Privacy Champions

Staying Safe Online

September 26, 2019

AGENDA

- Introduction (and caveats)
- How Information is Collected Online
- Privacy and Personal Devices
- Search Engines & Web Browsers
- Password Management
- Social Media Privacy Settings

Introduction:
Technology is Part of the Fabric of our Lives

I Tried Hiding From Silicon Valley in a Pile of Privacy Gadgets

Bloomberg, August 2019

I Cut the 'Big Five' Tech Giants From My Life. It Was Hell

Gizmodo, February 2019

Caveats:

- Everyone comes to this with their own context.
- Specific products are only mentioned as examples. There are many tools out there, and we aren't endorsing any particular product, tool, or service.
- No tool is perfect or foolproof.

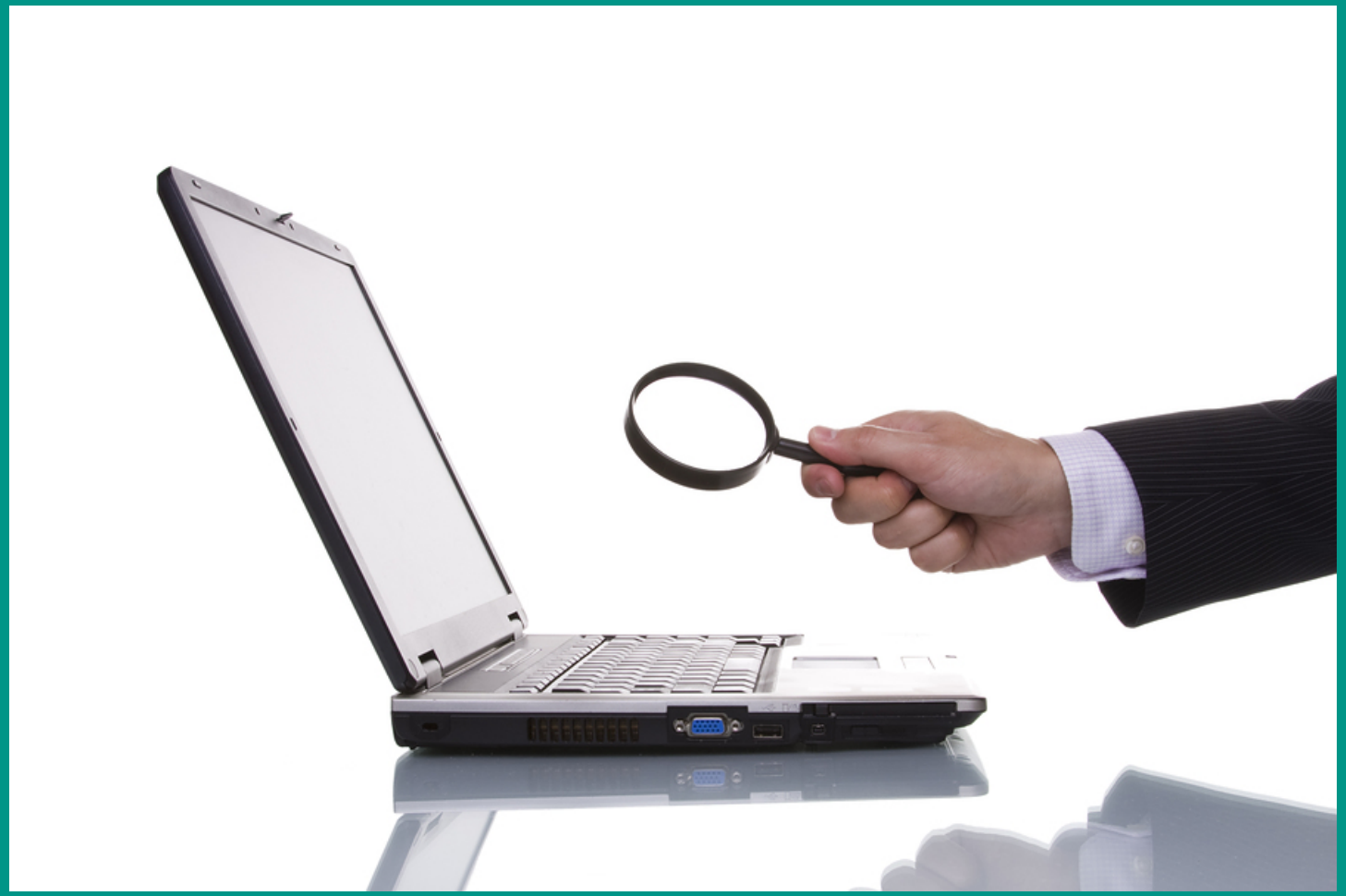
Why should we care about privacy online?

Practical

1. A few simple steps can reduce the likelihood of identity theft and loss of control over important accounts like email and banking.
2. Certain app/device settings can reveal a lot of information about you to other people that you may prefer to keep private (such as location).
3. Restricting what apps you use or services you sign up for can reduce risk (e.g. Cambridge Analytica).

