Privacy and Information Toolkit

A guide to digital and personal freedom and how to beat the lies of omission by the Mockingbird Media and Big Tech

"Shifting the Tech Paradigm"

-September, 2022 Edition-

"Of all tyrannies, a tyranny sincerely exercised for the good of its victims may be the most oppressive. It would be better to live under robber barons than under omnipotent moral busybodies. The robber baron's cruelty may sometimes sleep, his cupidity may at some point be satiated; but those who torment us for our own good will torment us without end for they do so with the approval of their own conscience."

— C. S. Lewis

Version 22.09


ONE STEP AT A TIME...

IN THIS GUIDE

Forward

”End the digital oppression”

toolkit@privacy:~$ In this guide, I offer the more useful bits of tech that I’ve learned along my own privacy and technology journey, my purpose is that while it is still relatively new in my head, I share this information in this stage to hopefully better serve those who were like me in the not so distant past, thinking that the tech is too far advanced for a ‘tech-normie’ to even bother attempting to learn. Easily are we defeated mentally when we see the scope and the depth of capability of our modern phones and computers, and the powerful technology behind the apps and products we use. However, I’ve found that most of these topics that I present are actually not all that difficult to adopt or figure out, in short time I think you’ll find many of these both relatively easy to use, as well as quite useful. In addition, you will drastically improve your privacy, peace of mind, and perhaps most importantly for the big picture, deprive big tech of much of your data, which I will discuss shortly. The guide is aimed towards those that may not be very skilled in using tech, but know that they are being watched and recorded, and don’t know what to do about it, or where to start. None of us are going to toss our phone in a lake and go live in a high mountain cave, as nice as that sounds some days… instead, I cover some basic entry points into a more private way of doing your daily tasks online.
This is not a read cover to cover type of presentation, nor would I expect anyone to do so in some checklist type fashion, take each section one at a time and employ the various tools as you can apply them to your situation. Most of these topics as presented are not comprehensive, so do your own research into each of the topics I discuss. There is no particular set order to these sections, however my general advice is to read over the guide bit by bit, and start doing the easy stuff as you go, if I had to pick just a few to start with, it would be creating a Password Manager file, set up a VPN service, get yourself a Proton Mail account and start using some of the various apps such as Signal for your calls and text messaging. Those simple steps will go a long way to secure your digital life.

This guide is written in response to the digital takeover of our private lives that I’ve witnessed in the past two decades, a digital tyranny that has been installed not quite by force, but by all of us ignoring our technology for too long. Not knowing what lives in the hidden code of the products and apps we use. Little by little, then all of a sudden; that is how tyranny happens in history, and I see that in real time now in our rapidly expanding technocracy. Why would we use or allow such pervasive digital infrastructure to manipulate the world we interface with through small pieces of glass every waking moment? My own belief is rooted in the observation that humans by nature are fundamentally lazy. Mostly by design, we are hard wired to preserve precious calories to rest until we gather our next feast. In our modern days we live in arguably the best human existence ever known with little such need to struggle to survive; and yet an existence that is quickly changing our lives for the worse in many ways as the few control the masses with increasingly potent ability to track and analyze nearly everything that we do and say (and with that information, also shape our behaviors.) Secondly, most of us are also very busy, and don’t have a lot of time to really think about the devices and apps we use.

toolkit@privacy:~$ Data is the new coin of the realm. Data becomes power. Microsoft, Apple, Google, Amazon, Facebook and Twitter, and many others have become more powerful and pervasive than anything even in George Orwell's novel '1984.' We are on a runaway train speeding towards the abyss of digital totalitarianism, **Dr Robert Malone** has put it best I think:

"Global Totalitarianism is here, it just hasn't been equally distributed yet."

