ΔUPGRADABLE

Upgrade Program Privacy Plan

Table of Contents

Introduction 2

Epistemic Status 2

Objectives 2

Metrics 2

Values 3

Value Analysis 3

Strategies 3

Actions 4

Schedule 5

Predictions 5

Outcomes 5

Assessments 6

Tools 6

Resources 6

Notes 7

Legal 7

Introduction

This document is part of a series of upgrade plans for every area of your life. It's broadly designed for a single, middle-class, 30-something living in a major city in a developed country.

Please go to "File" > "Make a copy" and make a copy of it for yourself. Then fill it out section by section according to your particular needs and circumstances. Perhaps add sections or items, delete them, change the order, and so on.

Your aim should be to make the plan as applicable and useful to you as possible. You should not follow the plan blindly–think it through for yourself.

Note that this process might be challenging. You might need to teach yourself things you aren't very knowledgeable about yet. You might feel like you need to do preliminary work in a different life area first. That's okay. Figure out broadly what makes sense for you, operationalize that understanding as specific actions in the Actions section, and then do them.

If it feels overwhelming, just start with the parts you find most valuable and do what you can. Tackle the rest over time. It may also help to set aside a dedicated day to work exclusively on this by yourself or with friends. Or you may choose to enlist an UP Coach to co-design and execute this plan alongside you.

Epistemic Status

This is an overview of how confident the principal author is in this plan.

- Generally moderate confidence in this plan
- Based on 20+ years of experience carefully protecting my personal privacy, 30+ hours of research on privacy threats and protections for self and clients, and first-hand experience of having my privacy compromised by a stalker intent on violence and slander

Objectives

Decide what objectives you have with this plan and rank them in order of importance. Below are some sample objectives.

1. Protect personal and professional information
2. Ensure dignity, safety, and self-determination
3. Maintain desired social boundaries

Metrics

Decide what metrics you will use to evaluate the effectiveness of this plan. Also include the frequency in which you'll evaluate those metrics. For example, ad hoc, once, hourly, daily, weekly, monthly, quarterly, annually or per decade. Below are some sample metrics.

- Privacy Rating: How would you rate your privacy, on a 1-10 scale?
- Number of Search Hits for [Name]
- Number of Online Profiles
- Annual Number of Hacks
- Annual Number of Scams
- Number of Known Security Threats
- Estimated Number of Unknown Security Threats

Values

List all of your relevant values and rank them in order of importance. Below are some sample values.

1. Privacy
2. Safety
3. Freedom
4. Dignity
5. Trust

Value Analysis

List and then analyze all of the costs and benefits of this plan. Potentially also estimate expected value and/or return on investment. Below is a sample value analysis.

- Time costs: 1 - 250 hours
- Financial costs: $0 - $10,000 dollars (e.g., professional security audit, brand manager, computer hardware and software, secondary phones, etc.)
- Benefits: $X in potentially extremely large objective and subjective benefits in reducing privacy risks (e.g., blackmail, extortion, stalking, personal data leaks, compromised passwords, etc.)

Strategies

Decide on your high-level strategies for achieving your objectives. Below are some sample strategies.

Key People

- Do the work on your own
- Outsource some or most of the work to experts (e.g., professional security analysts, etc.)
- Outsource some or most of the work to assistants

Actions

List the specific actions you will take to achieve your objectives. You should add these tasks to your project management system unless you are choosing to do them now. Below is an example sequence of actions you might take.

One Time

1. Describe your mental model of privacy
    a. Create a visual representation of it from memory without referencing this plan or outside sources of information
    b. Create a new visual representation after thoroughly studying this plan and any relevant sources of information
    c. Pay special attention to the improvements in the second version as incorporating those new insights may be crucial to the success of your plan
2. Finish every section of this plan, including the assessments, tools, and resources below
3. Create a list of all of your digital devices
4. Set up two-factor authentication apps for your major services on all of your digital devices
5. Ensure all of your accounts have strong passwords through a password manager (e.g., LastPass)
6. Ask your wireless provider to require a PIN to access your account(s)
7. Set your devices to automatically lock after a lack of use
8. Ensure your devices do not have unnecessarily large amounts of private data or apps on them; remove whatever isn't regularly used
9. Minimize app permissions on your devices to only what is necessary
10. Ensure your devices are regularly scanning for security threats
    a. Android: Settings -> Security -> Google Play Protect -> Scan device for security threats
11. Set up a remote tracking and wipe tool on your devices (e.g., Prey)
12. Consider encrypting your devices
13. Consider using Google's Advanced Protection Program

14. Consider creating a pseudonym or stage name and solely use that in public settings

Ongoing

15. Consider using a privacy-focused browser for internet searches (e.g., Tor, Brave, etc.)
16. Always keep your operating systems up to date
17. Stay up-to-date on scam warnings from your bank, insurance company, or any other financial institution you use
18. Use a trusted antivirus and ensure its virus definitions are up to date
19. Use a trusted VPN at all times
    a. Potentially set up a personal server for this
20. Avoid public wifi whenever possible. Use data from your mobile hotspot
21. Avoid using public charging stations whenever possible
22. Keep your physical addresses, email address, mobile phone numbers, and other personal information private insofar as possible
    a. Consider using a burner number (e.g., Burner)
23. Use spam filters for your email
24. Always be vigilant against spam and phishing attempts through email, phone, and text
25. Always be vigilant when downloading programs and mobile apps onto any of your devices
26. Remove unnecessary apps from your devices regularly
27. Have a full security audit by a professional on a regular basis (e.g., once every five years)

Schedule

Decide on which days you will take which actions. You should add these dates to your calendar now.

- [Date]: Finalize plan
- [Dates]: Execute plan
- [Dates]: Review plan's outcomes

Predictions

Predict how well you will do in achieving your objectives.

- [Name]: I predict with [X]% confidence that I will [Y] by [Z].
- [Team Member's Name]: I predict with [X]% confidence that [Name] will [Y] by [Z].
- [Team Member's Name]: I predict with [X]% confidence that [Name] will [Y] by [Z].

- Combined: We predict with an average [X]% confidence that [Name] will [Y] by [Z].

Outcomes

Objectively record how well you achieved your objectives.

- [Date #1]: [Outcomes]
- [Date #2]: [Outcomes]
- [Date #3]: [Outcomes]
- [Date #4]: [Outcomes]
- [Date #5]: [Outcomes]
- [Date #6]: [Outcomes]
- [Date #7]: [Outcomes]
- [Date #8]: [Outcomes]
- [Date #9]: [Outcomes]
- [Date #10]: [Outcomes]

Assessments

List all of the assessments you might take to understand how you're doing compared to your objectives.

-
-
-

Tools

List all of the tools you might use to achieve your objectives. Below are some sample tools.

- Avg
- Aura
- Avira
- Brave
- Burner
- CCleaner
- Client Access License (CAL)
- CrookCatcher
- DuckDuckGo
- ExpressVPN
- FlyVPN
- Google's Advanced Protection Program
- Kaspersky
- McAfee

- NextDNS
- Nomorobo
- NordVPN
- Pseudonym
- Secure VPN
- Titan Security Key
- Tor
- VPN
- YubiKey

Resources

List all of the resources you might use to achieve your objectives. Below is a sample resource.

- Security List
- Tech Independence

Notes

Add any random thoughts, questions, uncertainties, etc.

-
-
-

Legal

- We do not profit off any product recommendations.
- We declare no conflicts of interest.
- This document is not for commercial re-use.
- This document is intended only for the person it was shared with.
- Please do not share with others.