Idealistic

4. Remaining intentional about our digital behavior can send a message about our current system of “surveillance capitalism.”



How is information collected from you online?

Information Collection Happens in Numerous Ways

Active Collection of Information

- Webforms
- Signing up for emails
- Creating accounts
- Linking profiles
- Activity, such as social media posts, sending emails, conducting web searches
- Electronic payments

Passive Collection of Information

- Cookies and Tracking Technologies
- Scrolling, typing, mouse behavior
- Passing by Bluetooth beacons or WiFi antennaes

Privacy and Your Personal Devices

Check your smartphone's privacy settings

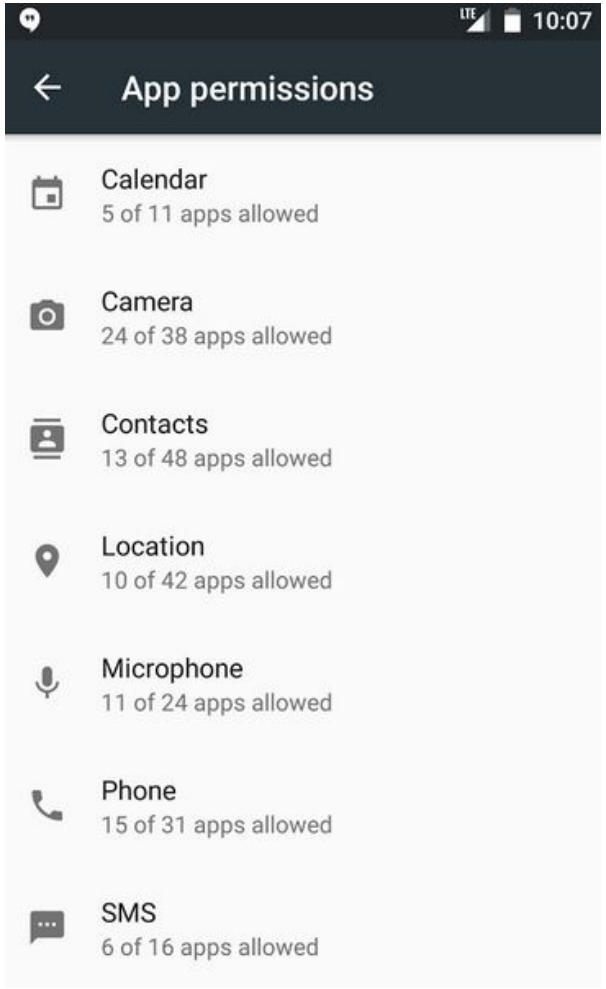
- Smartphone apps can run in the background of your phone, gathering all kinds of private data about you, such as your:
  - Location
  - Contact list
  - Photos
  - Videos
  - Etc.
- It's a good idea to audit and limit these permissions so apps don't gain access to data you don't want them to.

Check your smartphone’s privacy settings: iPhone

- Open up “Settings” and then go to the “Privacy” menu. Here, you’ll find a list of different privacy permissions, like location, contacts and more.
- Go through each option and disable access to any app where it doesn’t make sense. For example, a game you downloaded to fill time on the bus doesn’t need access to your location, the mic or your photo library.

