Privacy Hygiene

Small tips and tricks to make your data more your own, on a corporate internet.

Contents

1) So What's The Problem?
2) Google Yourself!
3) Accessorize your browser
4) Alias
5) Signal!
6) Camera stickers!
7) Spring App Cleaning!

Cypurrsclaimer (Disclaimer)

Expiration: 06/20

Hygiene- Conditions and practices that serve to promote or preserve health.

Digital Hygiene- like brushing your teeth, but with your browsing history

Tip #1- So What's The Problem?

Threat Modeling

"A way of thinking about the sorts of protection you want for your data so you can decide which potential threats you are going to take seriously.

It's impossible to protect against every kind of trick or adversary, so you should concentrate on which people might want your data, what they might want from it, and how they might get it.

Coming up with a set of possible threats you plan to protect against is called threat modeling or assessing your risks."- EFF Surveillance Self-Defense

Tip #1- So What's the Problem?

- "What are you protecting?"
  "Who are you protecting it from?"
- "What resources do they have to take it from you?"
- "What are you willing to do to protect it?"
- "What vulnerabilities do you need to fill to better protect it?"
- or
- the Bar Test!

Tip #1- So What's The Problem?

- "Bar Test" Could Include:

- Friends
- Foes
- Corporations
- State Actors
- Yourself!

- ...take the test!

Tip #2- Google Yourself

- Things You Can Google
  - Name
  - Phone Number
  - Email
  - Social Security
  - Reverse Image Search

- **Notes**
- You can choose which criteria to search with!
- check out https://myshadow.org/ for more helpful resources on understanding your digital footprint!
- DuckDuckGo is great, Google may be more powerful

Tip #2- Google Yourself

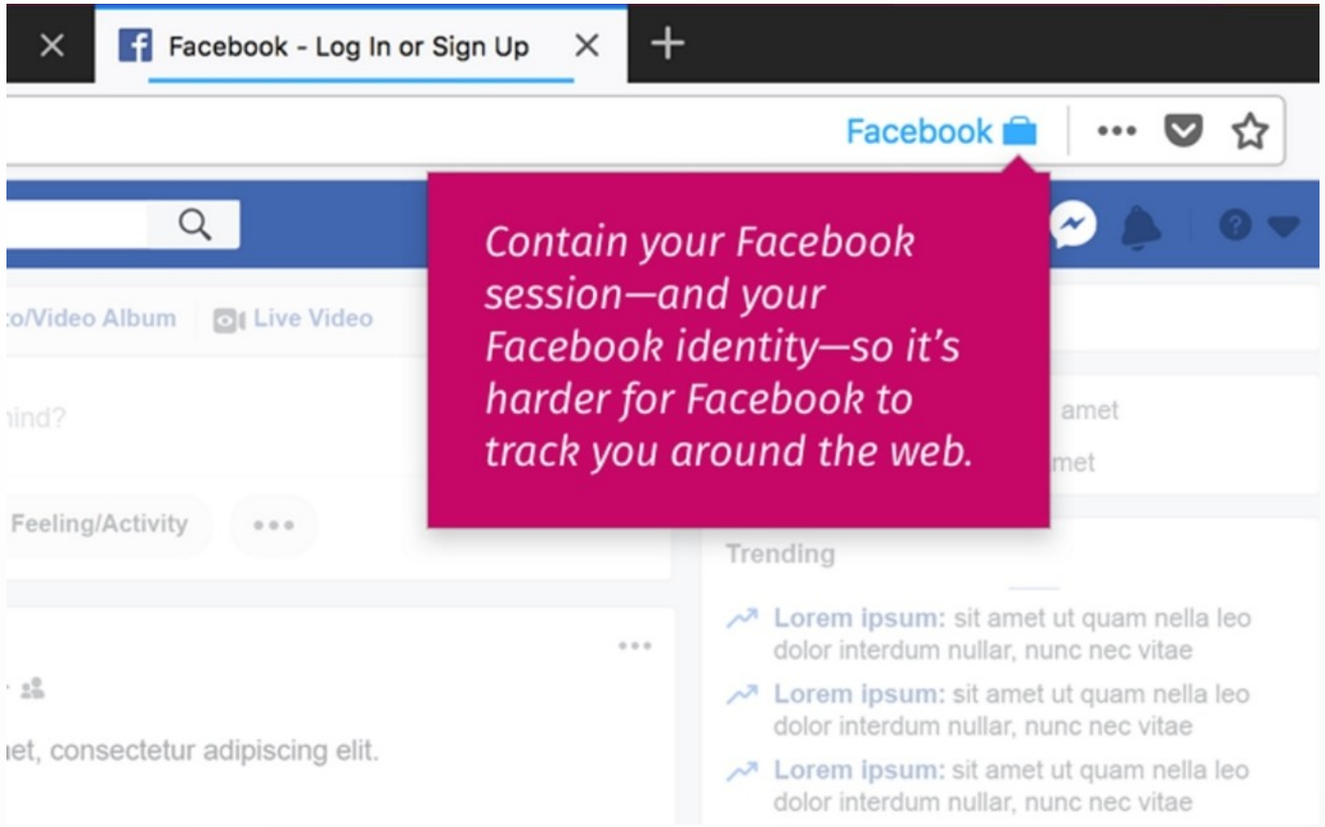
- Data Brokers- Companies that collect, package, and re-sell your information
- Tons of profiles out there with your name, address, birthdate, places you lived, spouses, etc.
- Some regulation on accuracy of info, but mostly state-by-state issue atm (see Vermont and California, maybe NY…?)
- Privacyduck.com
- JustDeleteMe!

