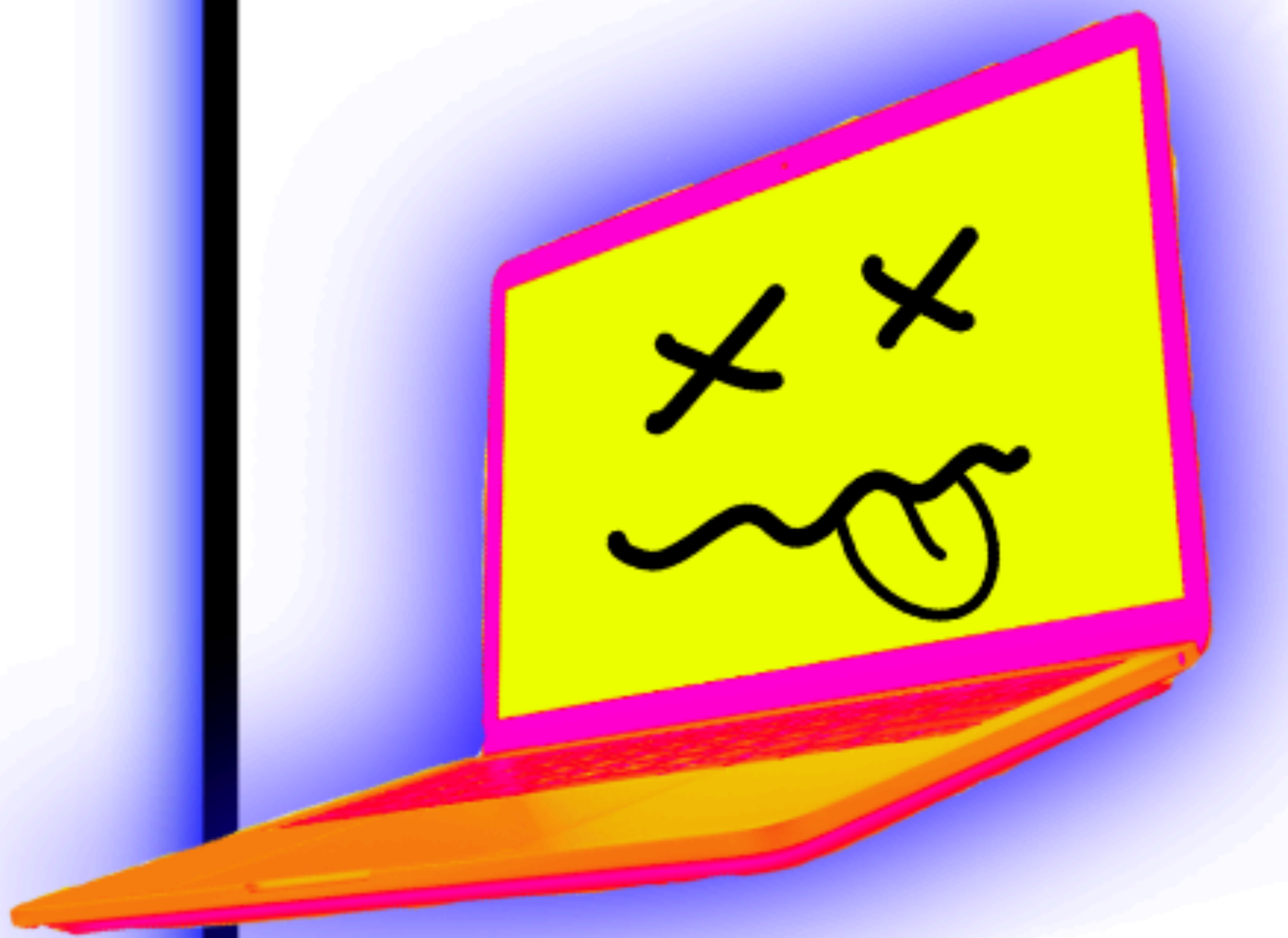
Digital Privacy & Security

Doxxing Prevention



Daly *(she/her)*
daly.barnett@protonmail.com
@ablanathtanalba

Compartmentalization Techniques Slides:

digitaldefensefund.org/ddf-slide-decks/compartmentalization

hackinghustling.org
@hackinghustling

Approaching this from two angles:

Doxxing = maliciously exposing personally identifying information & weaponizing open source intelligence. Leads to further harms.

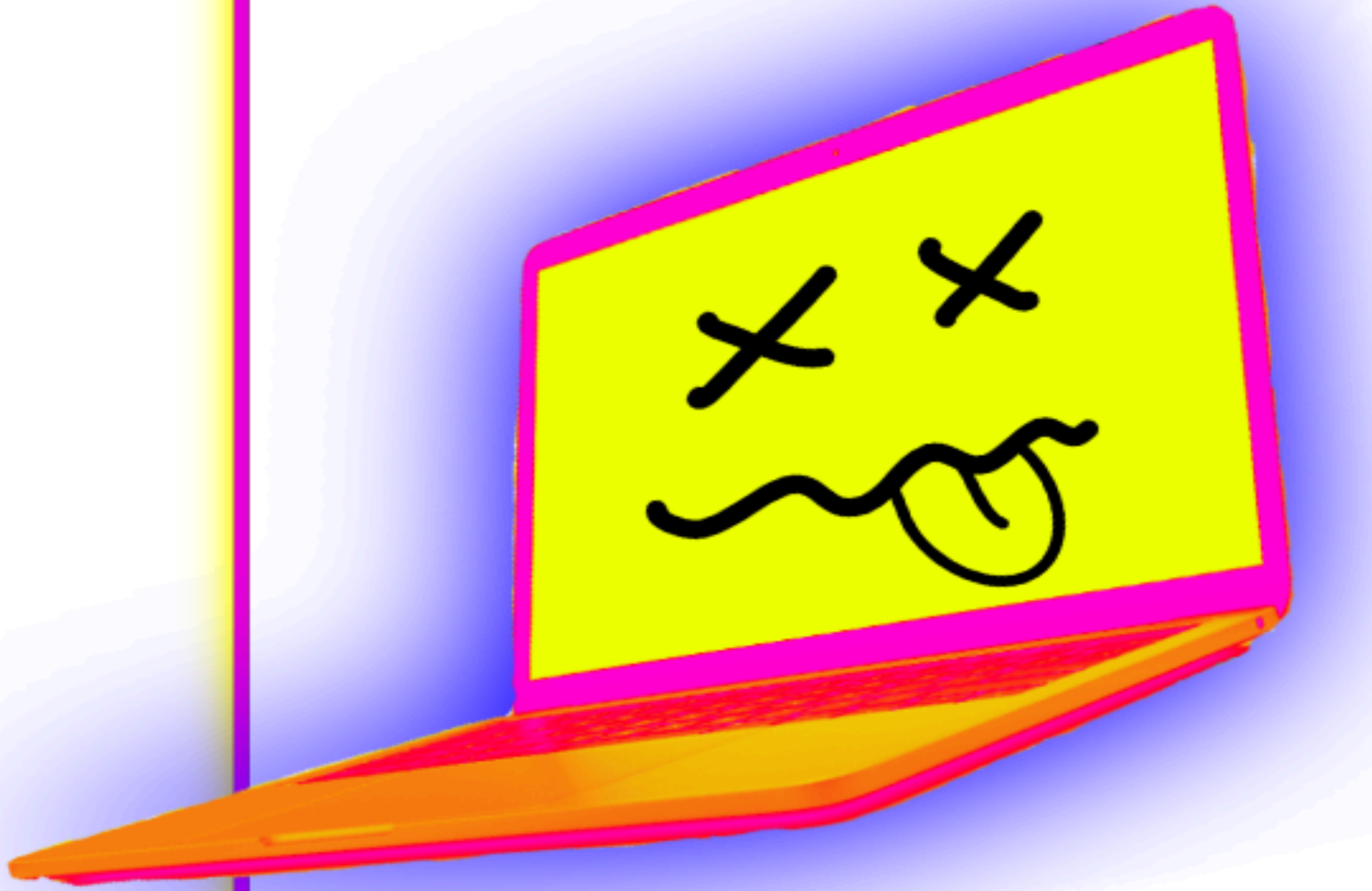
Part 1: Reducing digital footprint, stepping up personal privacy, and introducing chaff & honeypots

Part 2: Incident response, harm reduction, seeking outside support

Dox Yourself

logo
If you can't DOX yourself, how in the hell
you gonna DOX somebody else?

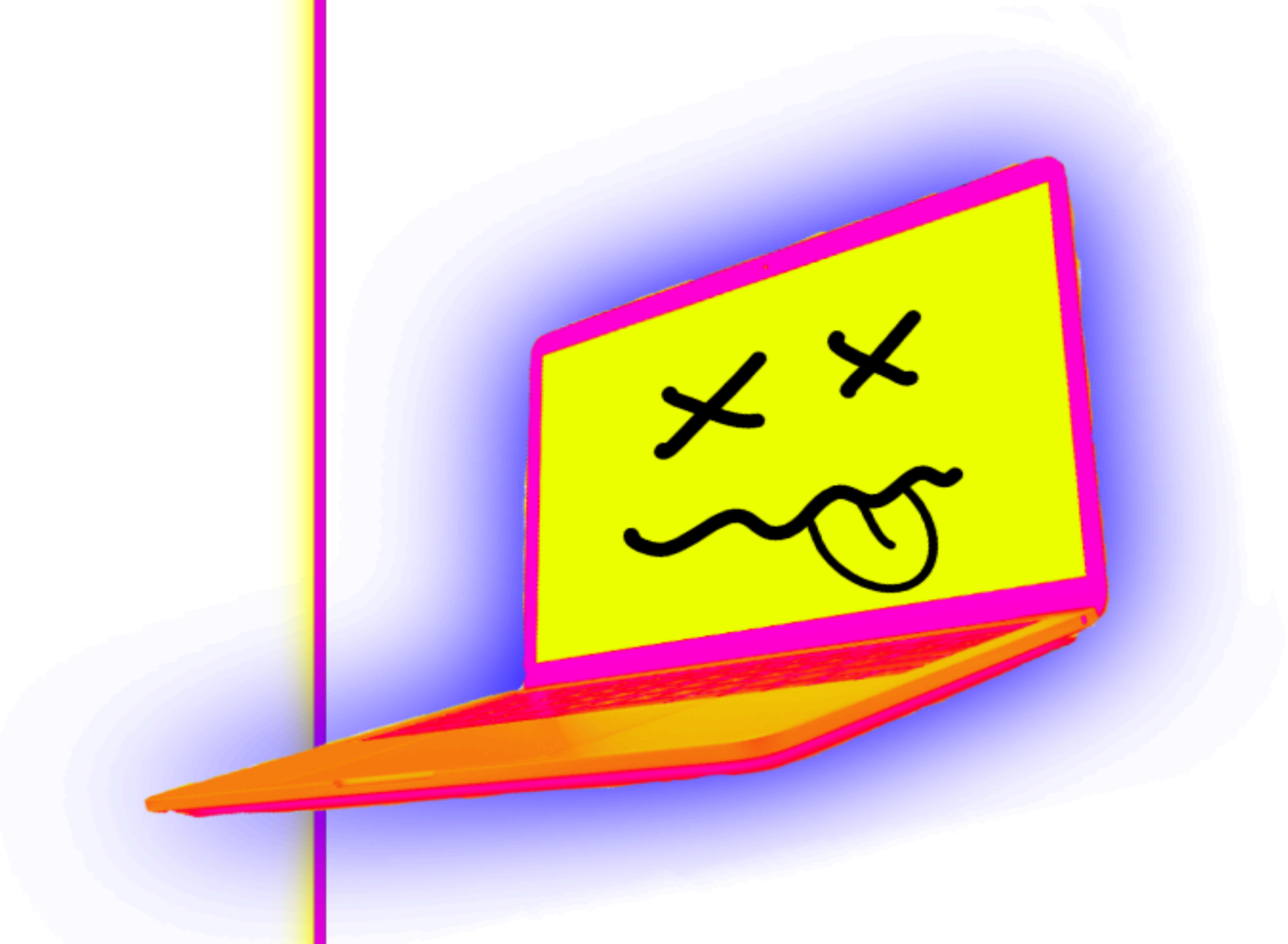
(JK, don't dox anyone else, that's illegal, but the point still stands)



Dox Yourself

Think like an attacker:

- Start where they would: Google
- Then branch out to other search engines and popular sites



Dox Yourself

Google Dorking:

```
site:reddit.com “daly barnett”

site:drive.google.com “daly”

site:docs.google.com “daly”
```

Dox Yourself

Have a business or website?
Dox that too.