I'd like to go back to the state we were in around 2005 and "rip the knob off."
While the United States has arguably the best footing to resist a global, and digital control system, we see what lies ahead with the push to have our government hold central control over virtually every aspect of our lives. Vaxports, or Central digital currency for example, allows the controller to freeze anyone's assets, or perhaps regulate anything they wish. Think shortages, let's say there is a shortage of baby formula, what's to stop a central authority from limiting you to purchasing only X amount of formula containers per month if that's the only payment method in use? In a centralized digital, cashless society, freedom becomes history. Cash is never coming back, but we can still demand **decentralized** and **open source** transparency in our new digital age.

CENTRALIZED and CLOSED SOURCE → DECENTRALIZED and OPEN SOURCE

Shift the tech paradigm, towards decentralized and fully transparent, (open source) software.

For a brief background on myself, I spent twenty years in the US Army as a Special Forces Medical Sergeant, with extensive travel to other countries. That time and travel cemented the fact that the US is truly the last bastion of anything resembling a free nation. Reagan famously said, and I firmly believe,

"If we lose freedom here, there is no place to escape to. This is the last stand on earth."

In this guide, I hope to help those who are unaware, apathetic, or otherwise disinterested, to take the effort and take a stand to defend your freedom, and for the freedom of our next generations, digital is here to stay. We must learn how to use technology to stay in the fight.

We must *change the paradigm* related to all aspects of our digital lives. Blind trust in Silicone Valley tech companies is gone forever. Moving forward, we must push towards decentralization, and open source code software (later I'll discuss the concept of FOSS, free and open source software) in as many areas of our lives as we can. If we give in to a CBDC (Centralized Bank Digital Currency) we will be controlled like puppets on a string by our digital masters. Even more accurately, we will be like ants in the backyard, with tech oligarchs being the humans trampling us, unaware of how many of us they squish beneath their feet as they enjoy a fine barbeque. If we allow for closed source, black box software for things like voting machines, we never know if the tabulation is correct, and not corrupted. We don't see the ridiculous algorithms running on our social media feeds, shaping what thoughts are 'Party approved or disapproved' through shadow banning, censorship, or outright bans. Inability to speak freely.

toolkit@privacy:~$ When big tech scans our cloud drives, scans and saves every word and attachment of our email conversations and every text message, we give them the power to predict and control our very thoughts and behavior. (Typing text into a Microsoft Word document now underlines what I mockingly call ‘Purple Wrongthink’ text with purple, suggesting what you are typing is ‘intolerant’ or ‘offensive.’ If you type ‘Policeman’ it will suggest ‘Law Enforcement’ or ‘Police Person’ to be more tolerant...)
I refuse to allow that type of brow beating, censorship and abuse to shape my thoughts and actions, as a born free human being. Throughout this guide, I will share some of my strategies and applications that shift and improve the paradigm of the tech that we use.

The Digital Gulag

You can ignore reality, but you cannot escape the consequences of ignoring reality. What if you were free to leave your home, but your payment methods were only accepted within a 10 mile radius of your address, you know, just for 15 days, to slow the spread? What if your SIM card or internet was shut off until you took an injection (or four) that you don’t want? (That actually happened in some countries) With license plate readers all over our highways, what if you were told to stay within 50 mile radius of your ‘approved residence’ but a plate reader detects your license plate outside of that arbitrary limit? With CBDC especially, a fine could be extracted from your account automatically, without even an human intervention. Camera software has become advanced enough to where it can be programmed to recognize certain people and even objects, such as presence of a firearm, to send alerts out in real time to an authority. There are few places left in public that are not captured on camera anymore. Your cell phone further adds to tracking where you go, and who you associate with, keeping accurate logs of activity. While this paints a hopeless picture, the contents of this guide, and having general awareness and interest, can take us a good ways in a better direction, and out of the big tech ‘commercial kill chute’ created for us.

“The price of liberty is eternal vigilance.” -Jefferson

We are at an inflection moment in history no doubt, it’s time to get interested in shifting the tech paradigm towards decentralization and open source code. Whether or not you are interested in technology, technology is *very* interested in you and your data.