Tip #3- Accessorize Your Browser

- Extensions- add onto your browser experience by running processes in the background. These could be pop up blockers, widgets, tools and more.
- Firefox and Chrome users have a bevy of options!

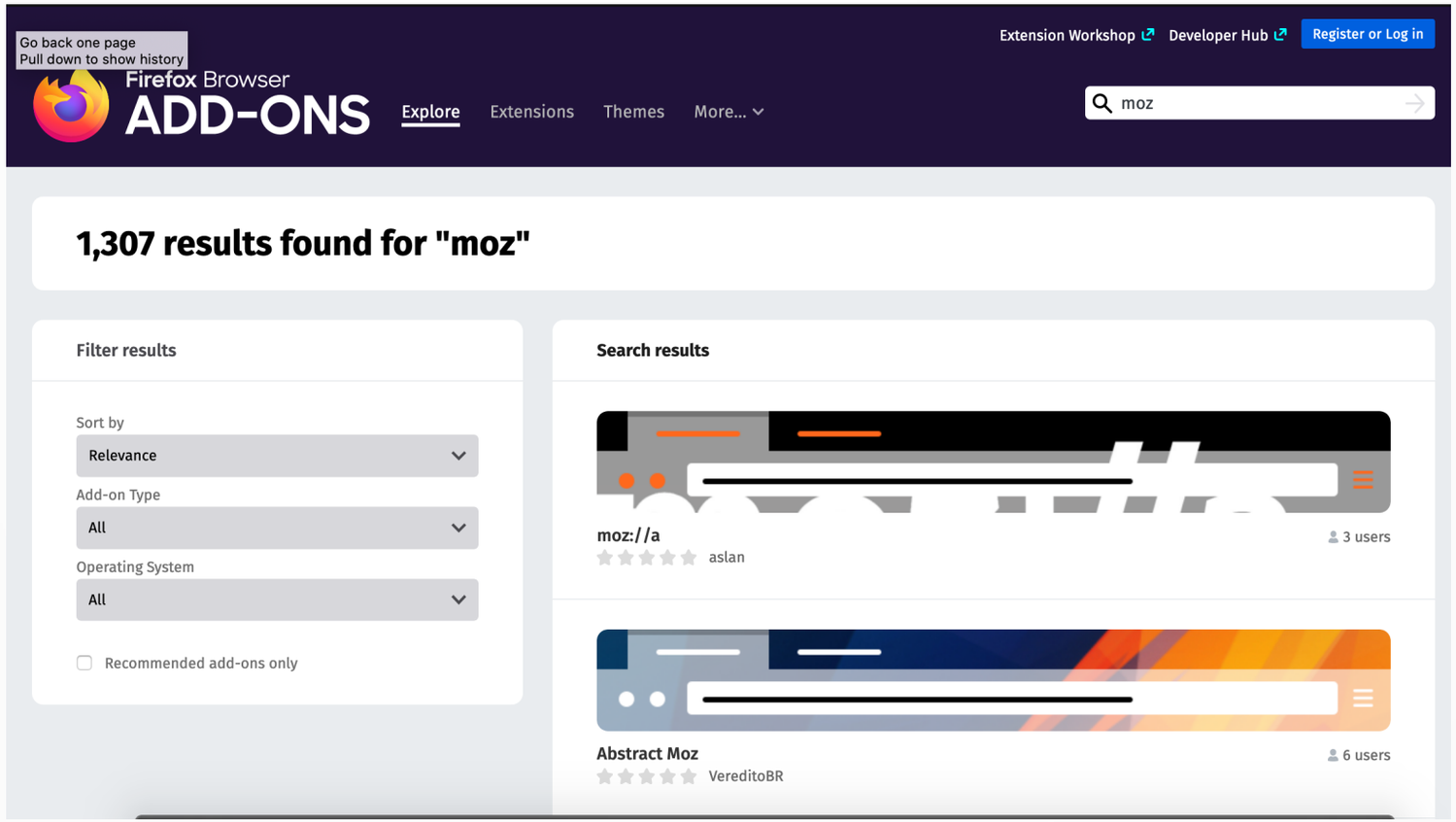
Tip #3- Accessorize Your Browser

- Some more-



Tip #3- Accessorize Your Browser

- Where do I get extensions? Usually through the “Tools” of Firefox or under “Settings” in Chrome



