Before I start, don't think "why would someone hack me? I'm broke/unimportant". Everyone has something, even if it seems trivial. You Spotify account could be on the dark web selling for 2 bucks. You could be on a master list of passwords and usernames. Someone could be using your uber account without your knowledge. Most importantly, your online presence is being tracked extensively and extremely personal and accurate profiles of you are being made and sold to advertisers. Apps don't need to secretly listen to you to give you extremely personal ads, you're giving them that information for free. Cops will use the same tactics to track and identify you.

I'm going to start with the basics, move to more complicated stuff, and end with some optional things that I personally do

So let's begin:

- Change your WIFI password. Most people use the password straight out of the box, some come up with simple passwords. It needs to be changed a be less simple.

- Visit your router dashboard and change the password there as well. To see your router dashboard, you typically type in the IP of the router into your browser. This information will be on the back/bottom of your router

- Make a list of every single online account you have. Bank account, social media, email... I'm talking everything. Once you have that list compiled, change the passwords.

- Get a password manager! This will make the previous steps way easier. Most internet browsers have their own built in password manager, as well as Iphone and android. You can take advantage of these or you can subscribe to a paid one. I recommend 1Password. Paid password managers work across the board, meaning your passwords are saved to your account and will work on any PC or phone your're using in the momenr. They also have built in password generators, I recommend using these. The more complex your password is, the less likely for a breach to occur. You can also find free password generators online.

- Bluetooth, WIFI, and location services should not always be on. This is one of those things where you'll have to create new a habit. Get use to completely turning off these settings when you don't need them. You can be tracked, and information can be stolen through when they are on. I find myself regularly toggling these settings throughout the day.

- ❖ Unless you have a VPN, only connect to trusted WIFI networks. No more free or public WIFI, that shit is dangerous. Deal with your cellular connection or get a VPN. (I'll get into VPNs a lil later)

- ❖ Don't use your fingerprint or face to unlock your phone. Or at the very least, know how to quickly turn these features off in case of a confrontation with the law. Cops can easily abuse these methods to gain access to your phone.

Now those are just the basics, so I really don't recommend just stopping there.

2-factor verification and your phone number:

A lot of damage can be done just by knowing your phone number. Sit back and think how often you're asked for your number. We are regularly required to cough this information up. Remove your number from all social media and sites where it's not required. Don't put your phone number down for promotions and sign ups.

- ❖ I recommend second number services like **Google Voice** for promotions/signups and random websites. Google voice is just an extra phone number. There are other free and paid alternatives but GV is simple to use, free, and well known.

- ❖ **2 factor verification** is when a site texts your phone a code before you can log in. The problem is that text based 2 factor is nearly pointless. That's because your phone number can be taken over very easily. Hackers can call your phone company, pretend to be you, and redirect text messages to a different sim card. It's called SIM Swapping, it's easy to do and pretty common.

    - What you should be using is an authentication app. These apps are constantly generating random codes. The codes are only active for a minute or so before changing.
    - When you use an authentication app for 2 factor, you will be asked to enter the code from the app rather than from a text message. Set up is simple but a lil time consuming if you have a lot of accounts. Some sites still require text based 2 factor, so there's nothing you can do about it. **Google Authenticator** is reliable and available for both iPhone and Android. Remember to remove your phone number as an option for 2 factor when setting up an authentication app.

- ❖ Password protect your SIM card. Every major cell provider gives you this option.
    - On AT&T, you can set up a “wireless passcode” that’s four to eight digits long by going to your profile, then Sign-in info, then Get a new passcode. You should also add what the carrier calls “extra security,” which just means it’ll require the passcode to manage your account online or in a retail store. You can find that by going again to Sign-in info, then Wireless passcode, and checking Manage extra security.
    - Verizon actually requires a PIN, but to set yours up or change it, head to this site, then sign into your account. Enter the PIN of your choice twice, click Submit, and you’re done.
    - For T-Mobile, you have to call instead; dial 611 from your mobile phone and ask to add “Port Validation” to your account, which lets you choose a six to 15 digit PIN.
    - On Sprint, sign into your account, click on My Sprint, then go to Profile and security. Scroll to Security information, and update your PIN there.