Why Privacy?

Shifting the Tech Paradigm

toolkit@privacy:~$ **“I don’t have anything to hide”** is the the most common phrase I hear when discussing digital privacy. I uttered similar thoughts when the Patriot Act was enacted, I thought, “I don’t talk to terrorists, so who cares, it may catch bad guys?” Foolish in hindsight of course. Fast forward to an age where the average person has three cameras on their phone, one on each TV and laptop, and microphones scattered throughout our IoT (Internet of Things) in our homes and vehicles. Who gets that data? What is being done with that data? Could that data be used to not only predict, but to perhaps shape our behavior? Think about the possibilities, if you installed various sensors including cameras, mics, GPS, accelerometers in a person’s home, vehicle and a device that they carried with them everywhere, do you think that after some time you could gather powerful data to exploit that person? Think beyond marketing, think of the pattern of life and habits you would discover. Where and when each family member works. How fast they drive, how hard they brake. What TV channels or radio stations, which movies and songs do they like. How often do they forget to lock their car or front door at night. Spending habits and trends. What if an insurance company paid for that data? How about a lender, to learn how likely it is that the person pays back the loan? Perhaps the government would pay for information about your driving, such as speeding, or driving too many miles in a month.

toolkit@privacy:~$ Maybe one day they would like to also know how much money you spend on meat, or ammunition, or any other category of goods? Would the government seek to one day limit your consumption of alcohol or certain types of food? Or would you be denied life insurance or certain medical care after they discover you don't buy enough vegetables, and don't purchase enough toothpaste, and buy too many energy drinks? Maybe you are not denied insurance, but what do you think your price would be if they knew more about you?
Through the power of data and analytics, we can see quickly how this information can be abused for the good of its masters, and for the detriment of those who are forced to live under those masters, in whatever way they want us to live and behave. Increasingly we see the world being built for us is a 'you will buy everything in a subscription model,' rather than ownership.
Also it is important to understand that privacy and freedom are not end states, nor achievements, but rather an ongoing state of being, hopefully being improved and practiced continuously. Like anything else we do, it becomes habit eventually, to find ways to mitigate the data we give up willingly. You don't have to live in a cave to shut down much of the data you give over, there are some easy button solutions to use. Each step we take to learn how to preserve privacy I believe compounds, and pays dividends. A small change now can reap much more meaningful gains in the future, by shaping the way we think about the tech that we are using. Once you get used to using encrypted messaging apps, sending regular text messages just feels… wrong. And intrusive. The same goes for Operating Systems, once you use and realize open source OS's don't spy on you, it feels wrong and intrusive to go back to a Windows or macOS product.

In the upcoming sections, I will walk you through some basic entry point topics, each one has many rabbit holes you can choose to go down as you get time to do so. By employing these techniques and later building on them, I believe you will live a more satisfied digital existence, by reducing the leak of your valuable data, and you will discover new ways of using your phones and computers to make them work for you more, and the monopolies less. You help shift the tech paradigm of today, into a more free and private existence for your future and well being. The more individuals that refuse to use closed source spyware products, the less influence those closed source product companies has over all of us.

As I'm finishing editing this August version of this guide, a story just dropped about a father losing his entire Google email and online file storage after taking a picture of his child for a medical reason to send to their doctor; only to have Google's AI flag his content as CSAM (child sexual abuse material) and delete all of his digital life with Google, as well as have an investigation opened up on him. Granted, law enforcement quickly realized that he was not distributing illegal content, but tried to contact him with no success. They did close the case, but Google refused to restore his account still. Currently he is working with law enforcement to try and recover his entire email and phone contact list, and personal pictures and files. This teaches us to dump big tech and instead-using open source, privacy respecting products would have prevented this entirely, and saved this family a huge headache. Is catching child abusers a great thing? Absolutely. Does anyone think that they have already caught on to not use Apple or Google products to distribute illegal materials?