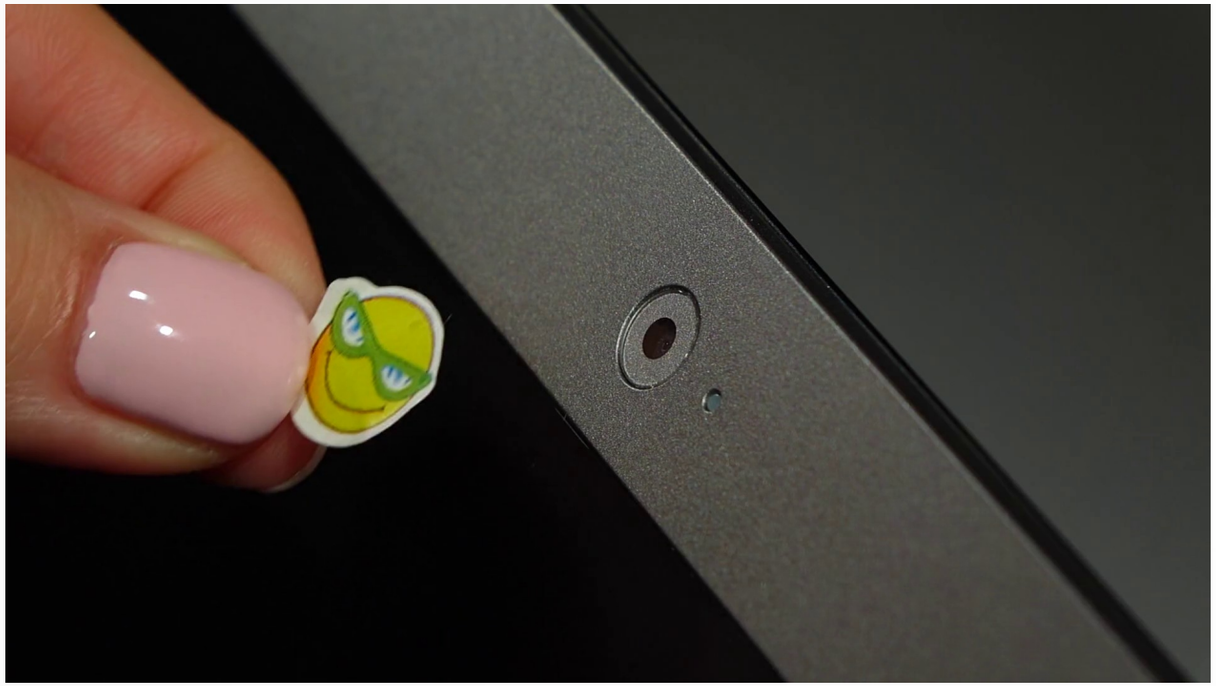
Tip #4- Alias

- Some sites don’t NEED your name/email/phone number
- Some sites you won’t ever come back to.
- Make up a name w/ Random Name Generator!
- Bonus Tip: Keep track of your identities w/ a Password Manager!

Tip #5- Signal

- End-to-end encrypted app
- Open Source, made by Open Whisper Systems
- Great way to send pics/docs to folks; when you don’t want to send through Messenger
- Available for Apple and Android Phones
- Note: only encrypted when sending to
- other Signal users