WHOIS records

Bizapedia - find your business address

hunter.io - find your business email addresses

opencorporates.com

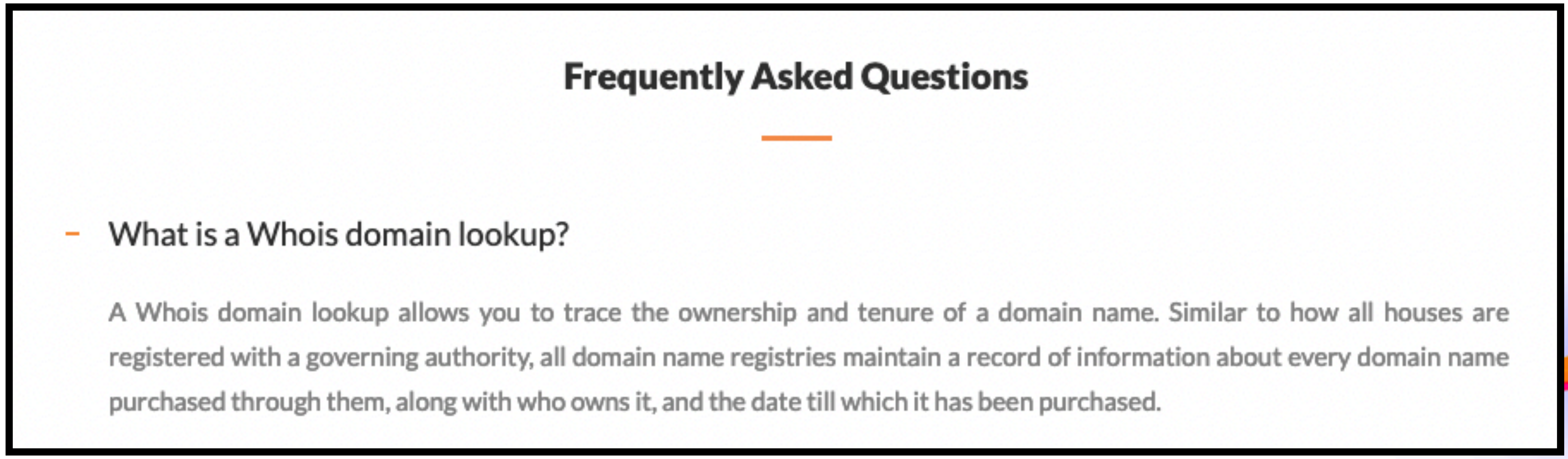
recruitin.net (linkedin search engine)

Dox Yourself

Have a business or website?
Dox that too.

`WHOIS records`

`www.whois.com/whois`



Frequently Asked Questions

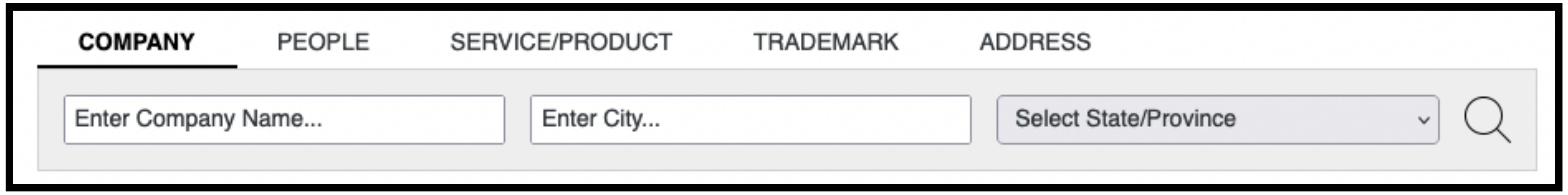
– What is a Whois domain lookup?

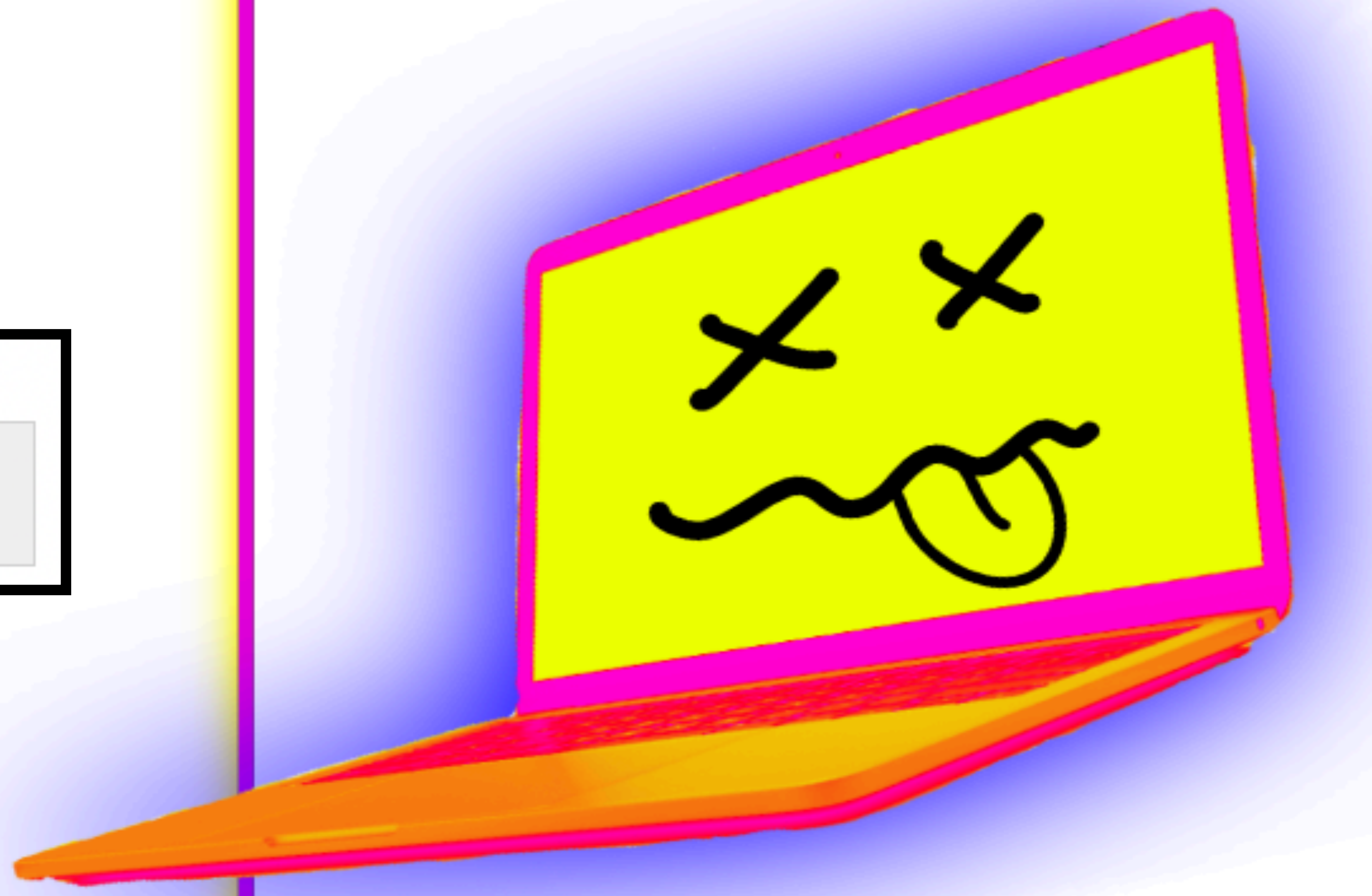
A Whois domain lookup allows you to trace the ownership and tenure of a domain name. Similar to how all houses are registered with a governing authority, all domain name registries maintain a record of information about every domain name purchased through them, along with who owns it, and the date till which it has been purchased.

Dox Yourself

Have a business or website?
Dox that too.

Bizapedia - find your business address

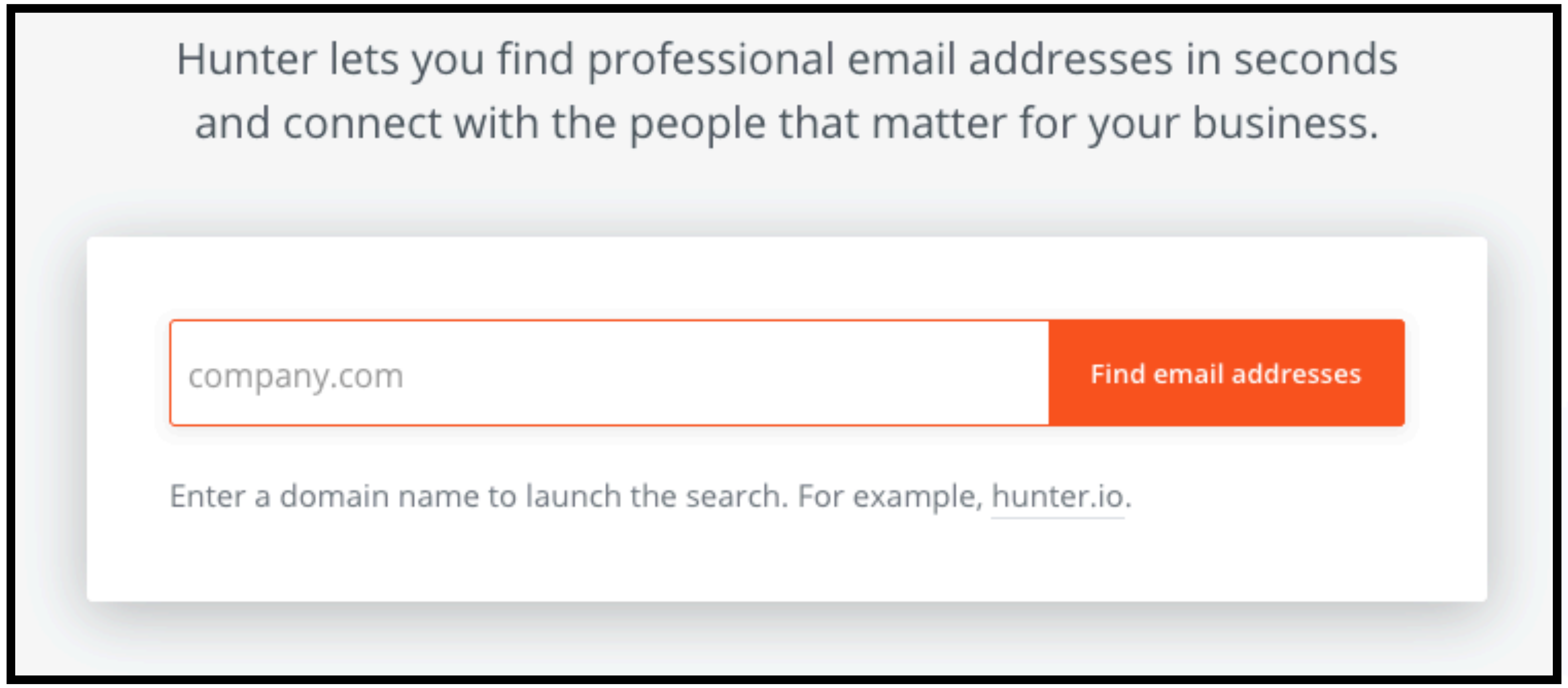




Dox Yourself

Have a business or website?
Dox that too.

hunter.io - find your business email addresses



Hunter lets you find professional email addresses in seconds and connect with the people that matter for your business.

Enter a domain name to launch the search. For example, hunter.io.

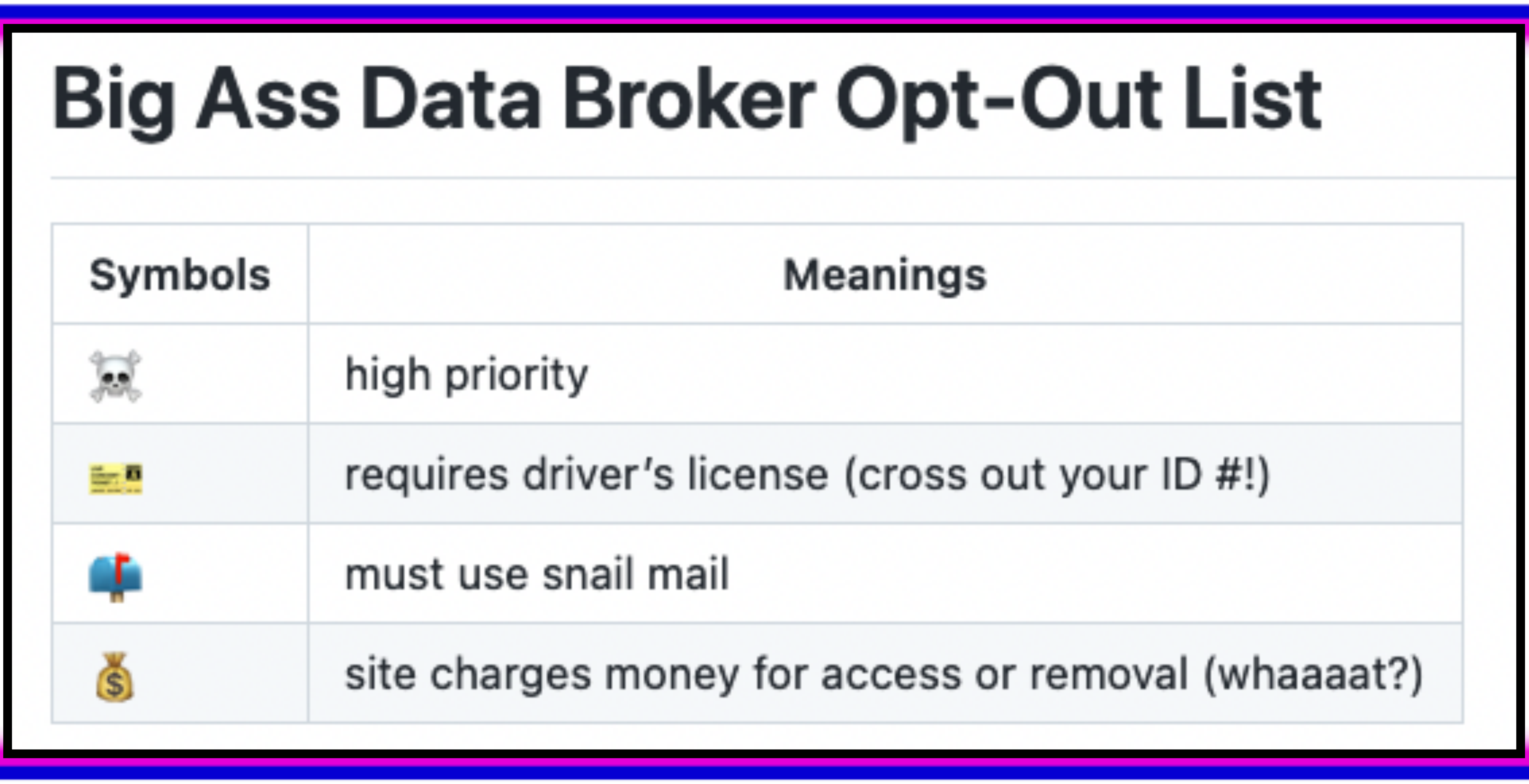
Data Brokers

A creepy, vampiric industry of services that compile, distribute, analyze, and resell personally identifying information on people. Some give information free, but offer data analytics as a premium service to go along with it

They are legally required to give you opt-out options.

