
4. Find your home address on a people finder site
5. Find other information about you from social media

Paths of Escalation

- Taking a threat from one level to the next is called escalation
- Note that as the severity of a threat increases, its likelihood usually decreases
- **Our best defense is making escalation more difficult**

ddf

Know your doxxing risk: Search yourself!

Think like an attacker: Can you find your private personal info on Google?

- Open an incognito window
- Google “[your name]”
- Google “[your name] + phone number”

Why do we search ourselves?

- See what an attacker could find when they start targeting you
- Start making a list of things to remove from your search results
- Be aware of information that can’t be removed

Solutions: Keeping personal data private

How did people search websites get my address?

- Government records (like property tax records)
- Bought it from websites, apps, and stores (magazine subscriptions, rewards cards, credit cards, travel companies…)
- Scraped it from other people search websites

In some cases, your address will be public record.

- Do you own a home in your name? Property records are public.
- If you are involved with a non-profit or a business, are you one of the principal or registered agents with the Secretary of State or the IRS? This person's name and address are public.
- Did you file to run for office with your home address on public documents?

Know what information is out there!

- If you own property: search your local government's property tax or real estate transaction databases to see what information is attached to your name.
- If you are involved with a nonprofit: check their tax documents on the IRS website and your state's business entity database to see what information is available about you on their paperwork.
- If you have ever owned a website: look up the website registration data at https://lookup.icann.org/ to see if your address, email, or phone are publicly connected to your website.

Totally hiding your address is possible, but not realistic for many of us

In order to completely hide your address from the public, you'd have to:

- Buy your house in a trust
- Consider buying your car in a trust, too
- Always use a different name when ordering delivery
- Set up public utilities with a different name or address
- Have mail & packages delivered to a PO or CRMA box

You can do these things, and we'll talk about where you can learn more! But all is not lost if it's too late or if you don't want to do them.

You can make it harder to find your address by removing it from data aggregator sites!

- Spokeo (remove listing here)
- Whitepages (remove listing here)
- For instructions on removing yourself from additional people listing sites, go to these guides:
  - Abine's https://www.abine.com/optouts.php
  - Michael Bazzell's Extreme Privacy Opt Out Workbook

Remove Your Home Address/Phone Number

- Consider a paid service like DeleteMe or PrivacyDuck that can remove this information for you
- These services cost $150+/year and will take a few weeks to get your information removed

Remember: interrupt escalation!

Even if your address is public record because you bought a home in your own name, for example, it's still worth removing yourself from data aggregator sites.

Some attackers will give up if they can't find your address when they google you. That's a win!!

Protection through state programs

- Many states have Address Confidentiality Programs or laws allowing certain people to have their addresses removed from the voter lists
- These laws and who can qualify vary drastically from state to state
  - Ex: In Oklahoma, district attorneys, assistant district attorneys, and judges all qualify
- If you've had legal issues with domestic violence or stalking before, you likely qualify.

Get an alternate address & phone number.

Address:

- PO Box: USPS mailbox, usually cheapest
- Commercial Mail Receiving Agency box: offered by UPS Store or another private company; more expensive, but gives you a street address you can use on official paperwork

Phone number:

- Google Voice: free, must be connected to a real number
- MySudo: paid app for iOS
- Twilio: buy and manage phone numbers, very affordable

Start Giving Out Fake Information

- When registering or creating a new account, you can often give fake information!
- On consumer websites, you will not get in trouble for giving a fake name, address, or phone number!
  - Try ordering a magazine to your house in a different name. Do you start to get advertisements in that name?
- “Your safety is more of a priority than their consumer data.”

Read the full guide here: https://hackblossom.org/domestic-violence/threats/location.html

Want to learn more about extreme privacy techniques?

Privacy, Security, & OSINT Show: Podcast by Michael Bazzell

Pros: Really thorough podcast & materials about privacy. He's a leading expert on the topic.

Super dense, technical, and extreme tactics - your threat model may not require such extensive work.

Cons: He rarely has women on his show.

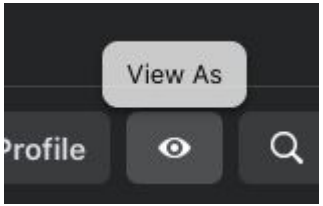
Key takeaway:

Identify what personal information you want to stay private, and take precautions to keep it that way.

Knowing your risks:
Look at your social media as someone else!

Look at your social media as someone else.

- Choose whether you want to look at your Facebook, Instagram, TikTok, or Twitter.
- Go to your chosen account and copy and paste your profile's URL.
- Open an incognito browser window (this window won't be logged into your accounts) and paste your profile URL.
    - For Facebook, go back to your Facebook profile and click the eye icon to "view as" the public
- What can you see?



Solutions: Social media privacy

Make your personal social media accounts as private as possible.

If you haven't already, **create a separation** between your professional social media accounts and your personal social media accounts.

If you use a personal account for both personal and professional activities, consider making a separate personal account (or communicating with friends & loved ones outside of social media!).

Did personal social media accounts show up in your Google search of yourself?

- Make sure your personal social media accounts aren't findable from Google
  - Almost every social platform has a way to hide your profile from search results.
- If you have professional social media: you may want to consider making sure your professional social media accounts *are* discoverable through Google searches, so that result pops up high on the results page.

Were any of your locations visible?

- Be mindful and careful with location sharing when you share posts
  - Could someone identify part of your routine (i.e. a coffee shop you frequent)?
  - Could someone identify where you live?
    - Your neighborhood?
- Consider saving photos to post later
  - Once you're home from vacation
  - Once you've left the event

Did you see an option to send yourself a message?

- Limit who can contact you on your personal social media
  - Consider only allowing friends or connections to send you messages

Platform Specific Privacy instructions

Facebook	https://digitaldefensefund.org/2019/05/03/privacy-and-security-on-facebook/
LinkedIn	https://digitaldefensefund.org/2019/05/20/privacy-and-security-on-linkedin/
Twitter	https://digitaldefensefund.org/2019/05/03/privacy-and-security-on-twitter/
Instagram	https://digitaldefensefund.org/2019/05/03/privacy-and-security-on-instagram/
TikTok	https://www.tiktok.com/safety/resources/safety-videos

You don’t have to delete social media!

In fact, claiming accounts on all the social media sites can help you prevent or take action against impersonation!

Key takeaway:

Be mindful in your use of social media, and familiarize yourself with the privacy settings available.

Resources

- Speak Up & Stay Safe(r): A Guide to Protecting Yourself From Online Harassment
- A DIY Guide to Feminist Cybersecurity
- Big Ass Data Broker Opt-Out List
- Surveillance Self-Defense Guide
- OnlineSOS