Privacy Recommendations

- Several hours of days of researching have been invested to find the best possible measures to defend & secure the common citizens' data privacy and freedom. These measures are aimed to deter data-mining corporations like Google Inc., Facebook & Apple Inc. or any other web site or service that aims to collect, store or sell your personal information.
- Although my suggestions are well-researched, you should always do supplementary research & make judgments about what measures you want to use to defend your privacy.

Minimum recommended measures for a common citizen :

- These measures are super user-friendly.

1. **VPN** : NordVPN
   - This is the most important measure that I could recommend. The function of a VPN is to change your “IP Address”. In other words, change your reported virtual location automatically, 24/7. Keep in mind that this is not the same as your phones given geographical location via built-in GPS, which is an inevitable function of Bluetooth.
   - There are free VPN services out there, but this measure is something worth paying for in my opinion. It is also the only recommended measure on this document that would require a paid subscription for basic use. A paid VPN is the best VPN.
   - IMPORTANT : In order for apps & websites to cooperate with your VPN usage, you need to follow these easy steps after you have installed NordVPN :

- open NordVPN > Settings > Disable “CyberSec”.
- open NordVPN > Settings > VPN Protocol > select “OpenVPN (TCP)”

2. **Web Browser** : FireFox (compared to Chrome & Safari).
   - Use Tor Web Browser if you want something that I would consider to be a step higher. Tor is also not offered on mobile, only desktop.

3. **Search Engine** : DuckDuckGo.com (compared to google.com). A beautiful resource that was made solely to protect your web search privacy.

4. **Map Navigation** : Magic Earth (compared to Google Maps & Apple Maps). Strong dedication to your privacy.

- **Note-Taking** : Some of you all keep your most sacred passwords, thoughts & personal information are kept in digital note form. Always use encryption features.

- Option 1 : Apple Notes

  This is the default note-taker service offered by Apple, but only private when used with their built-in encryption feature).

- Option 2 : Standard Notes (Apple or Android).

Measures that can require more time & effort but are honestly just as important:

NOTE : Utilizing these measures requires minimum time, effort & skill BUT actually detaching/discontinuing from your current email & cloud service(s) is hugely important in the world of digital privacy, and hugely important measures take more time & effort on your behalf.

NOTE : Your common email services & cloud services are widely subject to privacy invasion from the common service provider. It's suggested to use a servicer that respects privacy & security. I can almost guarantee that your current servicer does not.

1. **Email** : ProtonMail (or another email service that has optional outgoing end-to-end (E2E) encryption capability).

   - ProtonMail encrypts your emails as soon as you receive them so that only you can see them as if there was no encryption. The service provider - Proton Technologies AG cannot even view your emails.

2. **Cloud Service** :
   - I do not recommend that you use any cloud service as every aspect of your life is stored on the provider servers. if you must use a cloud service, use a privacy-respecting cloud service, like MEGA Cloud.

Other Recommended Measures :

1. **Private Text/Video Chat** : Signal Private Messenger
   - You don't have to use this for EVERY conversation with EVERYBODY, but if you feel that you need to discuss some private/personal then use this service.

2. **Two Factor Authentication (2FA)** : Authy
   - Use this third party 2FA service, instead of having a code sent to your phone.

Tips :

1. Decrease use of social media. This is not only for privacy but because we literally just need to stop using social media so much.
   If you willing, deactivate accounts that you feel the need to withdraw from.
   Facebook is the main concern for most.

2. Go through every single application that you use on your phone (and other devices). See if two-factor authentication (2FA) is offered. Enable 2FA, especially with banking apps. Use Authy if a third-party authenticator is an option for 2FA (compared to opting to receive codes via phone text in order to confirm your identity).

3. Go through every single application that you use & skim through the privacy settings to see what data-mining that you can reduce on the services behalf. This includes app that you don't suspect to invade your privacy. In other words, if an app settings offer an option for you to disable/discontinue certain personal data information collection then opt-out/disable or consider not using the service anymore if they would not like to respect your data privacy.

4. If you use WhatsApp for end-to-end (E2E) encrypted text/video chats... delete your chats, disable your account & delete the app. Google owns the rights to WhatsApp & stores your conversation data via Google Drive (their servers) & can plainly see your conversations. Use Signal Private Messenger App.

5. If you use YouTube, delete your account. It is okay to still use YouTube, just don't hold an account. This means that you can't subscribe to channels or have your own channel.
   - Ridding of your YouTube account is a huge step for some of you, but Google now owns this service & collects every single aspect of your interests and sells your private information.

6. Use Reddit to ask your many virtual questions in life. Follow interesting channels like r/doge! Don't ask your questions on google.com or mainstream social media.

Message me on Reddit with any questions!
u/macrohumanity

All progress starts when someone has a little extra time on their hands. This can be so defining for their themselves & society.