Check out Yael's Big Ass Data Broker Opt Out List:

https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List



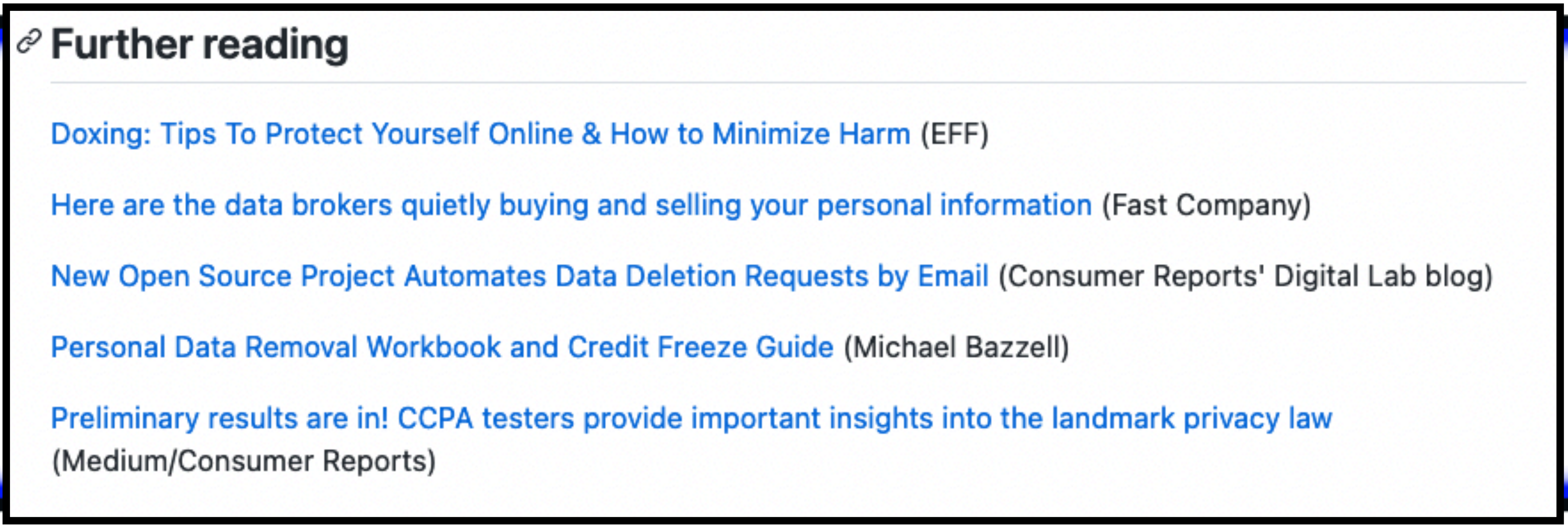
Big Ass Data Broker Opt-Out List

Symbols	Meanings
☠️	high priority
🪪	requires driver's license (cross out your ID #!)
📫	must use snail mail
💰	site charges money for access or removal (whaaaat?)

They are legally required to give you opt-out options.

Check out Yael's Big Ass Data Broker Opt Out List:

https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List



Further reading

Doxing: Tips To Protect Yourself Online & How to Minimize Harm (EFF)

Here are the data brokers quietly buying and selling your personal information (Fast Company)

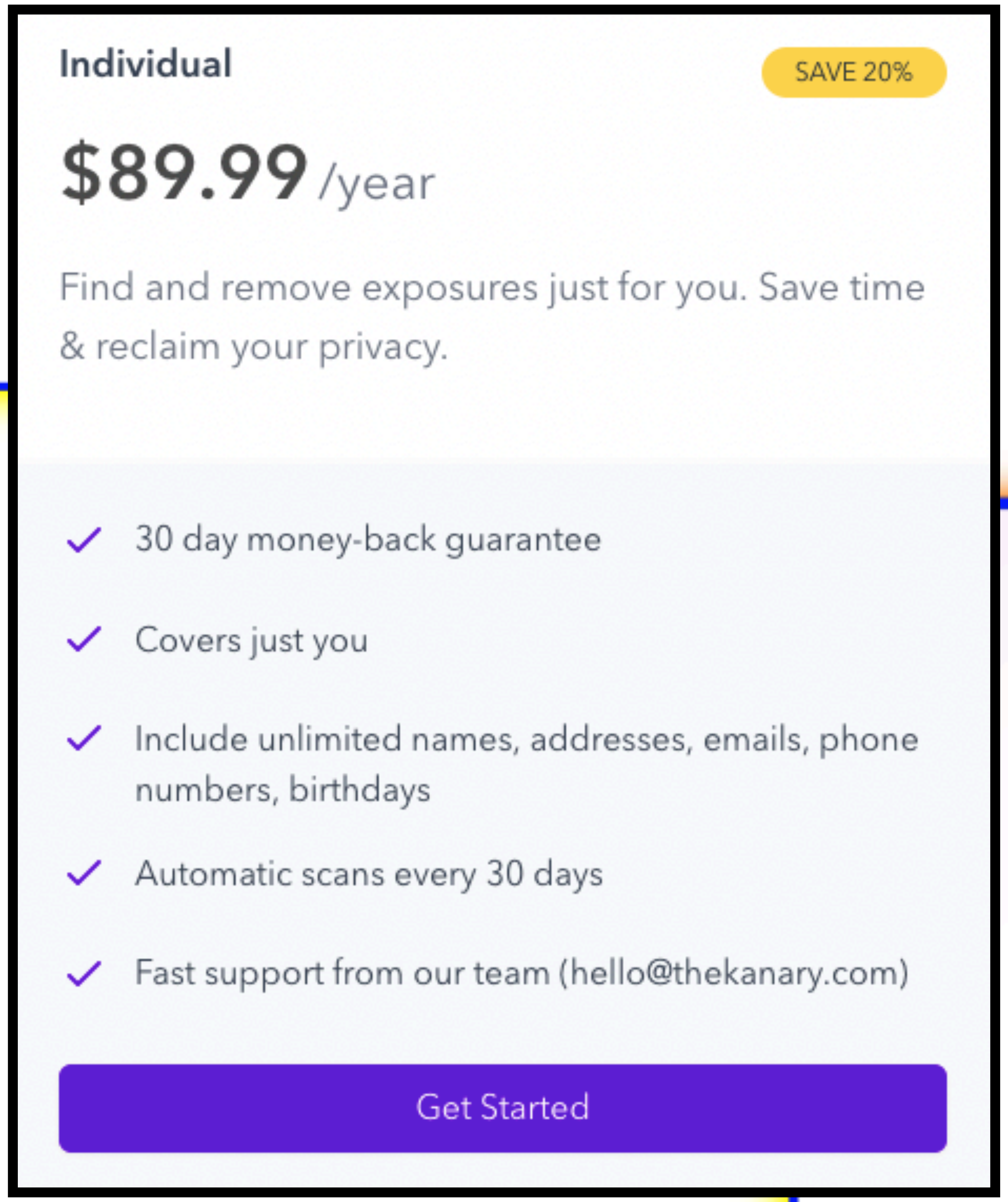
New Open Source Project Automates Data Deletion Requests by Email (Consumer Reports' Digital Lab blog)

Personal Data Removal Workbook and Credit Freeze Guide (Michael Bazzell)

Preliminary results are in! CCPA testers provide important insights into the landmark privacy law (Medium/Consumer Reports)

Paid Services for Deleting Data

kanary



Individual

SAVE 20%

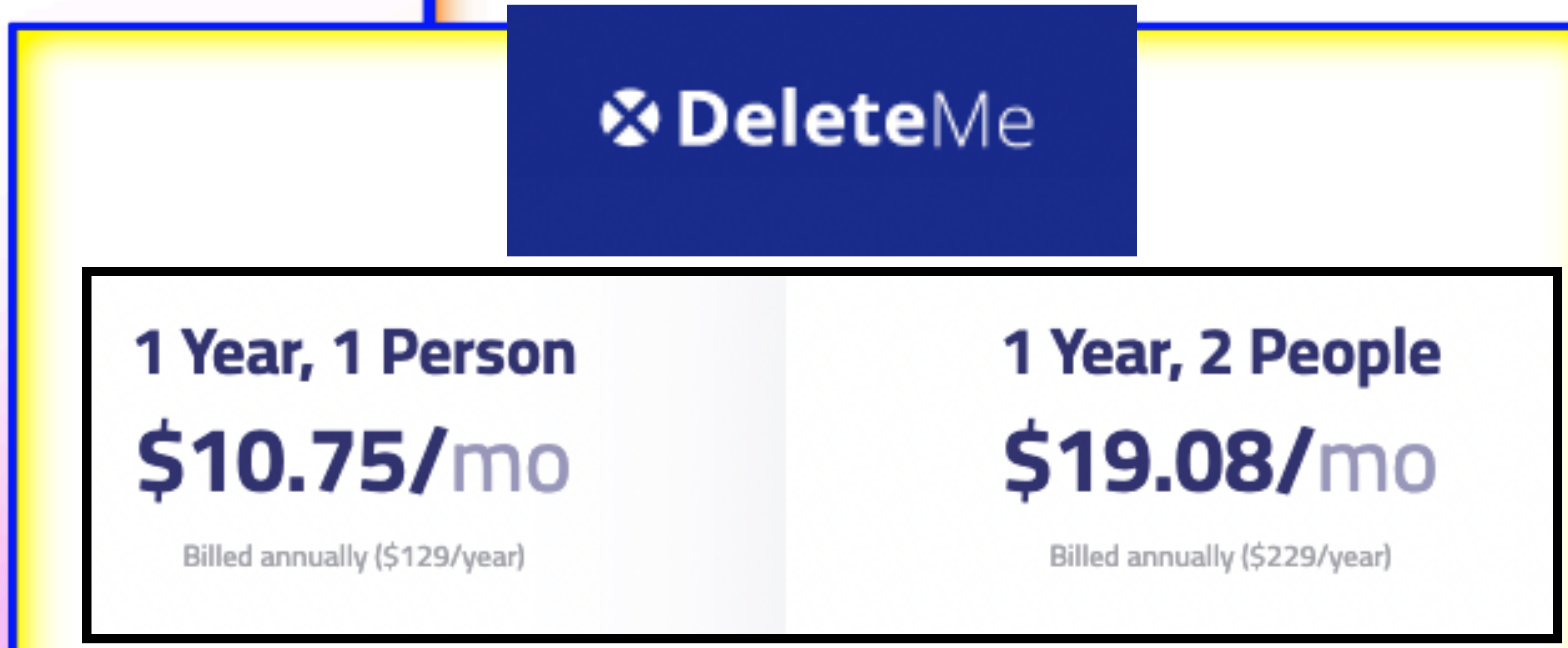
$89.99 /year

Find and remove exposures just for you. Save time & reclaim your privacy.

- ✓ 30 day money-back guarantee
- ✓ Covers just you
- ✓ Include unlimited names, addresses, emails, phone numbers, birthdays
- ✓ Automatic scans every 30 days
- ✓ Fast support from our team (hello@thekanary.com)

These take out the busy-work of doing all the opt-out lists yourself… but it’s expensive. They also do routine check-ups and cover name variations as well.

Paid Services for Deleting Data



DeleteMe

1 Year, 1 Person	1 Year, 2 People
$10.75/mo	$19.08/mo
Billed annually ($129/year)	Billed annually ($229/year)

joindeleteme.com/help/diy-free-opt-out-guide/

These take out the busy-work of doing all the opt-out lists yourself... but it's expensive. They also do routine check-ups and cover name variations as well.