Check your smartphone’s privacy settings: Android

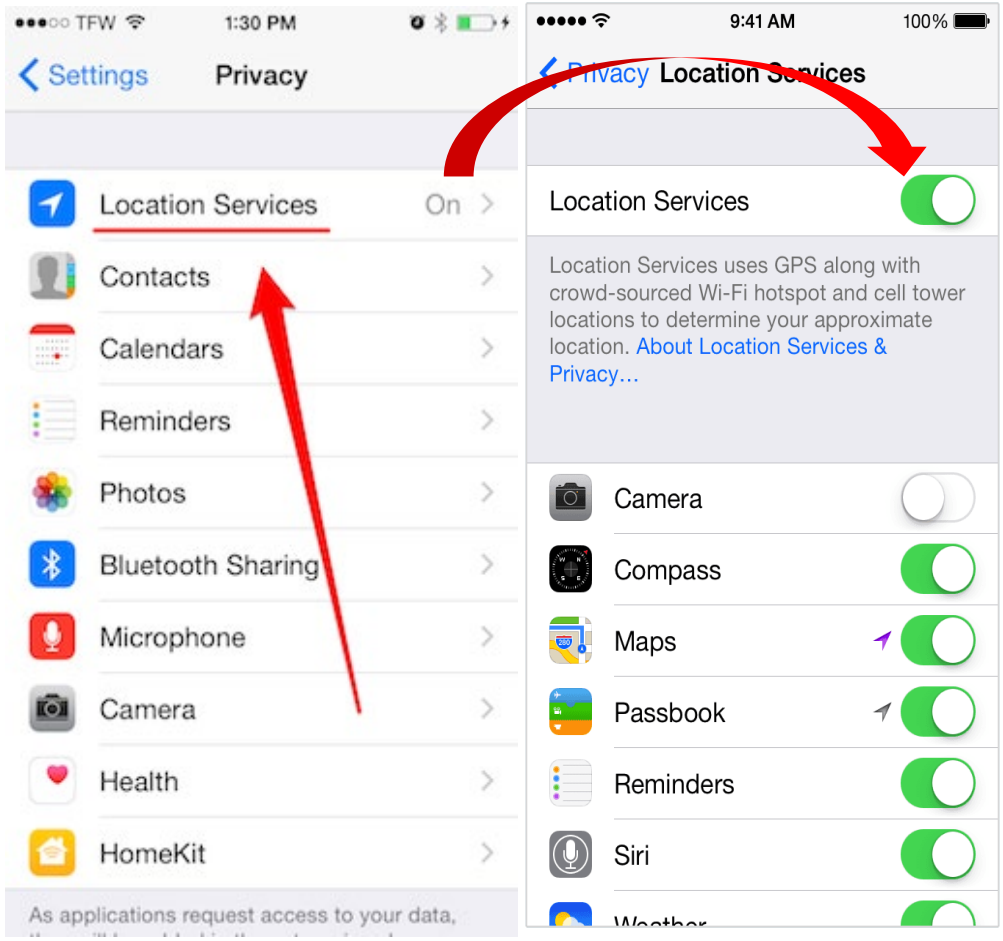
- On stock Android (it may be different on your phone), head to the Settings menu and open the Apps menu.
- Tap the gear icon, then tap “App permissions.” You will find permissions for location, microphones, contacts and more.
- Tap each and disable apps you don’t trust or don’t think need access to the data it’s requesting.



Control mobile device location tracking

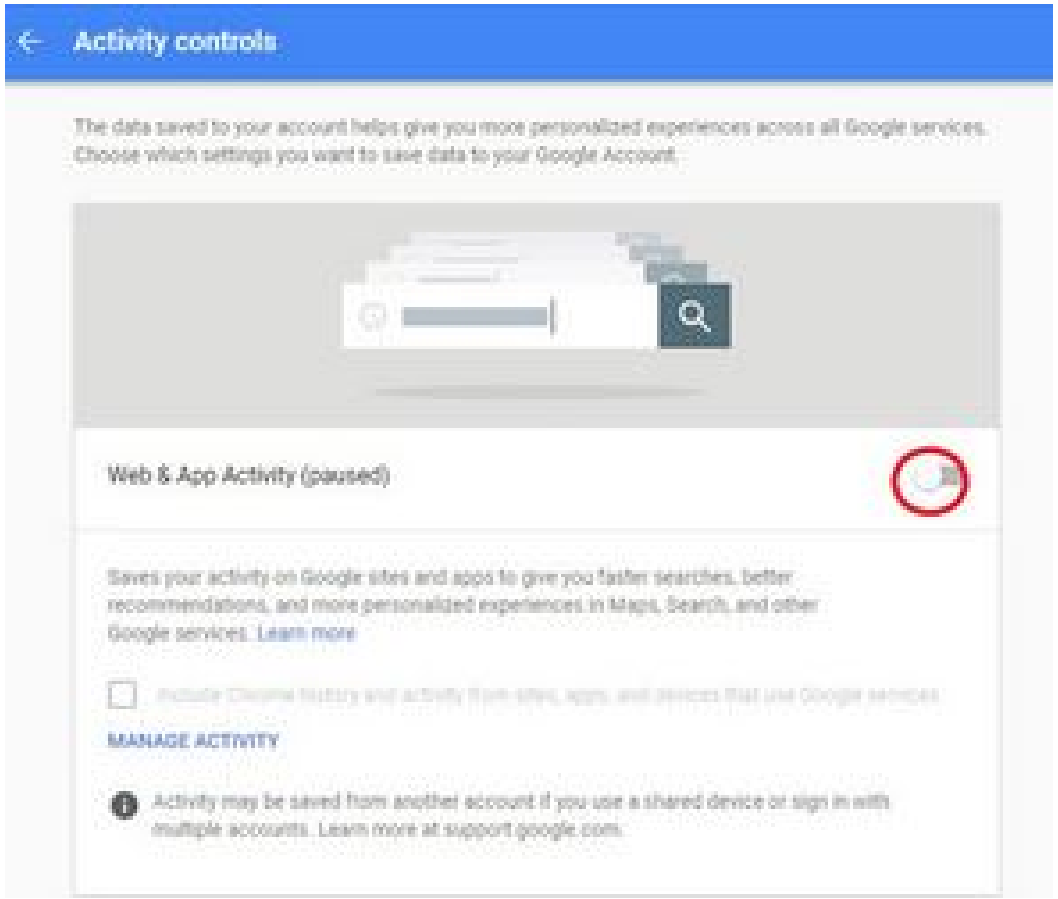
- **Limit location tracking to those apps that actually need it.**
- **Limit location tracking to only when the app is open.**
  - Not every app needs to know your location, and few apps need to know your location at all times. You can control this behavior in your phone's settings.

