PRIVACY RESOURCE SHEET

Recommended actions for everyone

1. Enable two-factor authentication for any sites that offer it.
2. Install updates (operating system, browser, etc.).
3. Use a password manager to store and generate passwords, along with a strong passcode (https://www.eff.org/dice) as your master password.
4. Be suspicious of links and files in email, especially links that take you to a page that asks you to enter your credentials (username and password). You can copy-and-paste suspicious links into https://urlscan.io/ to see if they contain malicious content.
5. Go through the steps in the Data Detox Kit to see and manage where your information exists online: https://datadetox.myshadow.org/en/detox.

Privacy tools

Browsers and Browser Extensions

- Privacy Badger (browser extension from EFF, works with Firefox and Opera; blocks ad trackers): https://www.eff.org/privacybadger
- HTTPS Everywhere (browser extension from the Electronic Frontier Foundation, works with Chrome, Firefox, and Opera; upgrades unencrypted websites to encrypted): https://www.eff.org/https-everywhere
- Tor browser (hides your location from the sites you visit and from your internet service provider; Google products typically don't work on Tor): https://www.torproject.org/
- Brave browser (block ads and ad trackers by default; upgrades websites to https; optional private Tor tabs): https://brave.com/
- Firefox + HTTPS Everywhere + Privacy Badger = also a good option

Search Engines

- DuckDuckGo (search engine that doesn't track you): https://duckduckgo.com/
- StartPage (another search engine that doesn't track you): https://www.startpage.com/

Helpful Websites

- Have I Been Pwned (check to see whether your email address has been included in any data breaches): https://haveibeenpwned.com/
- Somewhat silly website that exposes how much your browser can tell about who you are and what you're doing: https://clickclickclick.click/
- Test how private "private browsing" or "incognito mode" really is: https://www.nothingprivate.ml/
Mobile device privacy apps

- Signal (encrypted messaging app; available for iPhones and Android)
- OnionBrowser (iPhones only; private mobile browser)
- Orbot (Android only; free proxy app that encrypts mobile internet traffic): https://guardianproject.info/apps/orbot/

Data broker opt-out links

- https://www.whitepages.com/suppression_requests
- http://www.spokeo.com/opt_out/new
- https://www.intelius.com/optout.php
- http://www.peekyou.com/about/contact/optout/index.php
- http://www.beenverified.com/opt-out-instructions
- https://www.peoplefinders.com/manage
- https://neighbor.report/remove
- https://www.instantcheckmate.com/opt-out/
- https://www.truthfinder.com/opt-out/
- Mylife.com: Look up your name and copy the URL, then email privacy@mylife.com and ask to opt out

References list

Ad tracking and targeting

- "Cambridge Analytica: how did it turn clicks into votes?" The Independent: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie
- "How companies learn your secrets" New York Times: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html
- "Facebook (still) letting housing advertisers exclude users by race" Propublica: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin
Data collection and vulnerable populations

Password manager and VPN reviews
- "Best free password managers of 2018" PC Mag: https://www.pcmag.com/article2/0,2817,2475964,00.asp
- "Best password managers of 2018" PC Mag: https://www.pcmag.com/article2/0,2817,2407168,00.asp
- “The Best VPN services for 2019” PC Mag: https://www.pcmag.com/roundup/296955/the-best-vpn-services

Smart devices/internet of things
- "The house that spied on me" Gizmodo: https://gizmodo.com/the-house-that-spied-on-me-1822429852