Voter Registration Records

These states make voter records public and available online for free:

Alaska, Arkansas, Colorado, Connecticut, Delaware, Washington DC, Florida, Idaho, Louisiana, Michigan, Mississippi, Nevada, New Jersey, North Carolina, Ohio, Oklahoma, Rhode Island, Utah, Washington

These records often show your full legal name, address, party affiliation, voting history, and more

Remove your listing from:

- voterrecords.com
- blackbookonline.info

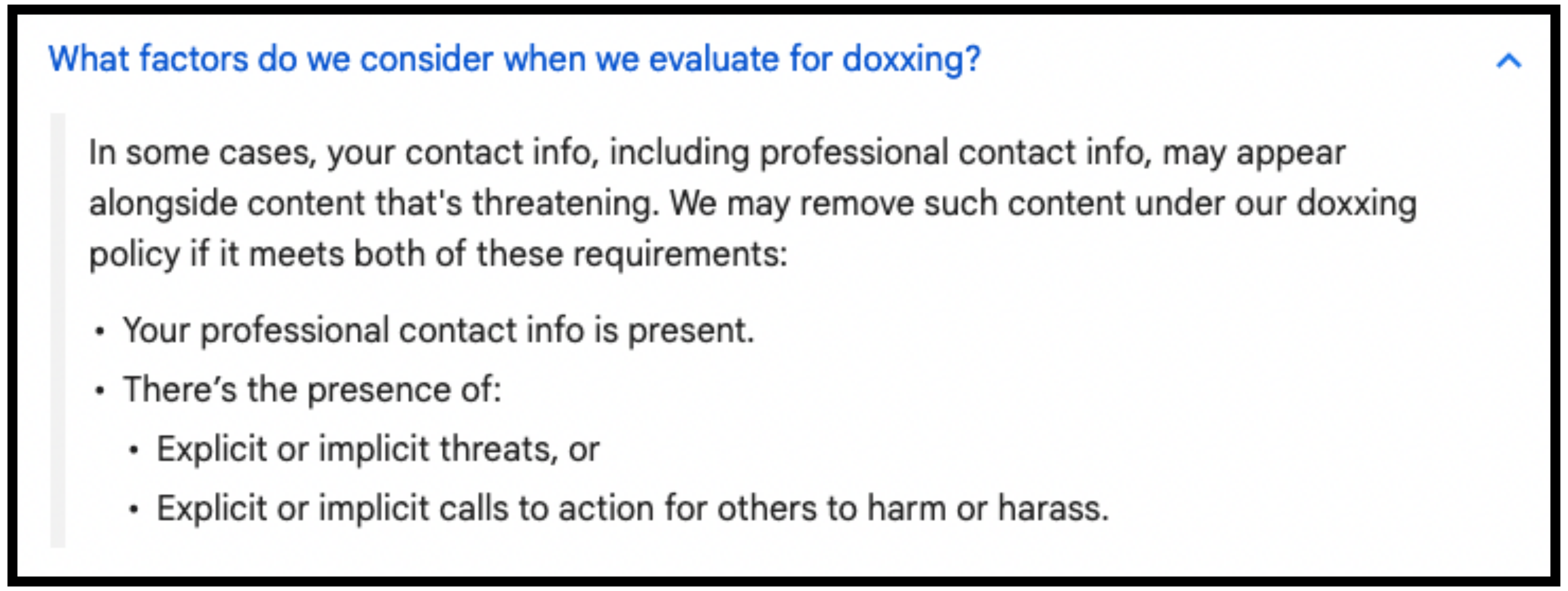
Remove PII from Google

Google takes requests to remove PII from Search results:

Gov ID numbers, Bank account info, credit card info, images of signatures or ID's, medical records, personal contact info, etc.

support.google.com/websearch/answer/9673730

They may also remove professional contact information in event of doxxing:



What factors do we consider when we evaluate for doxxing?

In some cases, your contact info, including professional contact info, may appear alongside content that's threatening. We may remove such content under our doxxing policy if it meets both of these requirements:

- Your professional contact info is present.
- There's the presence of:
  - Explicit or implicit threats, or
  - Explicit or implicit calls to action for others to harm or harass.

Locate all your registered accounts online (social media, email, and other websites)

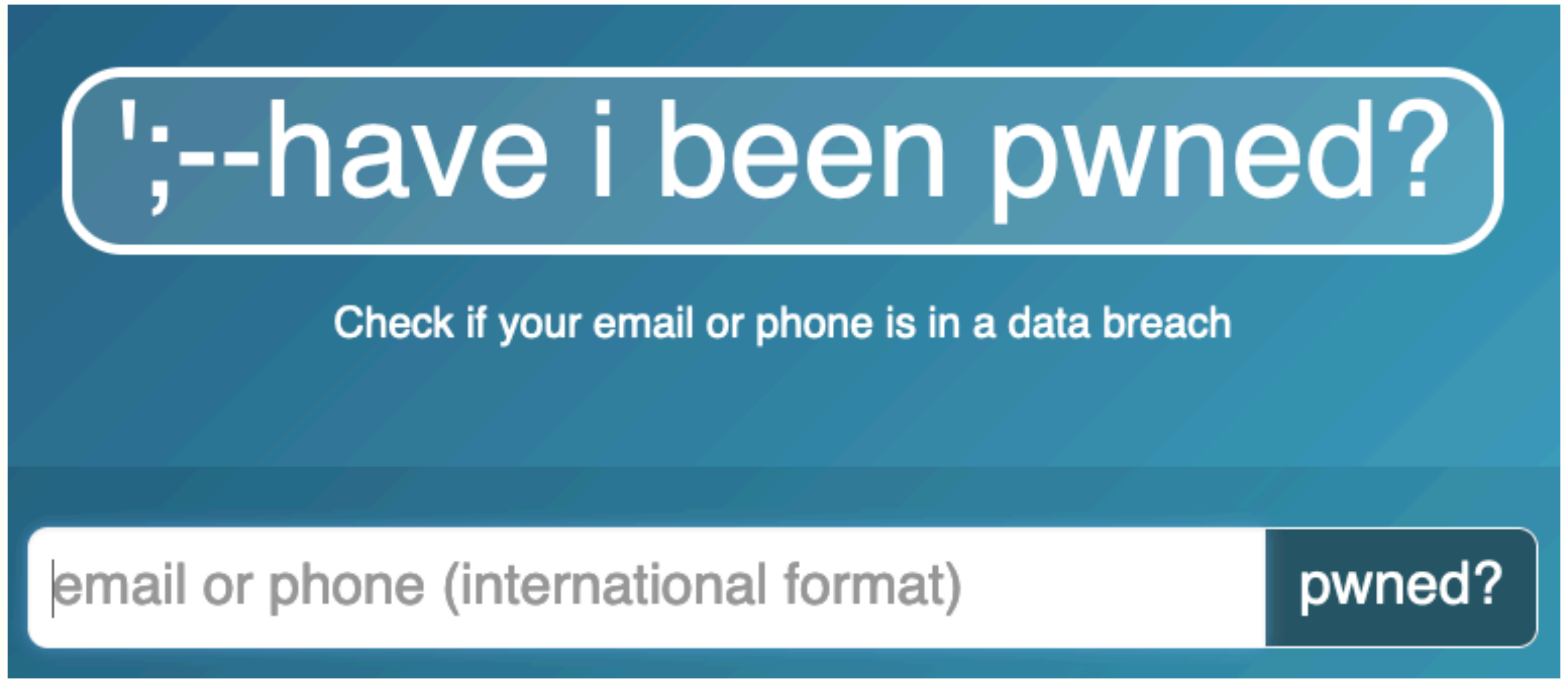
namecheck.com

whatsmyname.app

These are not always comprehensive or entirely correct. Consider working to deactivating the accounts you no longer need

Look for presence of your accounts in any breached databases

haveibeenpwned.com


';--have i been pwned?

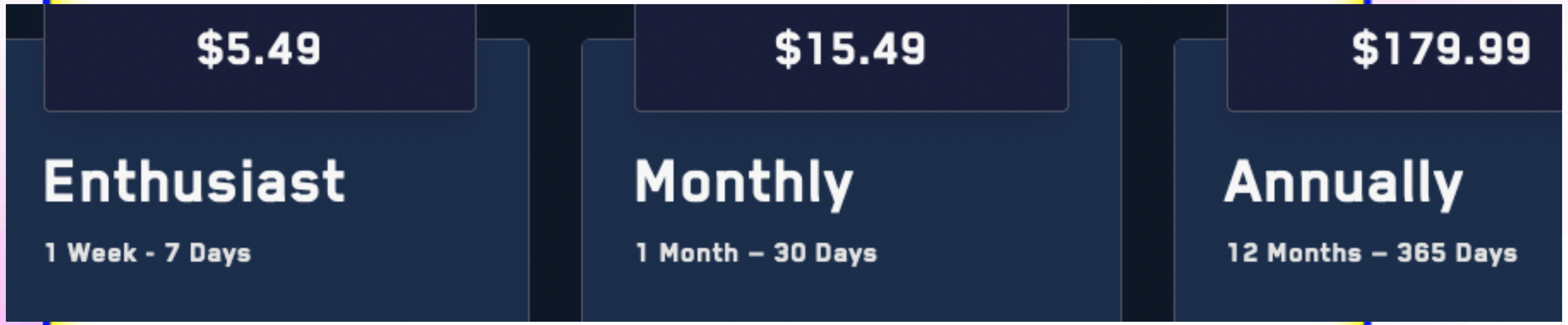
Check if your email or phone is in a data breach

This doesn't mean that your accounts are currently compromised, but it can show you where an attacker might begin.

Consider both the account itself, as well as the email address you registered with.

Look for presence of your accounts in any breached databases

dehashed.com



$5.49

Enthusiast

1 Week - 7 Days

$15.49

Monthly

1 Month – 30 Days

$179.99

Annually

12 Months – 365 Days

This doesn't mean that your accounts are currently compromised, but it can show you where an attacker might begin.

Consider both the account itself, as well as the email address you registered with.

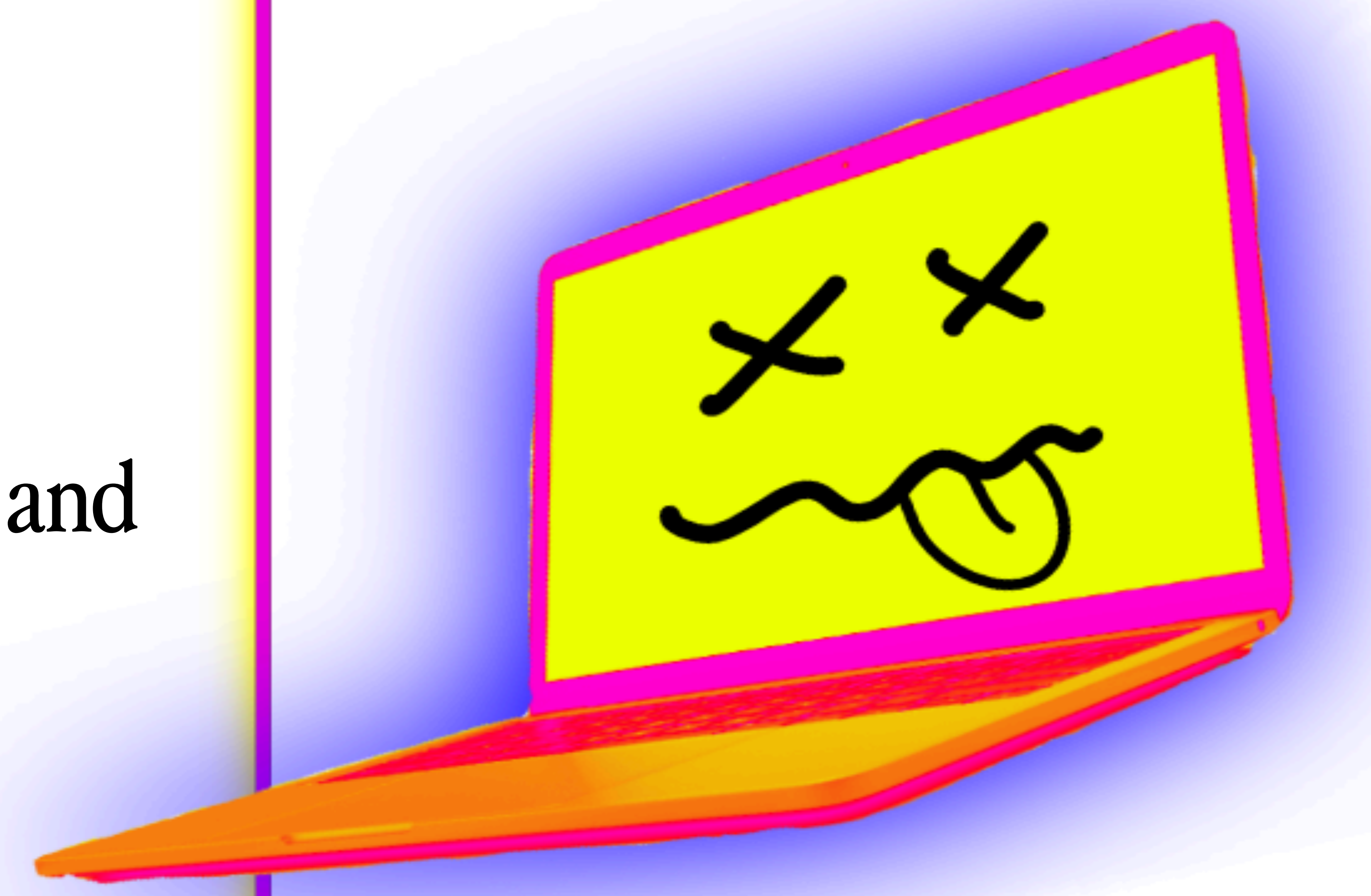
Private Browsing

Choose a browser with hardened privacy (and configure it yourself for even more) for basic needs, like Firefox, Brave, or DuckDuckGo.