What you give up: some app features may not work, e.g. Google Maps requires constant access if you want to share your location with someone.



Search Engines and Web Browsers

Control What Information Google Tracks



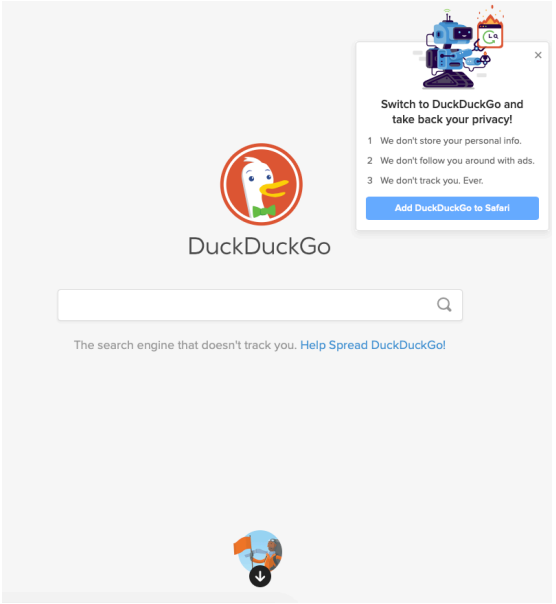
- **Google keeps track of every phrase you ever search for, every site you've visited and every YouTube video you've watched.**
  - On the web, go to Google's activity controls to turn off Web and App Activity.
  - While you're there, scroll down and also turn off YouTube Search History and YouTube Watch History.

- **What you give up**: You won't be able to dig back up websites and videos you once visited, and Google's systems won't get to know you as well.

Privacy-focused online tools

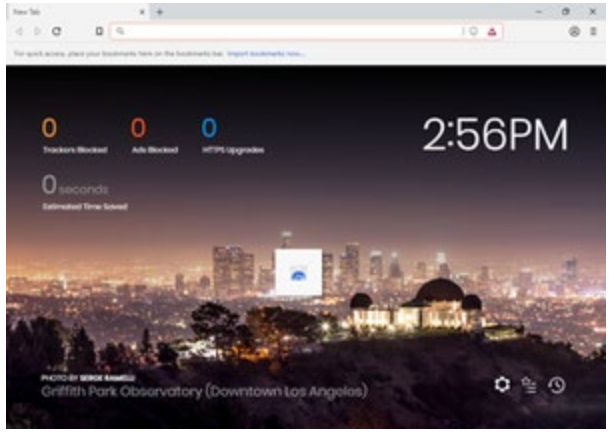
Google alternative: DuckDuckGo

- Search engine that places an emphasis on protecting users' privacy.
- Does not store IP addresses, does not log user information, and uses cookies only when required.
- www.duckduckgo.com



Web browser alternative: Brave

- Blocks ads by default.
- Restricts information that websites can gather on you through cookies and tracking scripts.
- www.brave.com



Other Tools for Controlling Your Information

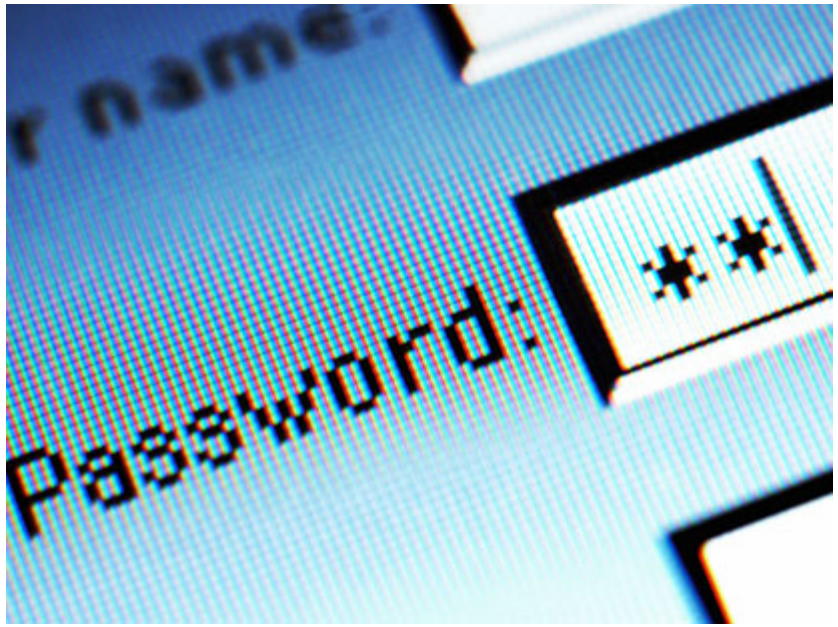
- Limiting internet tracking through your browser:
  - uBlock Origin: Blocks ads and the data they collect on Chrome and Firefox.
  - Privacy Badger: Blocks ad trackers on Chrome and Firefox.
  - HTTPS Everywhere: Directs you to the most secure version of a website on Chrome and Firefox.
  - Using “incognito” mode, or other private browsing mode.
- Online information removal services:
  - Abine (DeleteMe), MyLife, Reputation.com, OneRep.
  - Cost $100-200/year.
  - Fill out information removal forms on behalf of clients with data broker websites like Spokeo.
- Unwanted sales calls:
  - FTC National Do Not Call Registry: https://donotcall.gov/
  - Created to stop unwanted sales calls. It’s free to register your home or mobile phone number.
- Virtual Private Networks (VPN):
  - Tunnelbear, NordVPN
- Opt out of data collection at different websites:
  - https://simpleoptout.com/