Internet browsers and web trackers

You are constantly being tracked. Internet service providers can see what you’re doing, and advertisers are tracking you across every app you open and every website you visit. You are a commodity, the data you are constantly creating is being used to create an ad profile of you. These advertisers likely know you better than you know yourself. Luckily there are several tools to help you fight this.

- ❖ Use a safe internet browser and clear history/cookies often. To keep things simple, stop using chrome.
    - If you are an iPhone/mac user, you’ll be fine with safari.
    - Android users, switch to Firefox.
    - All browsers give you the option clear history, cookies, active logins, etc. Do this once a month at the very least.
- ❖ When browsing the web on a PC, I highly recommend **Firefox** as your browser. It automatically blocks most trackers and gives you 3 great options for security. There are other safe browsers, but I am biased. Using Firefox alongside specific addons will give you an even safer experience. Here are a few that don’t require maintenance:

- Decentraleyes
- Facebook Container
- HTTPS Everywhere
- UBlock Origins

VPNs and app trackers

There are other ways to stop trackers while also hiding your internet activity. VPNs route your traffic through random private networks that can't be traced by anyone without a lot of time, money, and computing resources on their hands. It even prevents your internet provider from tracking you. Your VPN service also masks your real location because you are given the option to choose from servers in any country. You've probably done this to watch location specific content.

- ❖ Buy a VPN. Free VPNs aren't exactly safe and rely on user data to be free. So, it's almost counter intuitive when it comes to these things. It's also worth noting that you'd want your VPN to work on your phone as well. I recommend **Mullvad**. It's cheap, secure, and has apps for both android and iPhone.

App trackers work the same way web trackers do, except they live in your phone and follow you from app to app. That info is being collected and organized into an ad profile specifically targeting you. It may seem like certain apps are using the mic to listen to you, but what's really happening is your every move is being traced and recorded. Mobile firewalls will block these trackers from following you around on your phone.

- ❖ iPhone has several tracker blocking apps, but I recommend **Lockdown.** It's free with a paid option.

- ❖ I don't have much experience with Android, but I hear **Blokada** is a great tracker and ad blocking app

Miscellaneous apps

I have all these apps on my phone and they work well together and require little maintenance

- ❖ **Malwarebytes** blocks ads and spam texts. The paid option blocks spam sites on you web browser and prevents spam calls. It is available for both Android and iPhone

- **Fing** allows you to monitor your WIFI connection and see what is connected to it. You can set restrictions, remove devices, test speeds, and more. Its available for both Android and iPhone

- **Jumbo** scans multiple social media apps and Gmail and then fixes privacy settings automatically. It deletes old posts from multiple services, block ads and trackers, reduces spam calls, and a lot more. I highly recommend this app. It's extremely easy to use and feature packed. It has a couple affordable paid options and is available for both Android and iPhone

Social media and Google

Odd are, it's social media sites and search engines doing most of the tracking. Specifically, Facebook and Google. Their entire business models are based on collecting information and selling it to advertisers. Luckily these companies have been called out so many times that they now have extensive privacy settings. This will probably be the most time-consuming task because of these settings.

- **Snapchat**
  - Change your password
  - Disconnect the app from your contacts
  - Remove your phone number
  - Set up 2 factor verification with an authenticator app
  - Make sure your email is correct
  - Go thru "connected apps" and remove what you don't recognize
  - Go into "manage" and turn off all ad preferences
  - In "manage", go to "maps" and turn off "share usage data"
  - In "manage", double check your contacts settings
  - Under "who can", review and adjust what people can see
  - At the very bottom of settings, clear whatever cache feels necessary

- **Twitter**
  - Change your password
  - Turn off photo tagging
  - Delete old tweets that feel necessary
  - Turn off "precise location"
  - Turn off "personalization and data"
  - Add 2 factor authentication using an app
  - Turn on password reset protect
  - Review "apps and sessions" and remove what is necessary

❖ **Instagram**

- Change your password
- Turn off “activity status”
- Review “login activity”
- Add 2 factor authentication using an app
- Review “apps and websites”
- Clear search history

❖ **Facebook *I’m doing this through the app***

Starting at “setttings”

- Make sure your email is correct
- Remove your phone number
- Turn off “upload contacts”