toolkit@privacy:~$ (cont'd) Criminals will always find a way to do their thing, this doesn't mean we have to give up our own valuable privacy, and have our lives upended.
Story:
https://dailycaller.com/2022/08/22/google-criminal-investigation-child-pornography-abuse-father-photos-son-doctor/

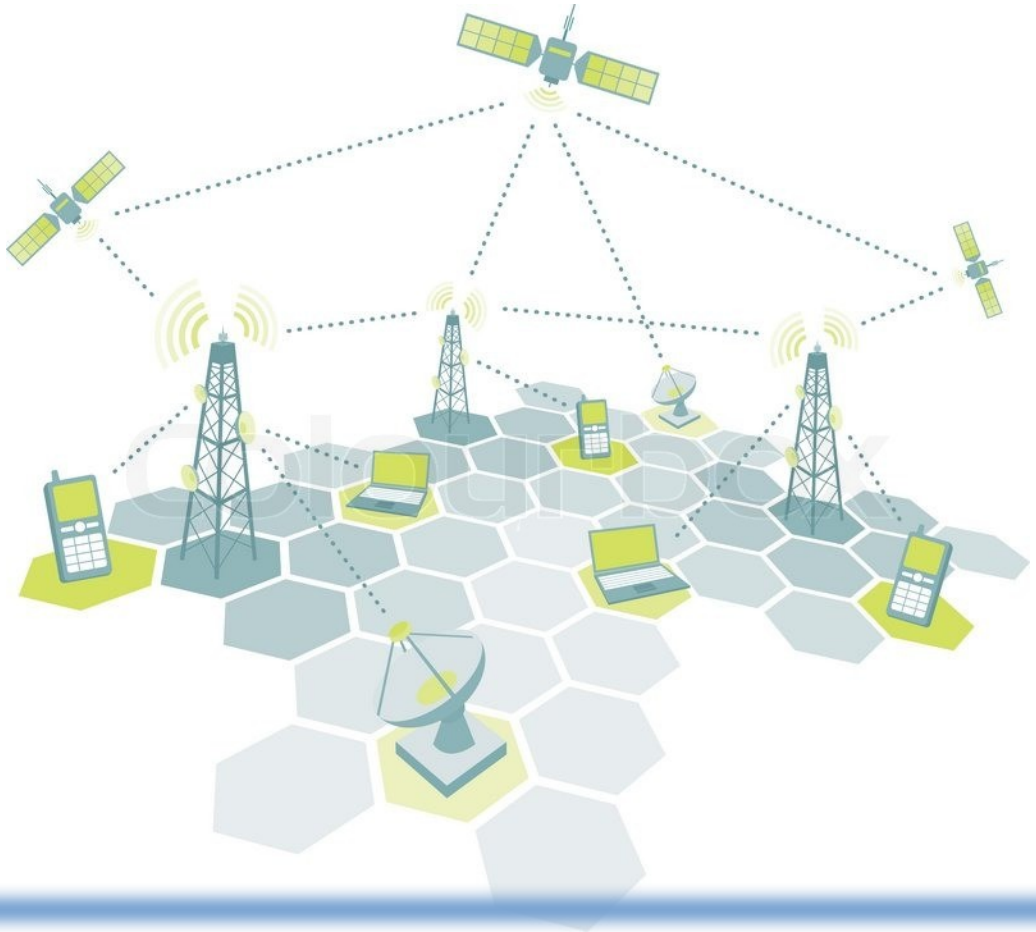
While privacy can cost money in some areas, most of the topics I discuss here are free, but some will require some cost. Hardware always costs money, but for not a lot of money, we can accomplish quite a bit of improvement. While I don't have any problem paying for a service that provides me value, I also don't hate my money, and I do not consent to any spying, collection or abuse of my data. Why pay for Microsoft Office subscriptions when I can use nearly identical software for free? In addition to free, it doesn't collect my keystrokes and other metadata or telemetry about me, for who knows what purpose.
We know the saying, "Power corrupts, absolute power corrupts absolutely." Being that data equals potential power, draw your own conclusions about who is in charge. (If you want to know who's in charge, determine who you are not allowed to criticize.) The last year has shown us the increasingly fluid relationship and almost a merger of big tech and our own federal government, with various agencies and authorities using big tech platforms to censor, artificially promote 'approved thought,' and outright abuse our data in ways that undeniably violate basic constitutional foundations.