***Caveat**: No tool can provide complete assurance of data deletion/privacy protection.*

Password-Based Attacks & Password Management

We are bad at passwords, 2018 edition

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou



Source: https://www.theverge.com/2018/12/13/18139431/donald-trump-2018-worst-password-splashdata

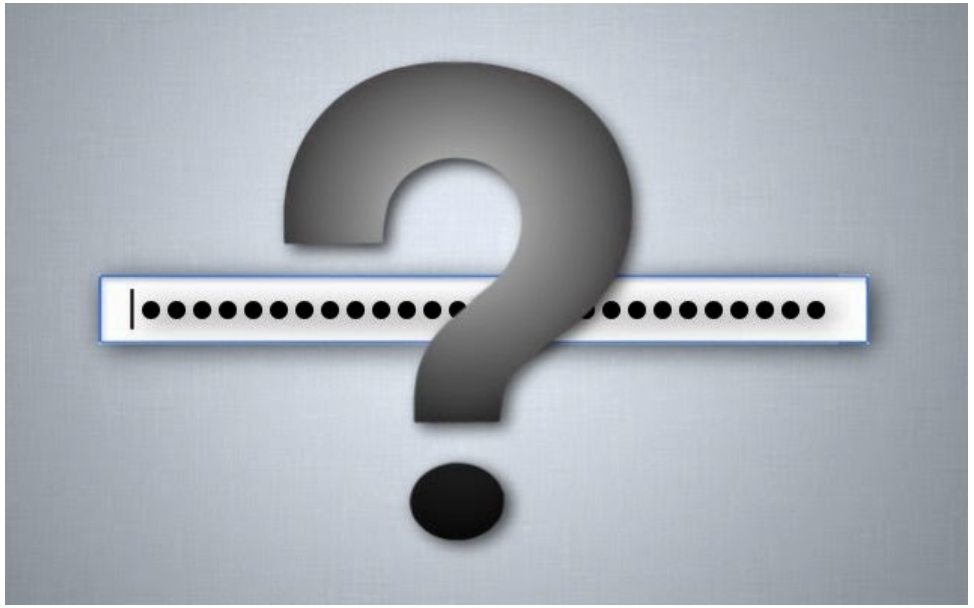
Passwords are vulnerable to a variety of threats

Passwords are the current standard for protecting personal accounts online. There are many ways passwords can be compromised:

- The Dark Web – Hackers can purchase massive lists of login and password information.
- Brute Force – A hacker may use a software program to try to log in with possible password combinations, usually starting with the easiest-to-guess passwords.
- Key Loggers – A hacker may user a software program to track a user's keystrokes. By analyzing the entries, a user's ID and password can be easily found.

Reusing login credentials is one of the biggest online privacy risks

- Reuse of login credentials is common: a recent study found that 52% of users have the same passwords (or very similar) for at least two different services.
- Reusing username/password combinations across multiple sites leaves users open to “credential stuffing” attacks.
- If credentials from one account are compromised, hackers can reuse those credentials to access other accounts.
- That puts email and banking sites at risk, and puts users in a position to be victims of more complicated identity theft down the road.



Source: https://www.pandasecurity.com/mediacenter/security/password-reuse/

Reusing login credentials is one of the biggest online privacy risks

Family says hacked Nest camera warned them of North Korean missile attack

- An Orinda family was enjoying their Sunday afternoon when “a warning claiming to be from Civil Defense rang out from their living room, alerting the family of three missiles aimed at Los Angeles, Chicago and Ohio.”
- “It was five minutes of sheer terror and another 30 minutes trying to figure out what was going on.”
- According to Nest, the problem was compromised passwords.

