Privacy and Security Suggestions

Coolio

coolio.one

Preface

These suggestions were written with desktops in mind. I am not knowledgable on mobile devices. These suggestions are not permanent and are subject to change. I will listen to all honest criticism and if you have a critique/suggestion for this document, please contact me at one of my contacts at https://coolio.one/contact/

1. Search Engine

You should try to avoid search engines as much as you practically can. But when you have to use one, the best option in my opinion is to use searx. If you don't want to self-host it you can use an insance from https://searx.space.

2. Browser

Tor Browser ideally as it routes all of your traffic through Tor network.[1] Using Brave is a good option as well. Avoid Firefox and especially browsers based off of Firefox (With an exception being Tor Browser) as Firefox's security is very lacking as of writing this document and browsers such as Pale Moon and Waterfox have it even worse.

2.1. Elaboration on Tor Browser and other options to access Tor

The most anonymous way to access Tor is to use the operating system known as Tails.[2] However, you are not supposed to use it as a general use desktop OS, it's only for Tor usage. I personally just use Tor Browser as it is much more convienent but still a good option. I would highly recommend against using Brave's Tor mode, as in terms of anonyminity, you stick out like a sore thumb as not nearly as many people use Brave over Tor as Tails/Tor Browser and the Brave browser is severely lacking in fingerprint protection compared to Tor Browser. Using Brave over Tor *is* better for anonymity than just using a browser withour Tor but when Tor Browser is an option for a similar level of convienence, I don't see a reason to use Brave's Tor mode.

3. Operating System

Windows is lacking in terms of privacy[3], however, a significant portion of the tracking can be disabled/removed. Windows 10 is significantly better in the security department than Linux. Qubes OS is a good option for security and privacy. Avoid versions of Windows that don't receive security updates any more like the plague (ie Windows 7/Vista/XP). An antivirus **cannot** fix security issues that result from not receiving updates.

Certain distributions of Linux are good in terms of privacy, but as stated earlier are not good in terms of security.[4]

4. Email Providers

Email is inherently insecure[5] and should be avoided as much as possible. However, it is unrealistic to assume that you can completely ditch it. Protonmail and Tutanota have a good track record and encrypt messages sent between their own respective domains. Self-hosting is also an option but that is difficult and typically has worse security than the email providers previously mentioned unless you really know what you're doing. For an email client, there isn't really a 'best one' as long as you're using one that is free as in

freedom and supports your email provider. I use Thunderbird and it works fine for me.

4.1. Alternative messaging protocols

There are many significantly better options than email. I find Matrix, Signal and XMPP to all be secure options. Signal is the most novice-friendly out of the three but requires a phone number. Matrix is what I personally use the most out of these three and is quite novice-friendly in my opinion. XMPP is by far the hardest to use and set up and I wouldn't recommend it for most people. All three of the options mentioned use end-to-end encryption.

5. OpenPGP Introduction

A modern and effective solution of encrypting messages (or anything, really) is PGP, specifically OpenPGP. Essentially, with a PGP certificate (You can think of it like an account that doesn't require signing up anywhere online) you are given a private key and a public key. You *never* want to share your private key with anybody, as that is what's used to decrypt messages that you receive. However, you should share your public key with people who you want to send you encrypted text. It is completely safe to publicly share your public key. Your public key is what the sender (encryptor, I suppose) uses to encrypt text they want you to decrypt and see. If they do not have your public key, then they cannot send you and only you an encrypted message.

Every email client worth its weight in sand (Thunderbird, KMail, Evolution, etc.) supports adding your PGP key to it to automatically encrypt and decrypt emails. This makes sending emails very secure if the messages are encrypted. There are public key directories that you can attach to your email if you want people to be easily able to find your public key to send you encrypted messages. You can also attach your public key file to emails you send (Some email clients like the ones listed previously allow you to automatically do this) to let the receiver know what your public key is.

5.1. Kleopatra Guide

The OpenPGP certificate manager (Think of it as a client) that I use is Kleopatra, and I am a big fan of it. It is quite intuitive, runs well, and has lots of useful features. Here is how to set it up:

Bibliography

[1] http://www.webupd8.org/2013/12/tor-browser-bundle-ubuntu-ppa.html

[2] https://tails.boum.org/

[3] https://www.groovypost.com/unplugged/how-much-does-windows-10-spy-on-you/

[4] https://madaidans.insecurities.github.io/

[5] https://www.jdfoxmicro.com/resource-center/articles/email-is-insecure/