Again, as I write this today, Facebook / Meta's Mark Zuckerburg **just admitted** on the worlds largest podcast, Joe Rogan Experience, that the FBI asked him to censor information related to a presidential candidate prior to an election. Is that democracy, or an abusive technocracy with their thumb on the scale? Was the true will of the people heard, with the government using powerful private companies to influence and shape the world we see? Jumping topics slightly, but same company, did you know that if you use Facebook, you have a 'Vaccine Hesitancy Score?' What other types of social credit-like scores do you have? Who has access to that information? Will that information be tied to your centralized bank digital currency in the future? Imagine instead of a three day suspension on social media for posting 'wrongthink,' your debit card doesn't work for three days after attending the wrong protest, or posting a certain political view. What good is freedom of speech, if the cost to exercise it is your freedom?
Another fundamental thing to consider is that privacy can be achieved by disassociating our identity with a product we use. While we may be giving tons of data up by using a Google app, if you don't use your true identity, then that data has far less meaning to it. While I prefer to use only open source products, the reality is that sometimes we need some of the closed source stuff from big tech. Give them only trash data by remaining anonymous.

Shift the tech paradigm. Read on to discover how I have done this in my own life, and be sure to share this guide with your circles of influence. If you have any feedback, or find any errors or updates to any of the material in this guide, you can send those to:

toolkit@graphenegoat.33mail.com

Public Enemy #1: Phones



Public Enemy #1: Phones

toolkit@privacy:~$ Before we launch into a way to defeat much of the tracking and data hoovering that's happening on your phone in the next pages, here is an excellent read. This article shows exactly how accurate your phone is being geolocated in real time as the device interacts with all kinds of signals as you move through various areas throughout your day:

https://cognitivecarbon.substack.com/p/about-those-patriot-phones?s=w

While the technology is impressive, it is also an obvious obliteration of privacy. Even with the phones that I discuss in this section, as secure as they are, still cannot avoid all of the tracking laid out in this article. However it does drastically reduce the information that hemorrhages from your average device by comparison, and although it's frequently referred to as a 'privacy' phone, it really is just what a phone should be-a phone where you can actually turn off location, microphone, camera, airplane mode, etc. Apple for example, uses your device in part of their mesh network of bluetooth, essentially making it a bot in their entire network of Apple devices, to support things like Air Tags, and to help locate other devices and relay information, regardless of whether you bluetooth is on or off, even with no cell or WiFi connection. Even with the phone off, Google and Apple can push software updates to your device, and collect location data still. Here is a short video with an example of location tracking of several Android devices. Note that not only can they track your location and movement, Google also differentiates among walking, riding in a vehicle, and public transit.

Google location tracking test

This massive surveillance data in the hands of a few big tech companies should be enough to frighten us with the possibilities of what can be done with that data, especially when we stop and think of who buys that data, and for what purpose. While you may not think you have anything to hide, big tech is making a ton of cash with your personal information and habits, location history, and using their profits to further entrench their abusive business model through marketing and information suppression to achieve a populace that is okay with constant spying and censorship of ideas and content. If your 'boring' information is being sold for a ton of money, what does that say about its value? We have a population that only knows about big tech options, and isn't even aware of other technology platforms that don't abuse us. I call this the corporate or psychological 'kill chute,' where you are funneled into only using big tech's products. In this section we will discuss some better options, rather than using Google, Apple, Microsoft, etc.