Source: https://www.washingtonpost.com/technology/2019/01/23/family-says-hacked-nest-camera-warned-them-north-korean-missile-attack/

Best practices for use of credentials online: password managers

Best practice for passwords include:

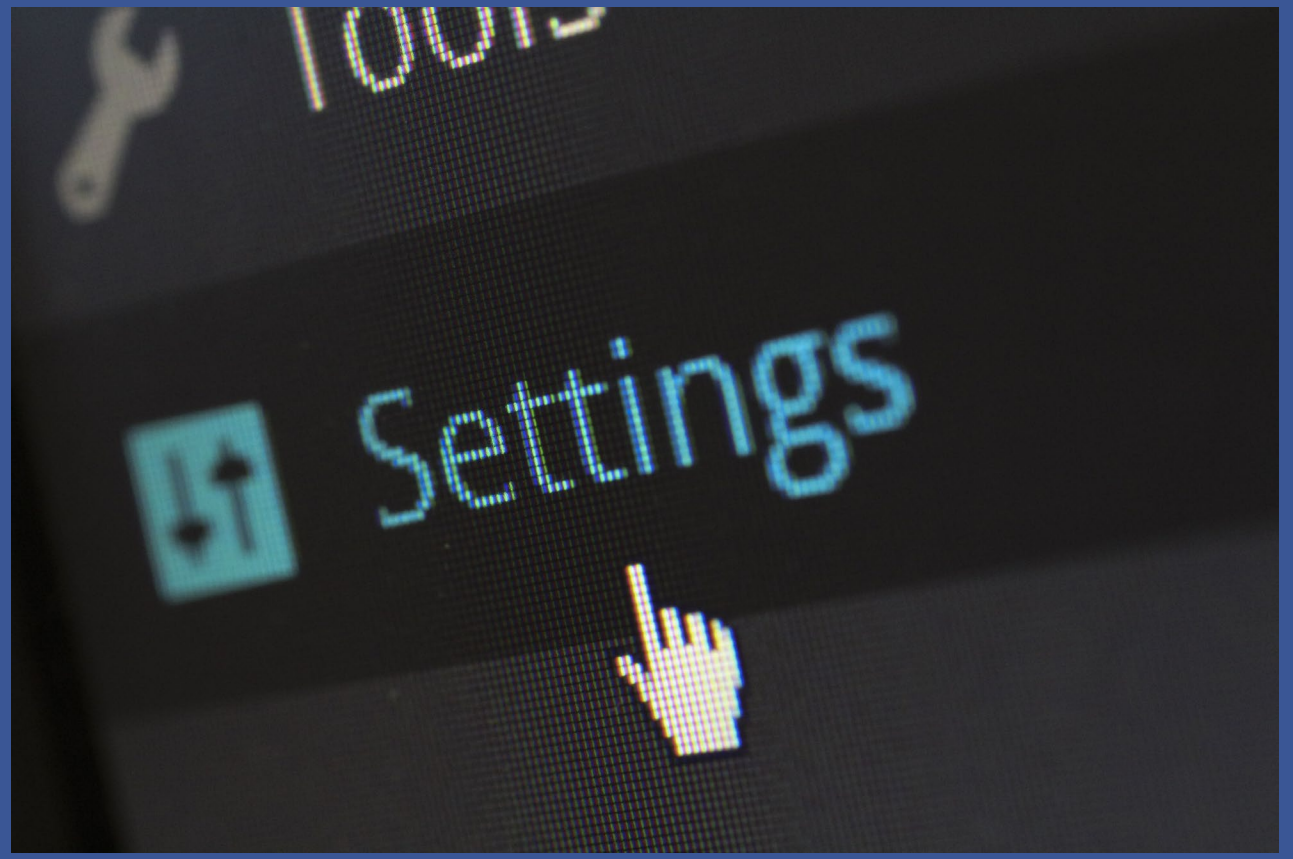
- Use different passwords for every online service.
- Make your password long, strong, and complex.
- Change your passwords with some level of frequency.
- How can anyone actually do this? With a password manager. Some options include:
  - 1Password
  - Dashlane
  - LastPass
  - Several others
- Actually use the password manager.

Sources: https://www.pcmag.com/roundup/300318/the-best-password-managers

Best practices for use of credentials online: two-factor authentication

- There are three generally recognized factors for authentication: **something you know** (such as a password), **something you have** (such as a hardware token or cell phone), and **something you are** (such as your fingerprint). Two-factor means the system is using two of these options.
- Two-factor authentication comes in two primary forms:
  - Text message verification: A numerical code is sent to you as a text message.
  - Application authentication: An authentication app constantly generates new codes valid for 30 seconds each.
- High priority accounts: Email, bank accounts, your password manager and social networks.