Tip #6- Camera Stickers

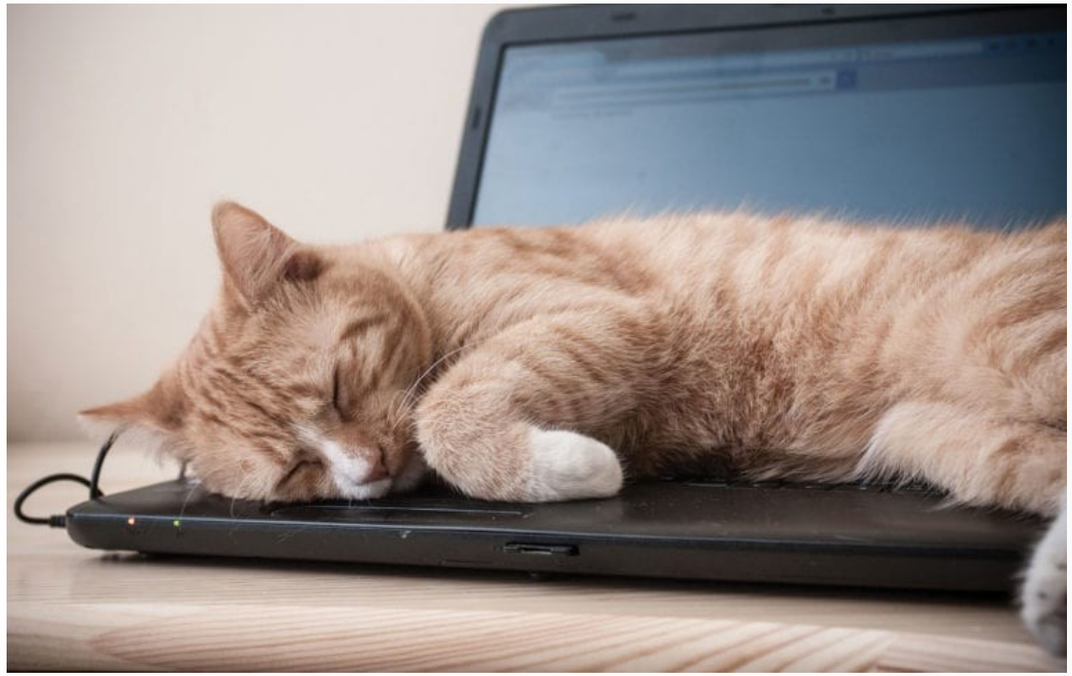


Tip #7- Spring App Cleaning

- What apps do I use a lot?
- What apps don’t I use at all?
- Do I need to have them on my phone?
- For the apps I keep, what permissions have I given them for my phone?

Review

1) So What's The Problem?
2) Google Yourself!
3) Accessorize your browser
4) Alias
5) Signal!
6) Camera stickers!
7) Spring App Cleaning!



Other Resources

- For more privacy and cybersecurity fun, check out:

- EFF Surveilance Self-Defense
- MyShadow.org
- Data Detox Kit