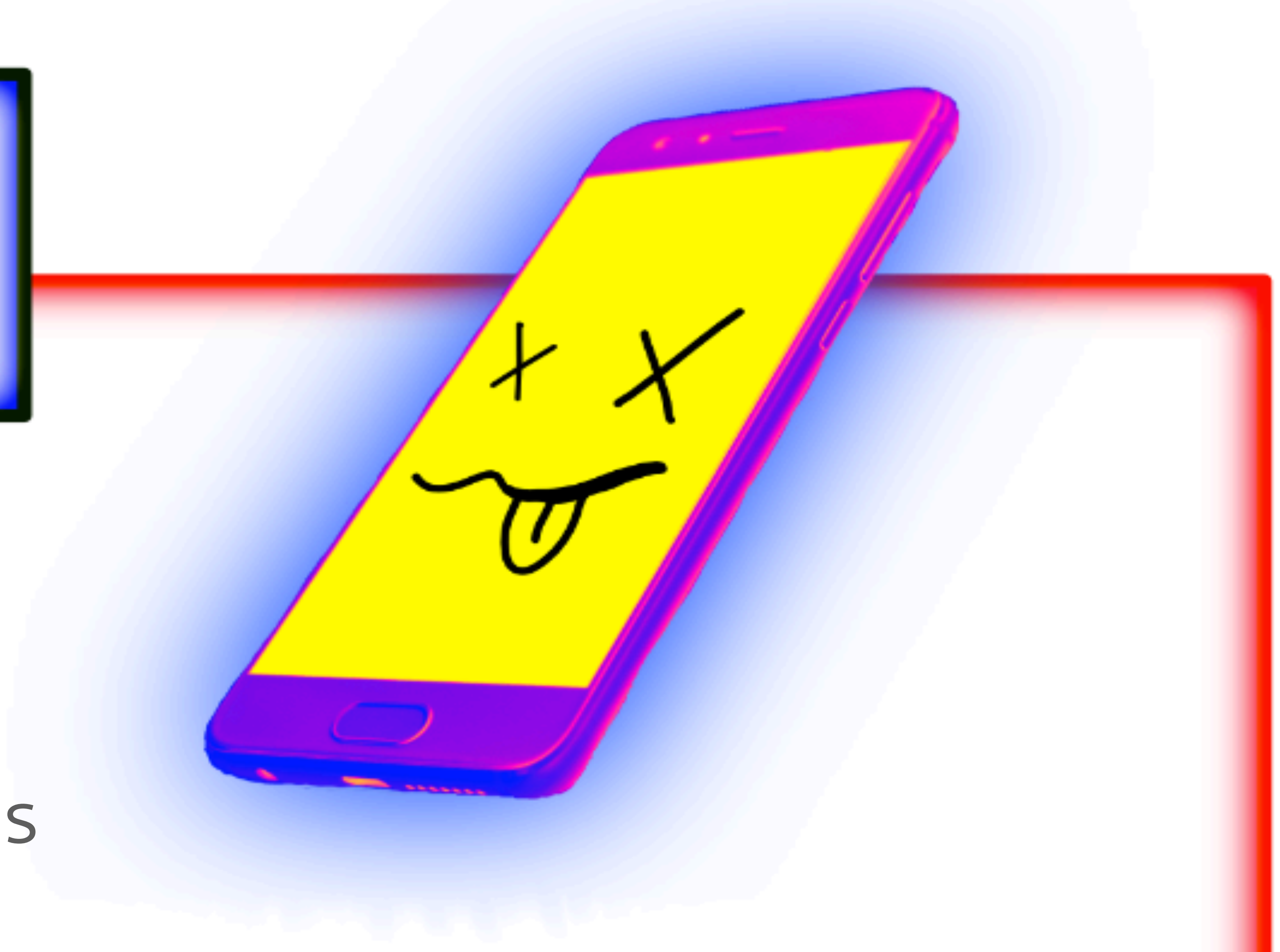
Go for a more intensive option like Tor for more sensitive browsing.

Install Privacy Extensions like uBlockOrigin, Privacy Badger, and DuckDuckGo.

Use a VPN to dissociate your internet traffic from your IP



Locking Down Twitter



Settings > Security & Account Access

Privacy > Audience & Tagging > Protect Your Tweets

Privacy > Data Sharing

Privacy > Discoverability & Contacts

The above flows are how to tighten up privacy & security settings on Twitter.

Definitely turn on multi-factor authentication. Definitely turn off data sharing and discoverability.

Locking your account or turning off "discoverability" is optional, but recommended.

Locking Down Instagram

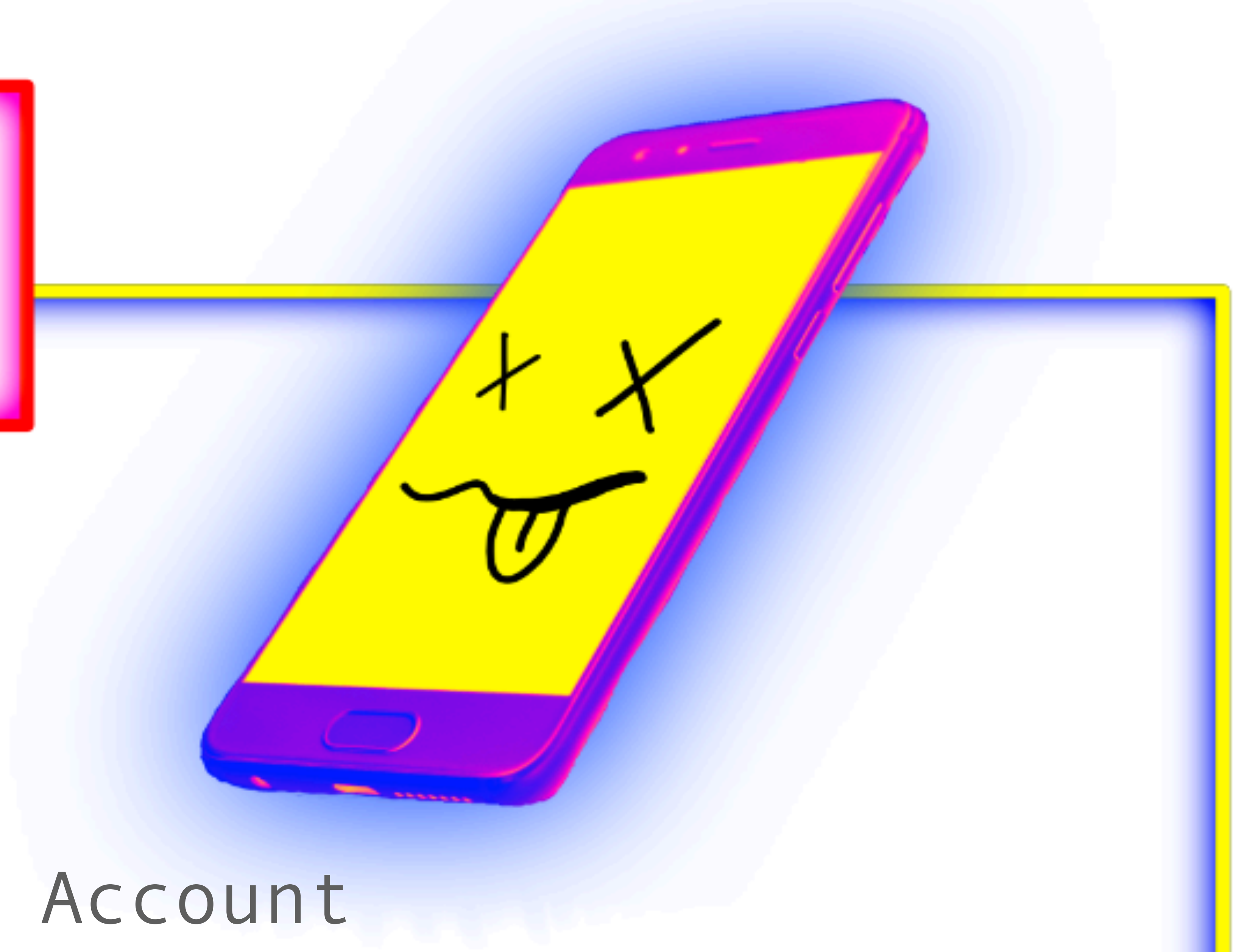
```
Settings > Privacy > Private Account

Settings > Security > Two-Factor Auth
```

The above flows are how to tighten up privacy & security settings on Instagram.

Definitely turn on two-factor authentication.

Making your account private is optional, but highly recommended for non-professional accounts or any accounts that don't rely on publicity or public sharing.

Locking Down TikTok



Profile > Settings & Privacy > Privacy > Private Account

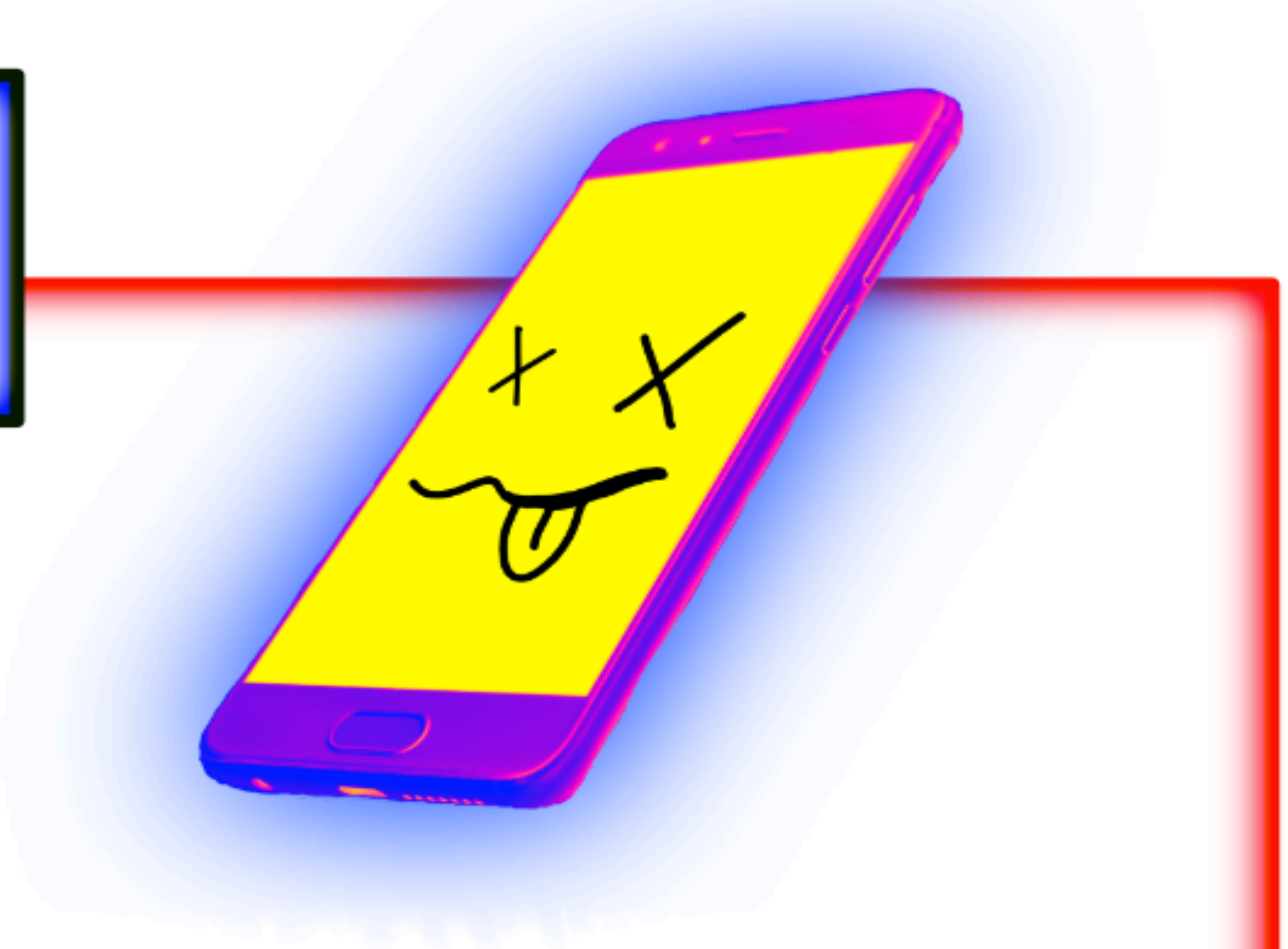
Profile > Settings & Privacy > Privacy > Suggest Your Account to Others

Profile > Sync Contacts & Facebook Friends

Profile > Security & Login > 2-Step verification

Unless your TikTok account is used to promote things very publicly or it can stay word-of-mouth, it is highly recommended that you turn on all of these settings.

Locking Down Venmo



Profile > Settings > Privacy > Private

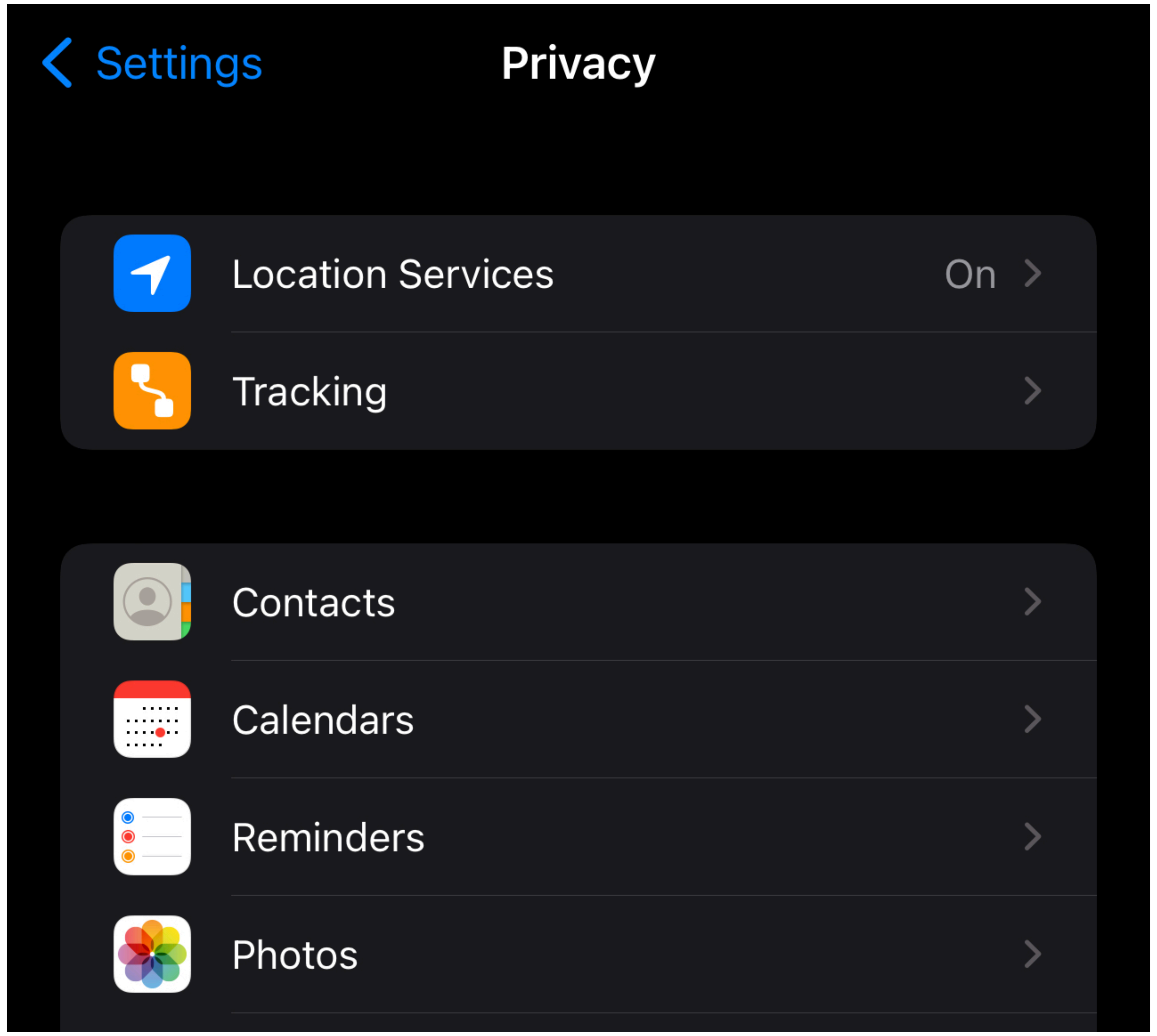
Venmo is neither fun nor social media, for the love of god don't give into it's coercion to use it as such. Make your account private and not discoverable by others.