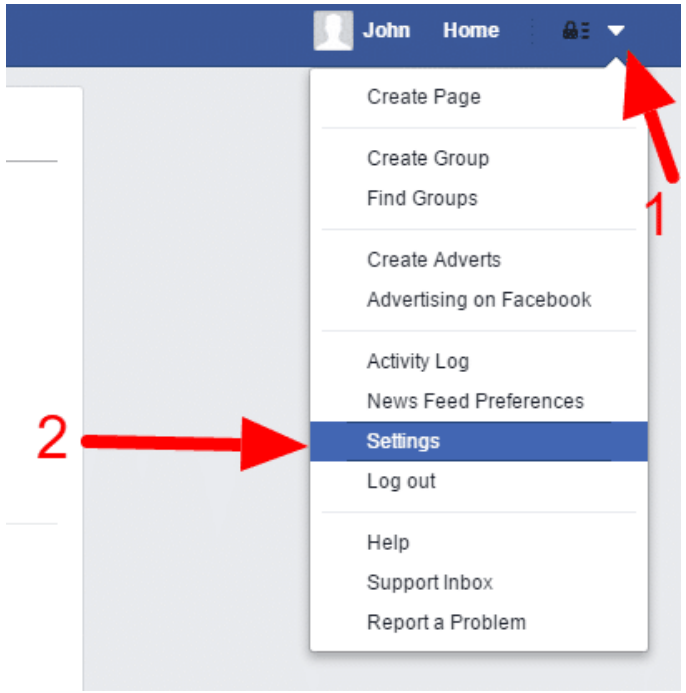
Source: https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up

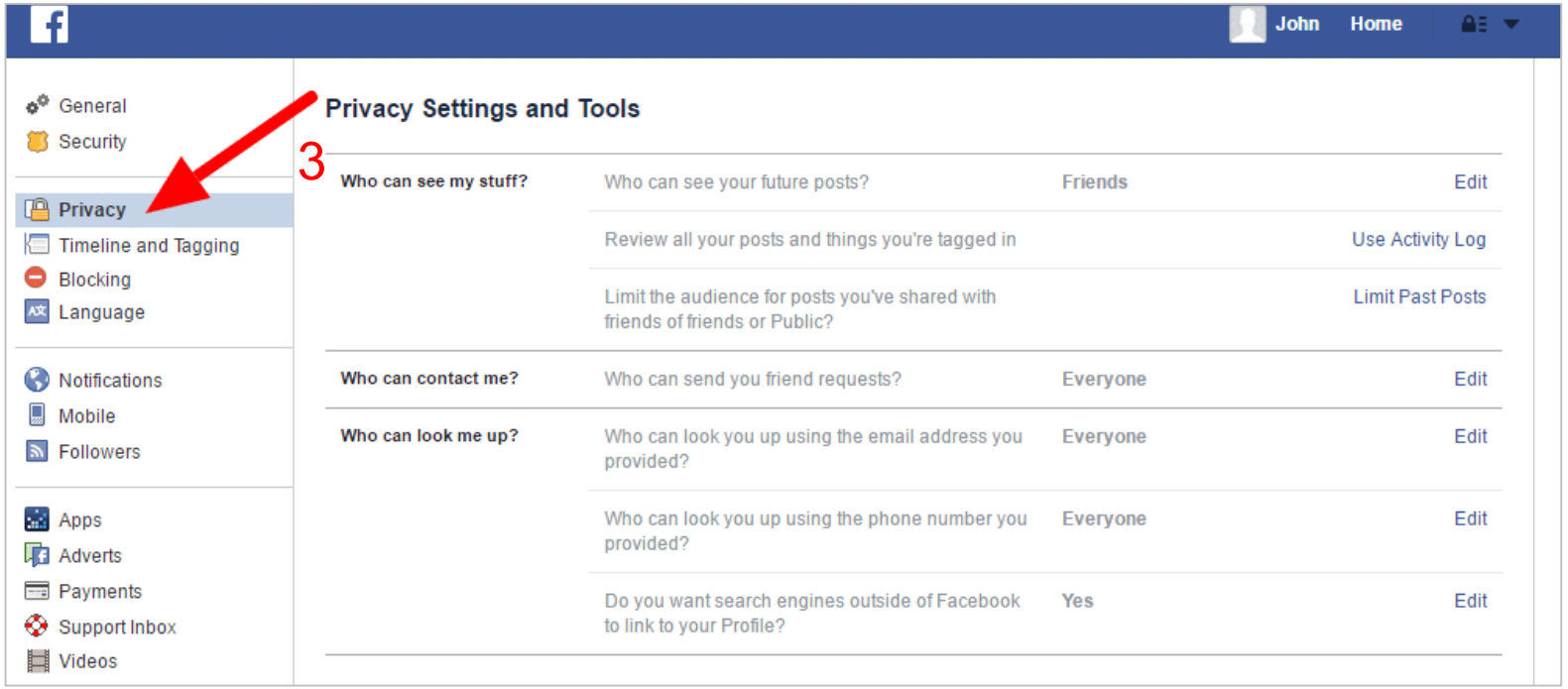


Privacy Settings in Social Media and Other Accounts

Facebook: Accessing Privacy Settings in 3 Clicks

Facebook is one of the most widely used social media platforms, with over 2.23 billion monthly active users. We often use the site to keep up with our friends, but a wealth of personal information can be found on our profiles. **You should regularly review privacy settings on social media accounts to ensure they match your personal privacy preferences.**