Now under “security”

- Review “where you’re logged in”
- Change your password
- Add 2 factor authentication using an app
- Review “authorized logins”
- Turn on “get alerts about unrecognized logins”
- Turn off both location settings
- View your location history and delete all of it
- Review “apps and websites”

Now under “privacy”

- Go thru “check a few important settings” and change things to your liking
- Make sure people can’t search for you using your email and phone number. Set these to “only me”
- Under “do you want search engines outside of fakebook to link to your profile?” set it to no
- Turn off facial recognition
- In “public posts” change what you want
- Turn off “activity status”

*The next settings require you to be on the **desktop version** of Facebook through **Firefox***

So, Facebook is really good at tracking you. They take all your data and turn it into incredibly accurate profiles. The data points they collect on you are officially called “interests” and “behaviors”. Its creepy how accurate these profiles can be

- Download the addon **Facebook Advert Interest Cleaner**
- Log into Facebook
- Now go to this link: https://www.facebook.com/ads/preferences
- Near the top of the page you will see the addon you just downloaded
- Click “remove all interests from visible interest tabs”
- This will take a minute so just wait and watch
- Once its over click on the “more tab”
- You will see about 8 more tabs of interests that the addon didn’t delete
- You will have to go through these and delete every one of them individually
- Do this once every few months

❖ **Google *I am doing this on the desktop version of Gmail***

Like Facebook, Google is excellent at tracking you. Make sure to review these settings on all Gmail accounts

- Through Gmail, click on the square of dots in the top right and then go to “account”

Starting at “personal info”

- Change your password
- Add a recovery email if you want
- Go to “about me” and change the settings to your liking

Now under “data and personalization”

- Go to “activity controls” and pause “Web & App activity” and “Location History”
- Pause YouTube history if you want
- Turn off “Ad Personalization”
- In “My Activity” try and delete every single day of records.
- Review “my timeline” and delete history

Now under “Security”

- Turn on 2 factor authentication using your phone number
- Change 2 factor to google authenticator
- Now remove your phone number
- Review “recent security activity”
- Review “Your devices”

Now under "People and Sharing:

- Turn off "contact info from your devices"
- Turn off "Share recommendations in ads"

***That's about it when it comes to basic online security. I practice all the steps listed above alongside the steps below*:**

- ❖ Separate email accounts
  - I have multiple Gmail accounts for specific things like shopping, streaming, banking, social media, and a few others

  - For my more sensitive email accounts, I use **Protonmail**. Which is an encrypted email platform.

- ❖ Physical 2 factor authentication
  - On top of google authenticator, I also use a physical key for 2 step verification. Instead of a text message or authentication app, I plug this key into the USB port while logging in and I am granted access

  - Physical keys are the safest form of 2 factor authentication. I recommend **Yubikey**. Especially one with NFC.

- ❖ Data broker sites
  - Google your name. Odds are the first page will be nothing but random sites filled with your personal information. All the data that is collected from you, ends up in these people finder sites. There are tons of them and the chances that your info is on 50+ of these sites are high

  - I am currently paying for a service that scrapes the internet of your information and then removes it. Its 15 bucks a month but you can stop your subscription once it's done.
  - Go to www.onerep.com and type your name in. It will find and list every website your information is on. From there you can set up an account. I've had my account for about 3 weeks now and its removed my info from around 20 of 60 sites it discovered.

- Obfuscation
  - Obfuscation is a lil different than traditional online security. The idea is to create internet “noise” with the intent to confuse advertisers.

  - When you spend time on a particular thing online, that information is collected and added to your ad profile. Your searches, activities, and the time spent on these activities are all vital information. By drowning out this information with false internet activity and interests, you will make your ad profile less accurate and therefore, more private and less intrusive. There are a couple **Firefox addons** that will do this for you:

  - **TrackMeNot** automatically generates random searches and sits on them for a period of time. I have mine set to generate a random internet search every 10 minutes. By doing so, its filling my ad profile with what looks like genuine interests.

  - **Ad nauseum** is another addon that will automatically click on every ad that it detects. Whether it’s a popup, in the background, or active on a webpage, Ad nauseum will click on every single ad. Furthering the inaccuracy of your ad profile.