This goes for other payment apps (that will have nearly identical flows to accessing their privacy features) like Zelle, CashApp, PayPal, etc.

Review App Permissions

iOS

Settings > Privacy



Settings   Privacy

Location Services   On

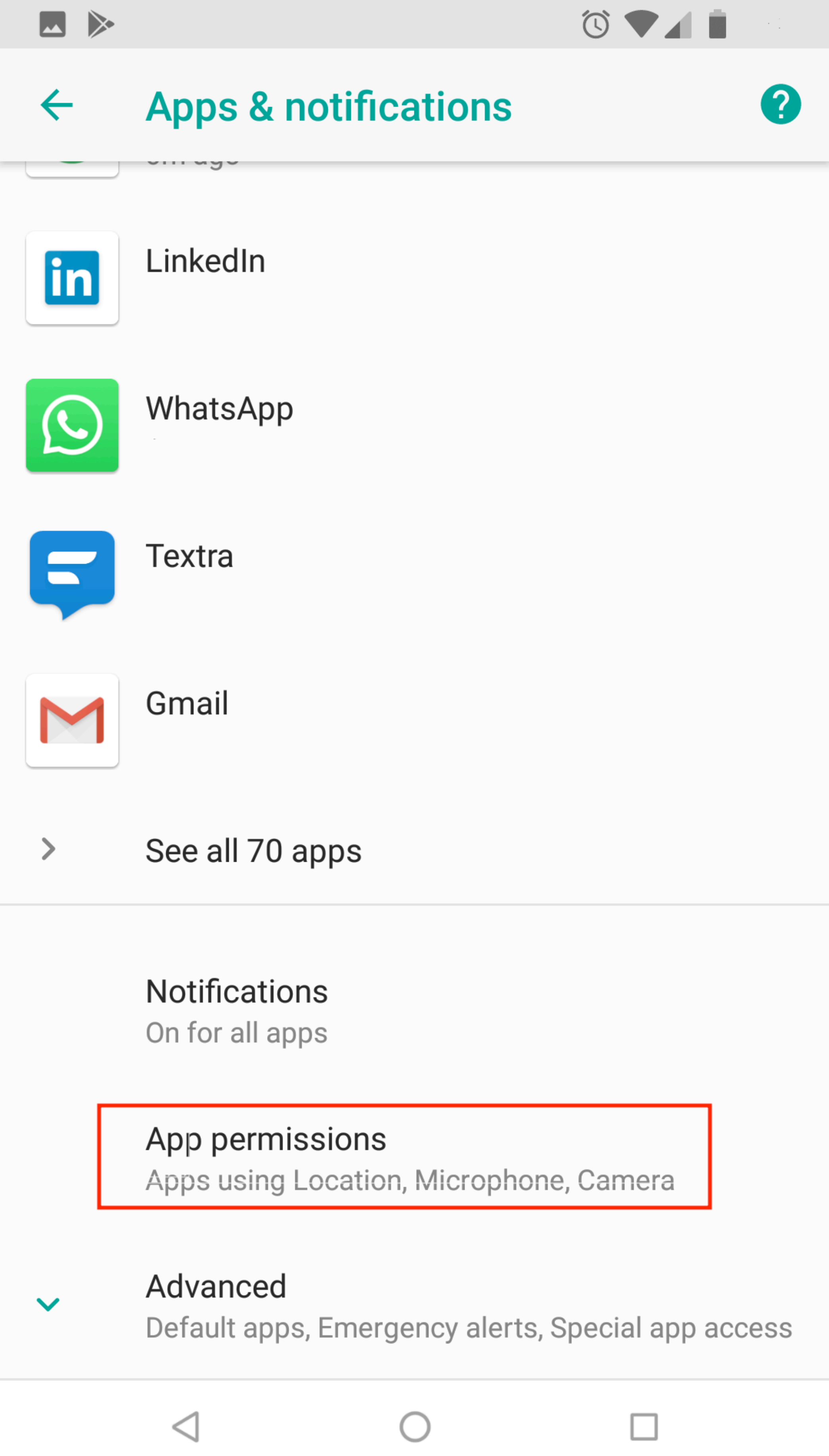
Tracking

Contacts

Calendars

Reminders

Photos



Apps & notifications

LinkedIn

WhatsApp

Textra

Gmail

See all 70 apps

Notifications
On for all apps

App permissions
Apps using Location, Microphone, Camera

Advanced
Default apps, Emergency alerts, Special app access

Android

Settings > Apps

Honey Pots & Chaff

Make a social media account to draw in those looking to stalk or harass you.

Keep it separate from other accounts, but still plausibly you.

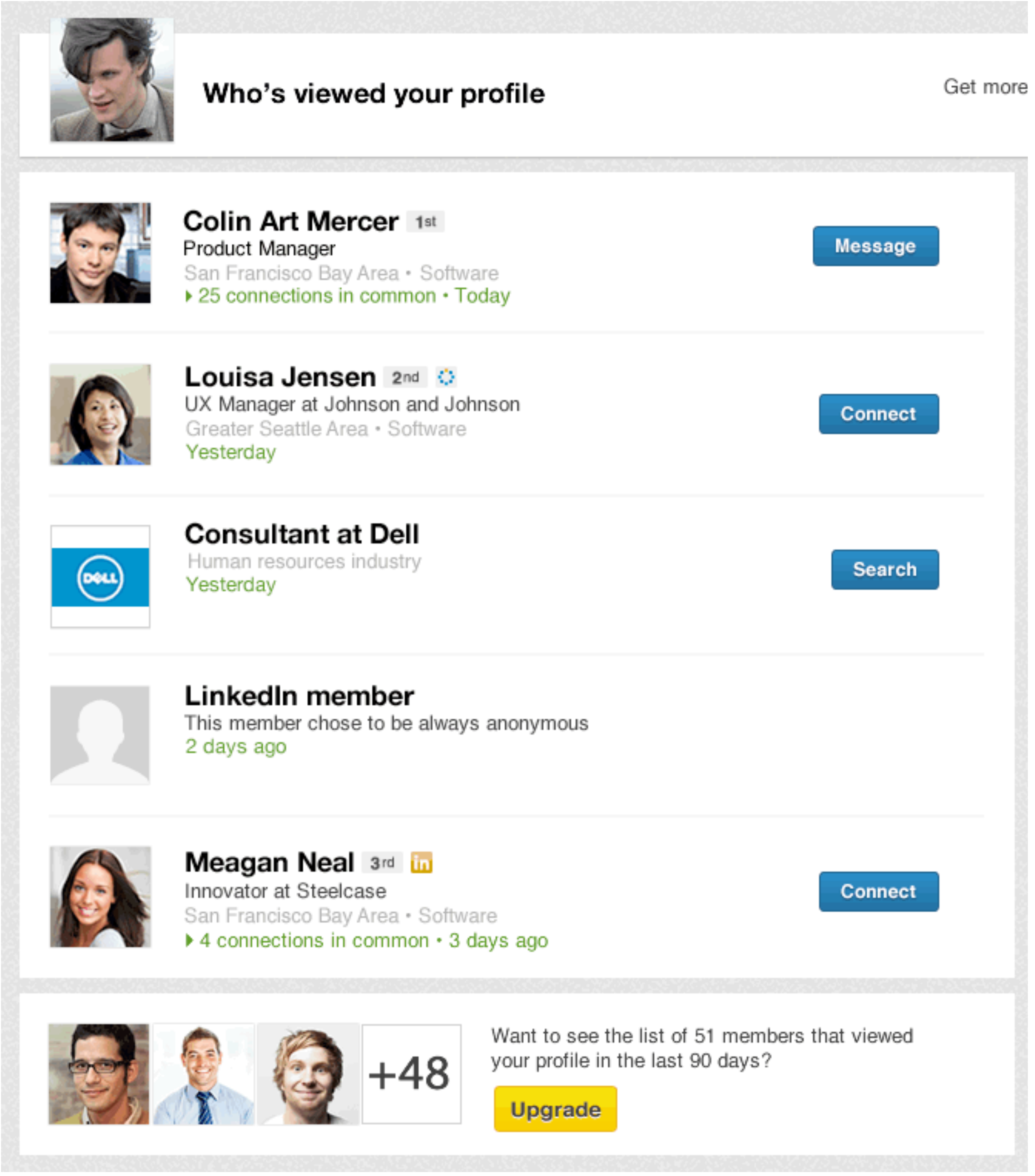
LinkedIn, Instagram, and Facebook are good options

Attackers often stop as soon as they find something: give them something shiny and useless.

Create plausible, but false and misleading bits of information on sites specifically for this purpose

Honey Pots & Chaff

LinkedIn Premium accounts allow you to view accounts that view you. If you make a honeypot account that no one from your “real” life would look into, only those who are actively investigating you, you’ll get some insight on who they are



Who’s viewed your profile

Get more

Colin Art Mercer 1st
Product Manager
San Francisco Bay Area • Software
25 connections in common • Today
Message

Louisa Jensen 2nd
UX Manager at Johnson and Johnson
Greater Seattle Area • Software
Yesterday
Connect

Consultant at Dell
Human resources industry
Yesterday
Search

LinkedIn member
This member chose to be always anonymous
2 days ago

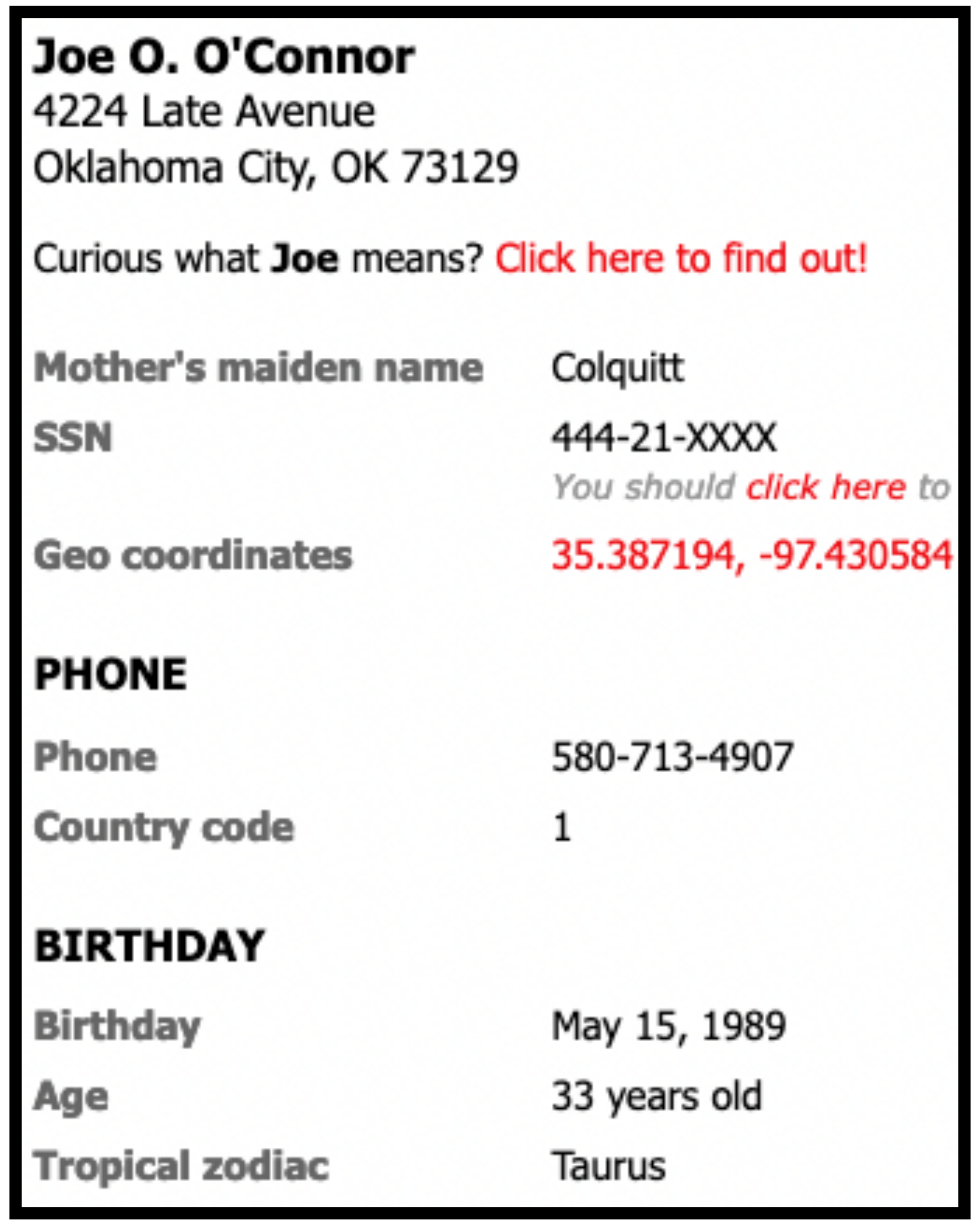
Meagan Neal 3rd
Innovator at Steelcase
San Francisco Bay Area • Software
4 connections in common • 3 days ago
Connect

+48

Want to see the list of 51 members that viewed your profile in the last 90 days?
Upgrade

thispersondoesnotexist.com

fakenamegenerator.com



Joe O. O'Connor
4224 Late Avenue
Oklahoma City, OK 73129

Curious what **Joe** means? Click here to find out!

