Locking Down Social Media

Good security hygiene is like any other hygienic upkeep of something that involves others: maintaining your own good practices is in a way caring for others, and you should expect the same from them. Communication and consent are a necessary part of any security hygienic regimen.

In the event of an unwanted incident:

1. Notify those in your trusted network.
2. Don’t blame yourself.

Personally Identifiable Information

Sometimes called Sensitive Personal Information.
Any information that can be used to identify a person.

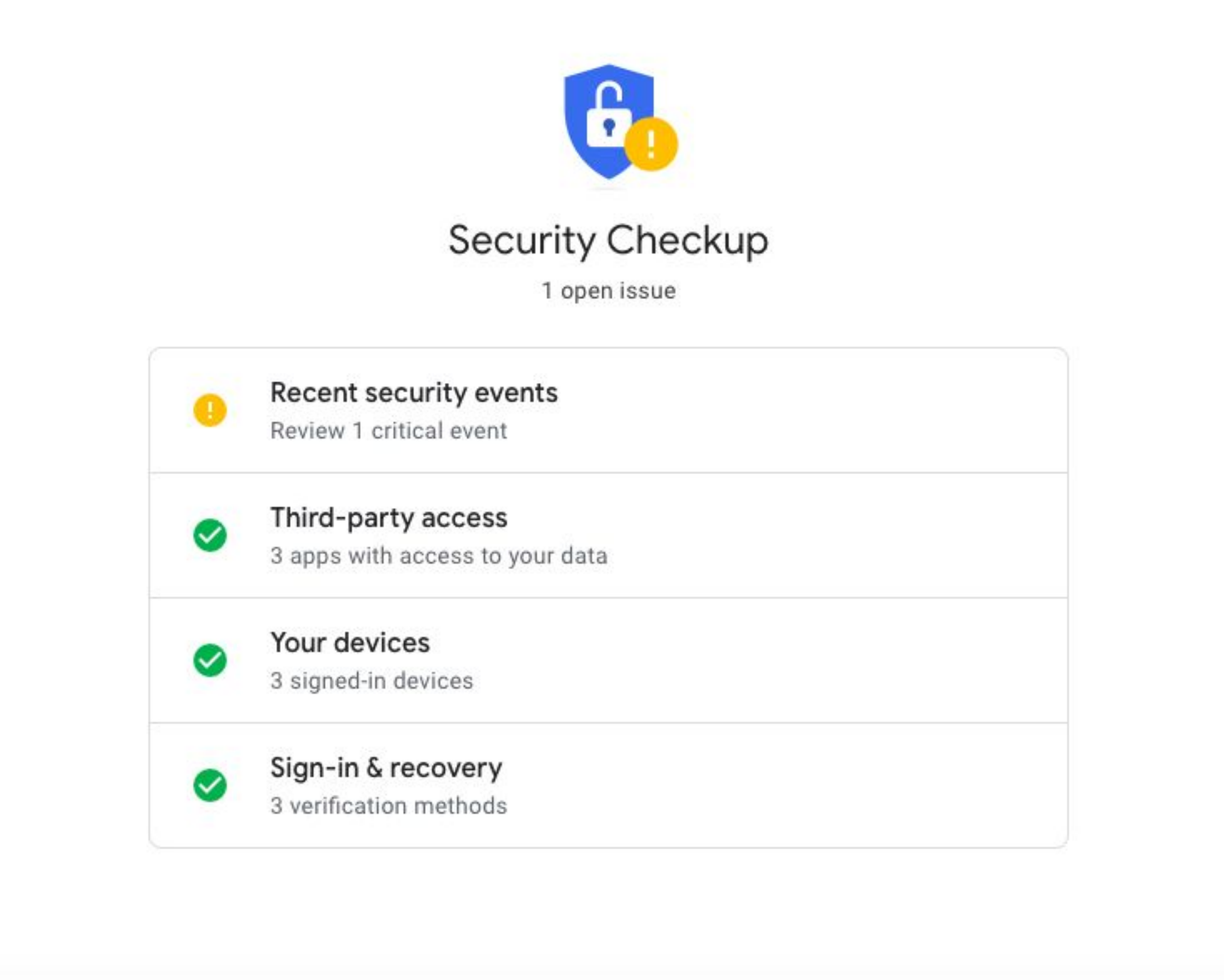
Though individual pieces of information can by themselves seem trivial, when pieced together they may paint a shockingly accurate portrait of a person’s habits, whereabouts, community, and legal information.

Almost all companies rely on at least one piece of PII for registry, and may surreptitiously collect others.