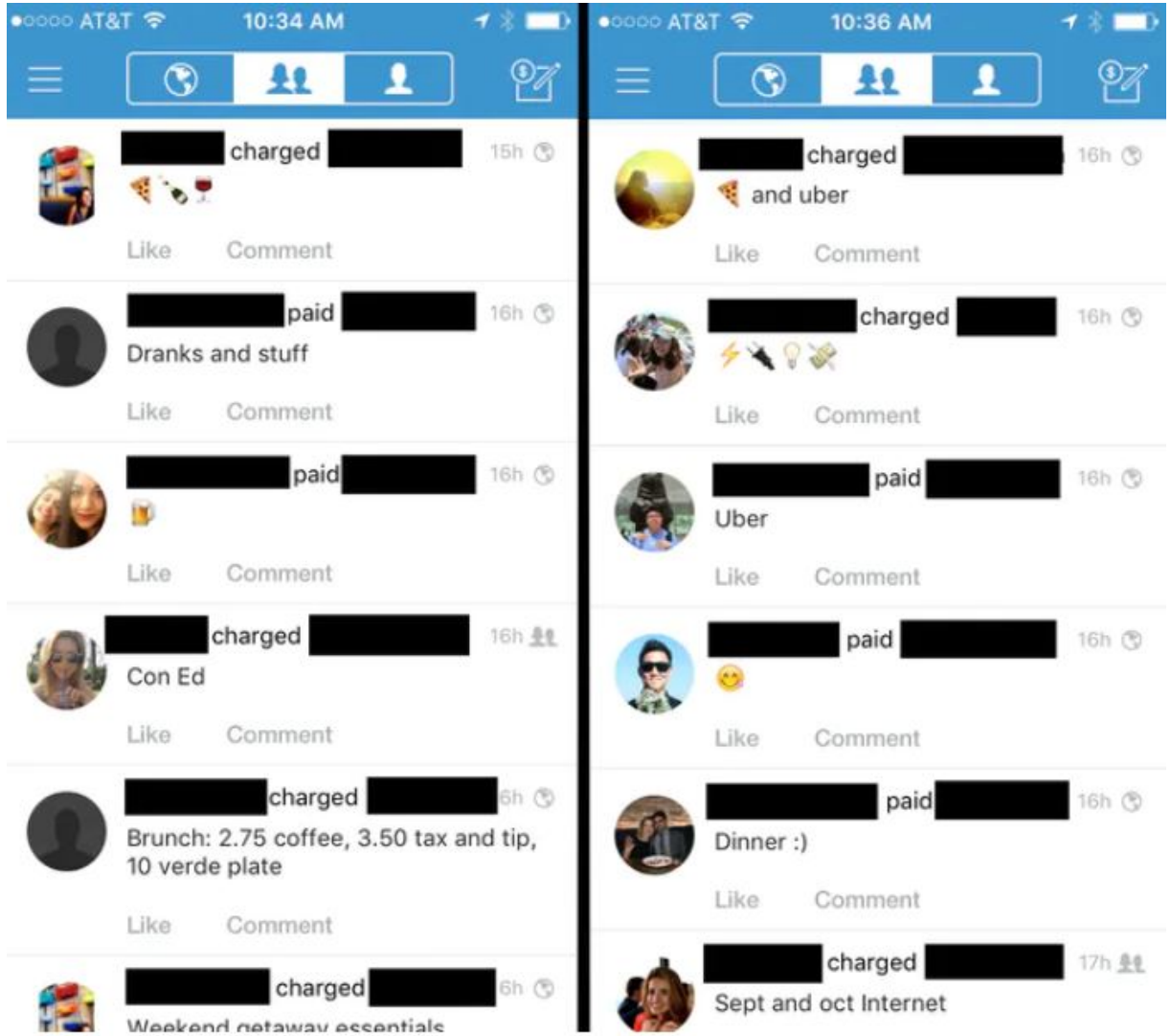




Source: https://iag.me/socialmedia/make-facebook-account-private/

Venmo: Change your payment activity to private

- By default, privacy settings allow all user transactions to be visible on a public feed.
- You can tell a lot from these feeds.
  - A researcher was able to track two users' transactions, determine that they were married, owned a car, had a dog that was recently taken to the vet, shopped at Walmart, live in San Diego, and mostly eat pizza when dining out.



Source: https://www.marketwatch.com/story/the-scary-reasons-you-should-make-your-venmo-account-private-2018-07-17

Conclusion

- Information collection is growing exponentially.
- Despite that, we can still exercise control over what we share.
- Limit app permissions on your phones and other devices.
- Explore tools for limiting information collected while using the web, such as privacy-focused search engines, web browsers, and ad blockers.
- Use a password manager.
- Exercise control over social media and other accounts.

PRIVACY OFFICE

COUNTY OF SANTA CLARA

Email: PrivacyOffice@ceo.sccgov.org

Internal website: https://sccconnect.sharepoint.com/sites/cpo

External website for constituents: https://www.sccgov.org/sites/cpo