Mother's maiden name	Colquitt
SSN	444-21-XXXX *You should click here to*
Geo coordinates	35.387194, -97.430584

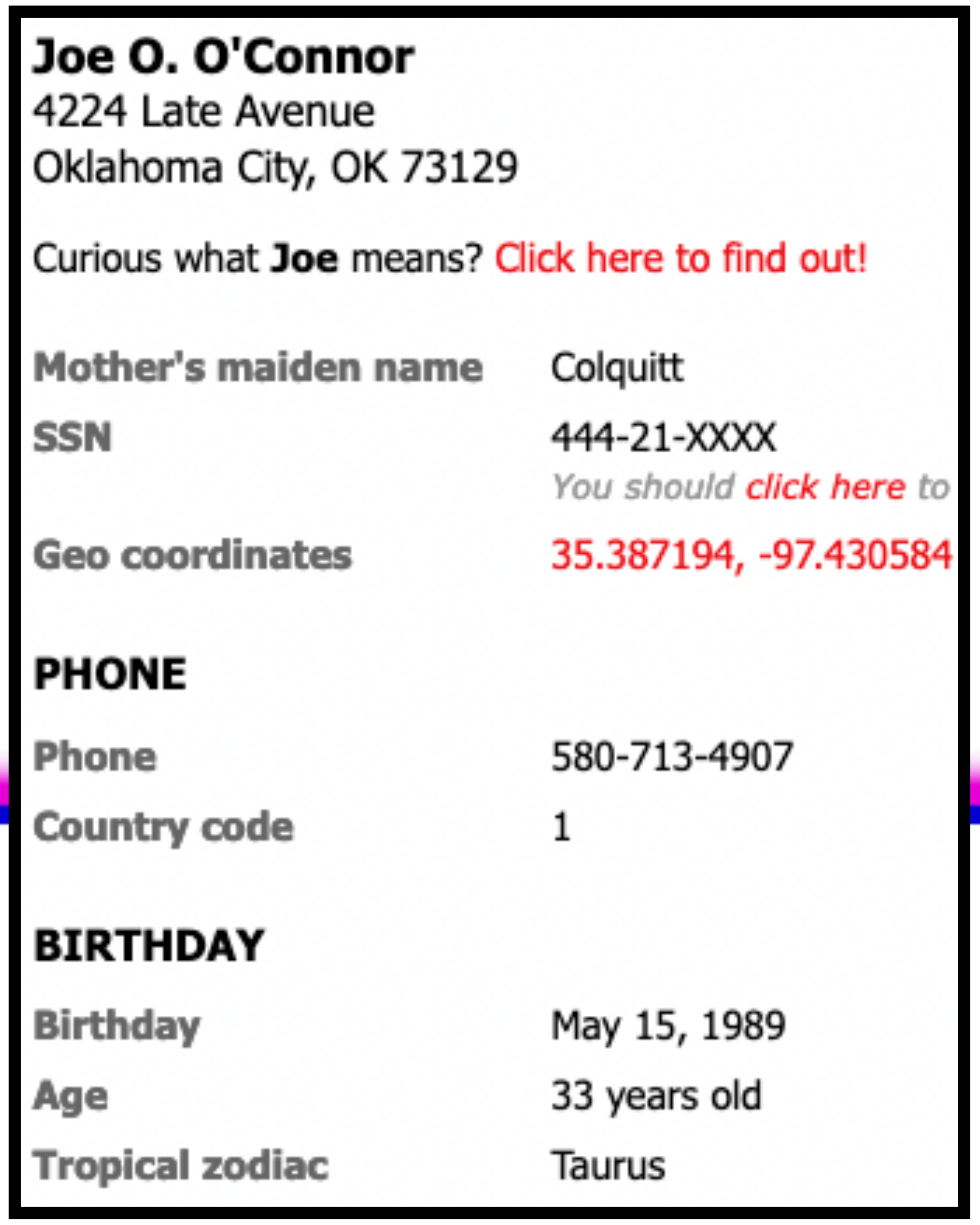
PHONE

Phone	580-713-4907
Country code	1

BIRTHDAY

Birthday	May 15, 1989
Age	33 years old
Tropical zodiac	Taurus

Chaff & Socks



Joe O. O'Connor
4224 Late Avenue
Oklahoma City, OK 73129

Curious what **Joe** means? Click here to find out!

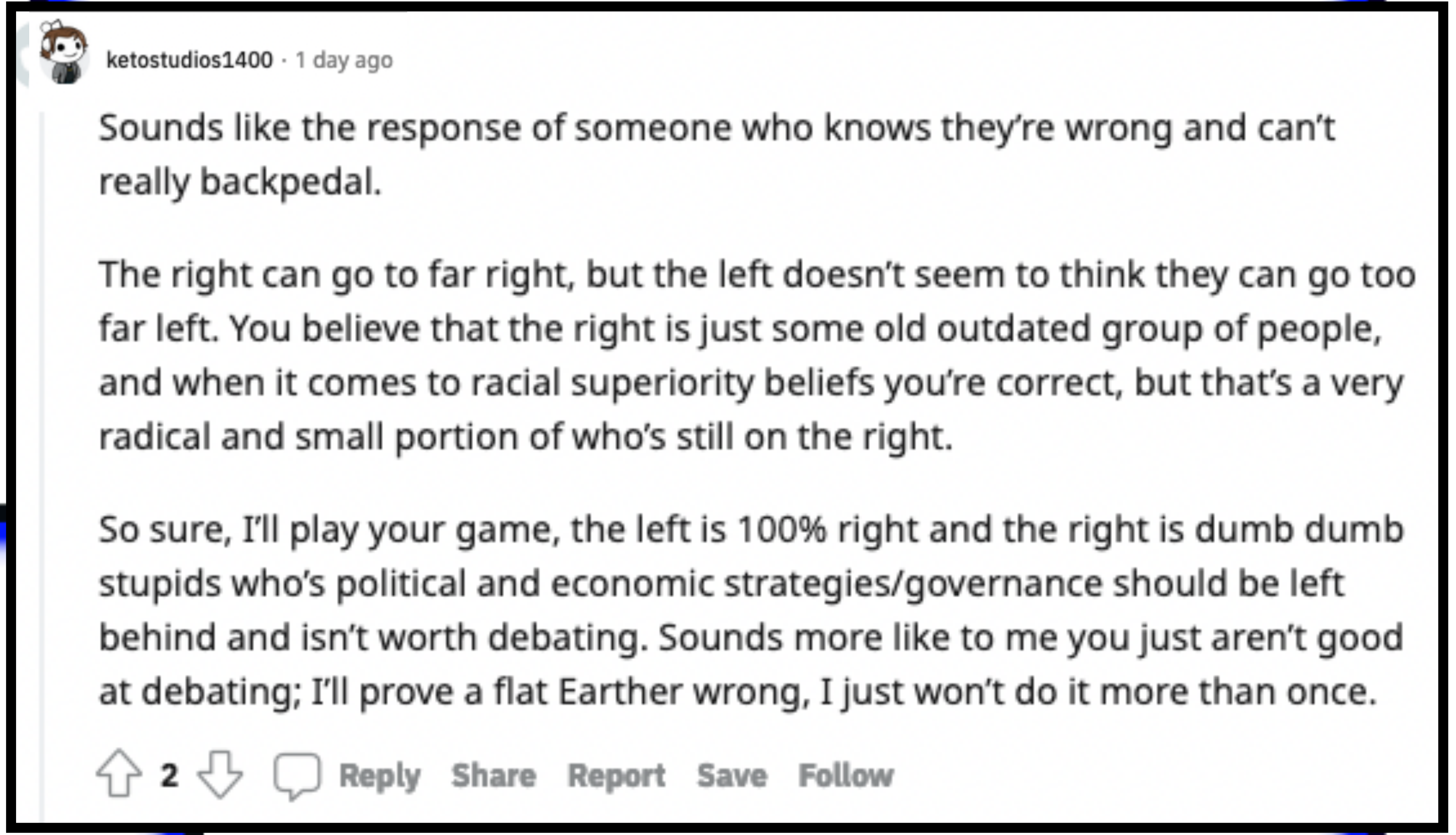
Mother's maiden name	Colquitt
SSN	444-21-XXXX *You should click here to*
Geo coordinates	35.387194, -97.430584

PHONE

Phone	580-713-4907
Country code	1

BIRTHDAY

Birthday	May 15, 1989
Age	33 years old
Tropical zodiac	Taurus

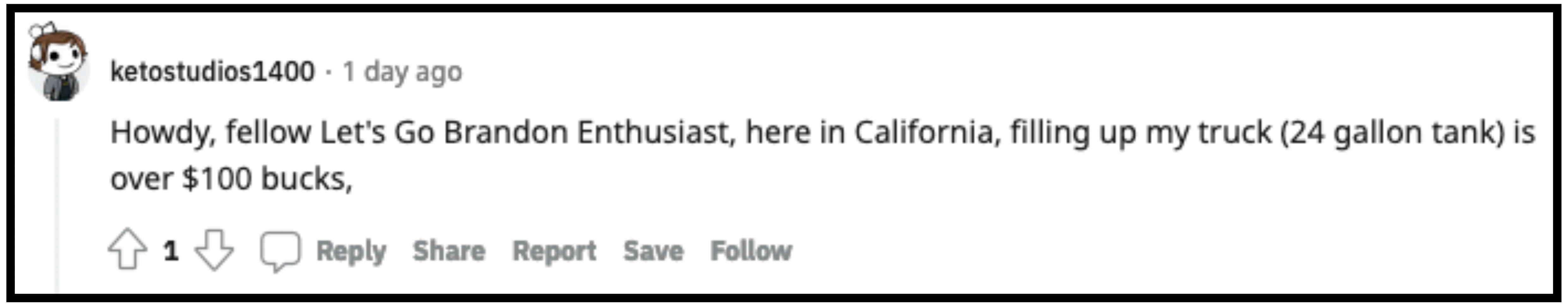


ketostudios1400 · 1 day ago

Sounds like the response of someone who knows they're wrong and can't really backpedal.

The right can go to far right, but the left doesn't seem to think they can go too far left. You believe that the right is just some old outdated group of people, and when it comes to racial superiority beliefs you're correct, but that's a very radical and small portion of who's still on the right.

So sure, I'll play your game, the left is 100% right and the right is dumb dumb stupids who's political and economic strategies/governance should be left behind and isn't worth debating. Sounds more like to me you just aren't good at debating; I'll prove a flat Earther wrong, I just won't do it more than once.

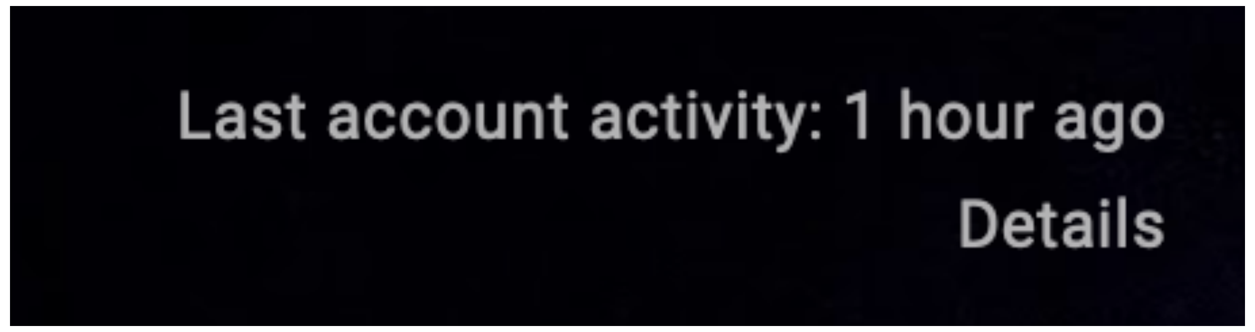


ketostudios1400 · 1 day ago

Howdy, fellow Let's Go Brandon Enthusiast, here in California, filling up my truck (24 gallon tank) is over $100 bucks,