Security Settings

Many major platforms offer “security check-up” features.

- These are tutorial style guides walk you through their privacy and security settings in plain language.



Security Checkup

1 open issue

! **Recent security events**
Review 1 critical event

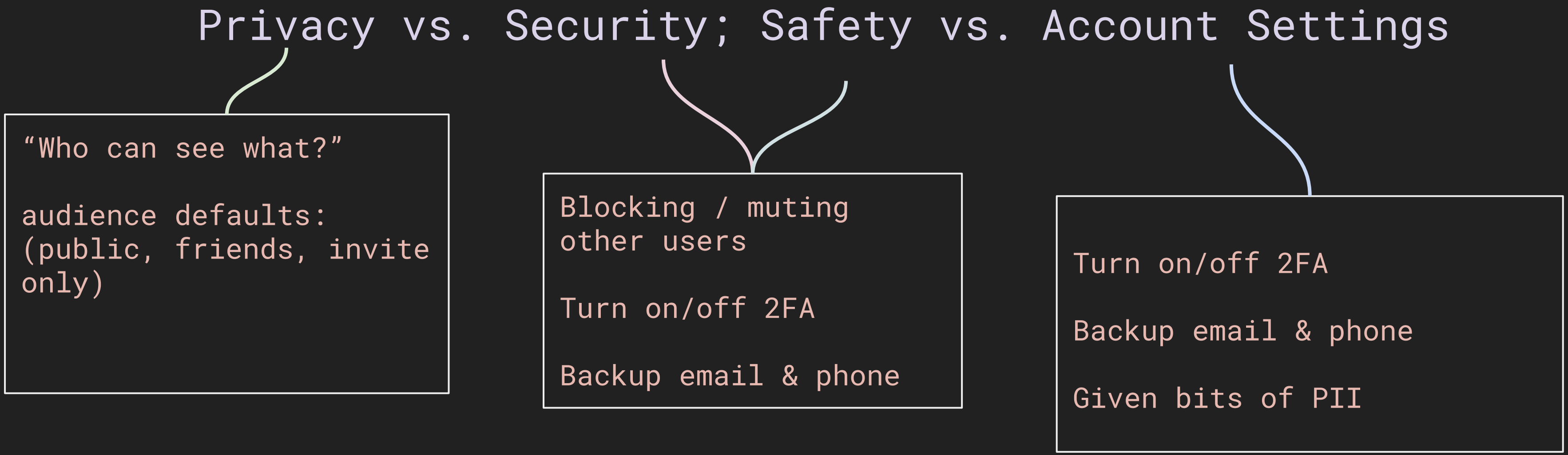
✓ **Third-party access**
3 apps with access to your data

✓ **Your devices**
3 signed-in devices

✓ **Sign-in & recovery**
3 verification methods

Security Settings

Common Settings Patterns



Privacy vs. Security; Safety vs. Account Settings

"Who can see what?"

audience defaults: (public, friends, invite only)

Blocking / muting other users

Turn on/off 2FA

Backup email & phone

Turn on/off 2FA

Backup email & phone

Given bits of PII

Always opt for higher settings.

And even then, raise the bar.

Even with users and infosec specialists advocating for data-collection transparency, it’s in the best interest of these monolithic companies to collect your data, profit off it, and keep you unaware that it’s happening.

Phone Numbers

Do not use for 2FA!

- SMS is not secure
- May reveal more PII than you intended

Only give when necessary

Some platforms will auto-fill your number elsewhere

Your phone number may be public without your knowledge

2FA

Don’t use phone numbers!

Apps like Authy or Google Authenticator

+ : kept local on your phone, generates for many accts

- : must have your phone on you

Yubikey

+ : not trusting another app to generate keysa

_ : if you lose it, you’re locked out

Browser Sessions

Every time you log on is the beginning of a new session.

Depending on the browser, that session may be able to read information from all your previous sessions.

Until you close that browser, everything you do during that session can potentially be associated with each other.

Be mindful of what each session is for.

Location Services

Some apps approximate location metadata by default, not just to tag your posts or content with, sometimes with no clear reason at all.

Android

Go to Settings > Google > Location

Apple

Go to Settings > Privacy > Location Services

Avoid being doxxed by the Algorithm

- Use a VPN
- Use Tor
- Separate browser sessions for logging into different accounts
- Avoid “single sign on” login methods when necessary
- Unique, random, complex passwords for every single account
- Give no more than the bare minimum information to register
  - Does the information even have to be legitimate?
- Keep cross posting to bare minimum
- No shared email addresses, no shared names (or nicknames)