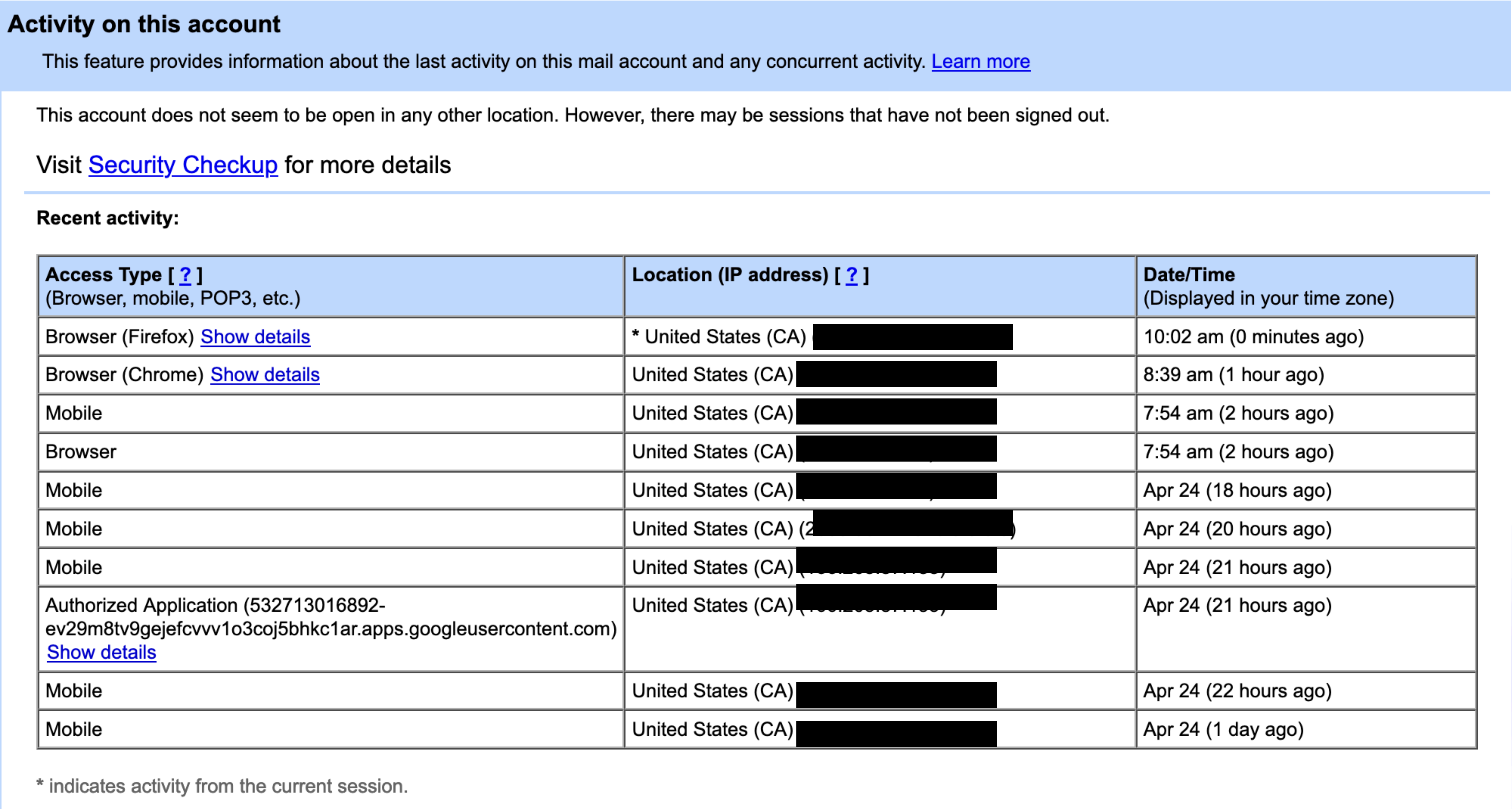
Monitor Gmail Logins

If you think someone is in your email, check the login details screen often



Last account activity: 1 hour ago

Details



Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

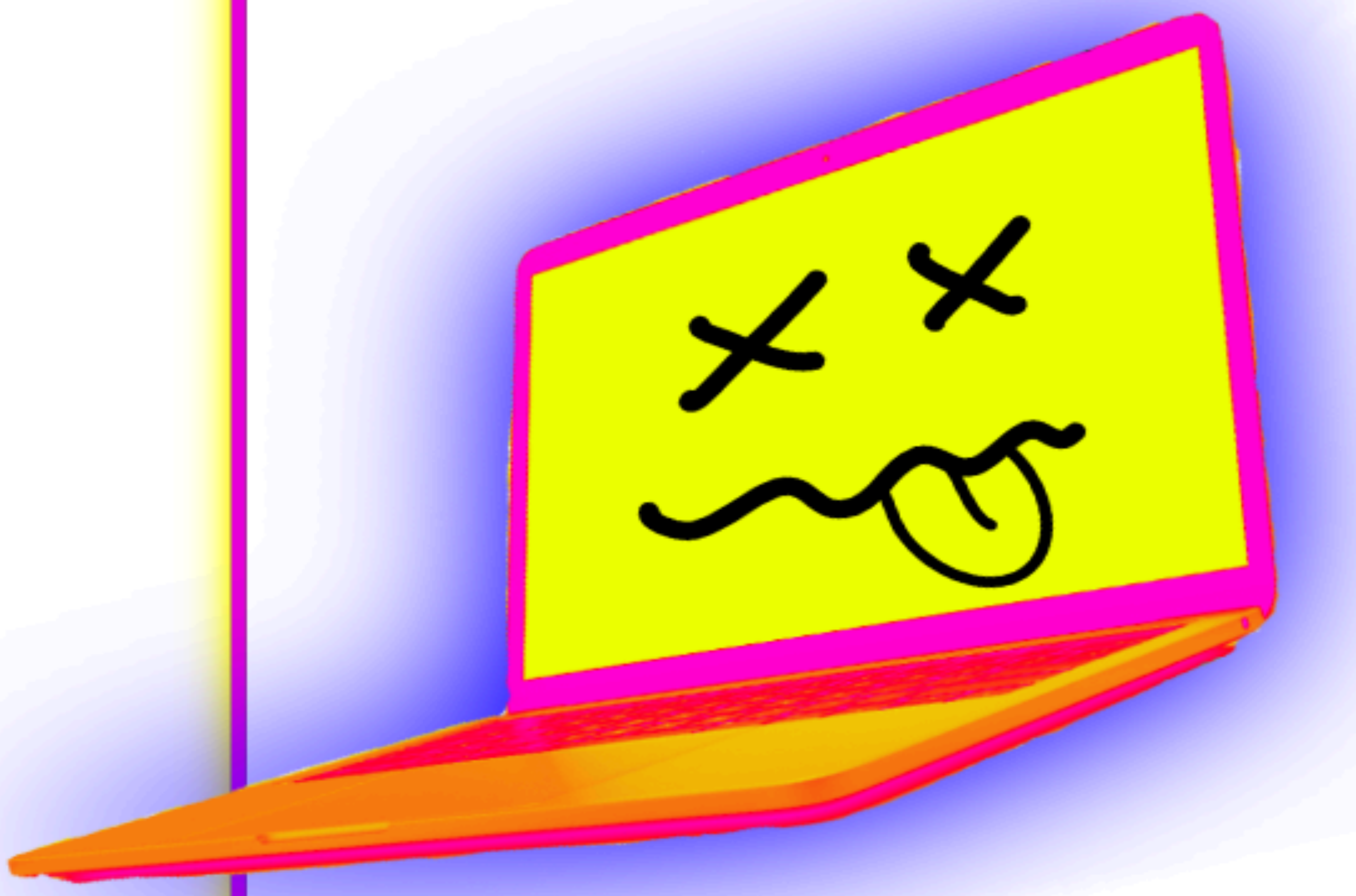
This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Visit Security Checkup for more details

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address)** [?]	**Date/Time** (Displayed in your time zone)
Browser (Firefox) Show details	* United States (CA) [redacted]	10:02 am (0 minutes ago)
Browser (Chrome) Show details	United States (CA) [redacted]	8:39 am (1 hour ago)
Mobile	United States (CA) [redacted]	7:54 am (2 hours ago)
Browser	United States (CA) [redacted]	7:54 am (2 hours ago)
Mobile	United States (CA) [redacted]	Apr 24 (18 hours ago)
Mobile	United States (CA) [redacted]	Apr 24 (20 hours ago)
Mobile	United States (CA) [redacted]	Apr 24 (21 hours ago)
Authorized Application (532713016892-ev29m8tv9gejefcvvv1o3coj5bhkc1ar.apps.googleusercontent.com) Show details	United States (CA) [redacted]	Apr 24 (21 hours ago)
Mobile	United States (CA) [redacted]	Apr 24 (22 hours ago)
Mobile	United States (CA) [redacted]	Apr 24 (1 day ago)

* indicates activity from the current session.



Make an Incident Log

Useful for not only learning about attackers, but also patterns, and where to focus.

Useful for yourself but also if/when you need to include the help of others

DATE	SITE/PLACE	USER	DESCRIPTION
7/20/21	twitter	@lazy_ghost_4000	Claimed to know my...

Incident Response

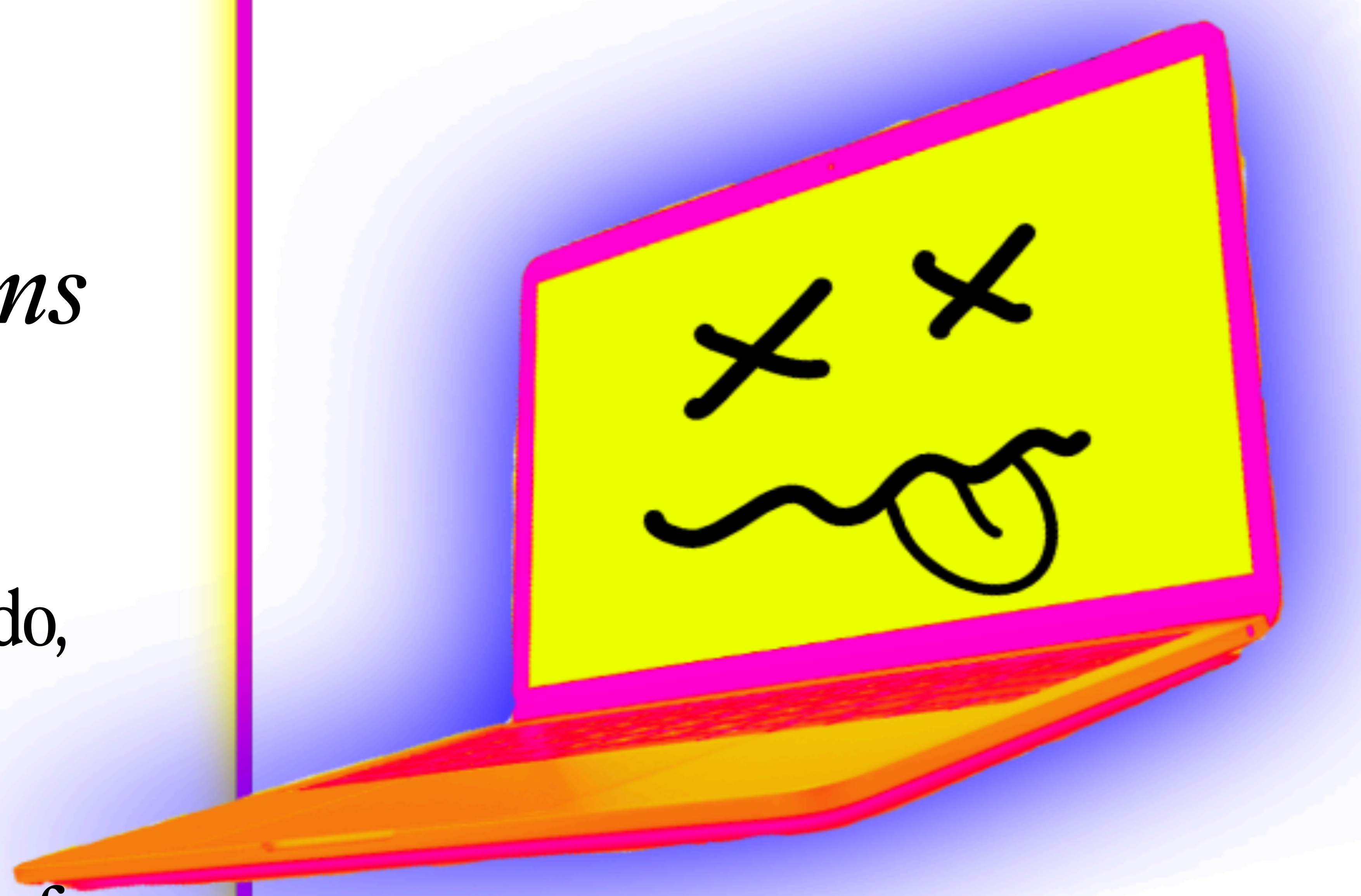
First, assess the situation.

- *What data has been exposed?*
- *Where was that data available?*
- *Which accounts were affected?*

Isolate the Problem.

- *Lock or deactivate the affected accounts*
- *Lock all other related accounts and check them for signs of compromise*

Keeping a written record of a plan of action, perhaps steps in order of what to do, will help immensely if you are in a stressful situation.



Employ the help of friends and trusted accomplices to monitor accounts, areas of threat action.

Running Recon on Suspected Attackers

Use the information gathered from your incident log, honeypot, and the tools we've gathered above to learn about them.

Username checking is especially useful here (whatsmyname and other apps)

Keep the recon you are doing passive. Don't engage, don't interact, and ALWAYS use good privacy hygiene while doing it. You don't want to reveal yourself in the process.

Doxxing and the Harassment and Abuse That Follows is Illegal & Against Platform ToS

All the techniques described are ways you can take matters into your own hands, but you can always engage with the platforms as well as law enforcement

It is in the platforms' best interest to prevent harassment on their app. Their response might not be as thorough, but it's worth trying

Daly *(she/her)*
daly.barnett@protonmail.com
@ablanathtanalba

Compartmentalization Techniques Slides:

digitaldefensefund.org/ddf-slide-decks/compartmentalization

hackinghustling.org
@hackinghustling