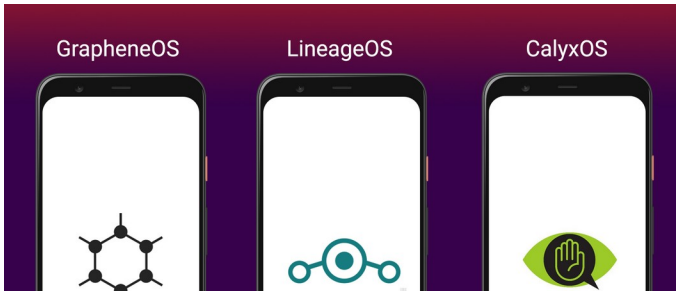
toolkit@privacy:~$ There are five Operating Systems (OS) in common use today: **Android, iPhone, Microsoft Windows, macOS and Linux.** Let's discuss the first two, our phones, in this section. Phones arguably are the biggest threat to our privacy due to several factors, one being that they have more sensors active on them than computers in general (more data to collect) although many people are using more and more advanced tablets and laptops, so that may be narrowing, but we as a society are using phones more than computers for many tasks, and we carry them with us almost everywhere. How many times a day do you get more than 50 feet away from your phone? Do you sleep with it in your bedroom? Many of us find an excuse to need them virtually every moment of our lives.

In this section we will briefly discuss a handful of alternative Android custom ROM (stands for Read Only Memory, think of it like an Operating System) but we will focus mainly on one that I find to be arguably the best for privacy and security. If you want privacy, we can forget the iPhone or any Apple products. The Apple ecosystem is relatively more secure against third party threats, but Apple collects a staggering amount of data from each device, regardless of what settings you enable or disable. Regular Androids also suffer from the same overwhelming telemetry from Google, we have been funneled down the psychological kill chute of having only two choices for phones, but there are in reality many very usable options. The same formula applies to our computer Operating System which is discussed in the next section of this guide.

Android Open Source Project (AOSP) is the foundation for Google's Android phones; with not a lot of effort, we can eliminate the Google proprietary spyware layer on certain phones, and install a custom ROM. Currently the more common ones are LineageOS, CalyxOS and GrapheneOS, but there are others still. LineageOS works on a wider variety of phones, but the ROM we will focus on in this guide is **GrapheneOS** loaded onto a Google Pixel phone (ironically, we can de-Google a Google phone to make one of the most secure phones available that's ready for the average user.) **GrapheneOS.org** offers detailed, step by step prerequisites and instructions for installation and use of their custom ROM phone. This process completely eliminates Google software from the device and replaces it with a secure system and a user friendly interface, still based on Android. For those on iPhones, you will have somewhat of a learning curve, for Android users, you will notice little change with this phone. You can also purchase phones with GrapheneOS already installed, but are more expensive than the DIY method. One last wonderful thing about GrapheneOS; it is **free.**

Before we go further, watch this video by Rob Braxman for a very concise explanation of what a 'de-Googled' phone is and how it works, and also importantly, what doesn't work.

https://odysee.com/@RobBraxmanTech:6/degoogled:7



Your phone is likely the most critical tool you depend on day to day, hour by hour, which means changing things up doesn't sound very appealing to most. However, a little bit of planning and effort can gain you an immense amount of privacy, and feel quite liberating, by exploring GrapheneOS. Let's walk through the overview of what this entails.

First, an overview summary of what we are physically doing here. In this example, we are buying a Google Pixel phone and using a prepaid SIM card to get a second device up and running in order to get familiar with it for a few weeks, before switching from your daily driver phone over to your de-Googled phone. **Mint Mobile** and others offer one week trial SIM cards for $1 or so, and if that's not enough time, pay for a three month plan at an introductory reduced cost to get you going a little further if you need more time to 'test drive' your new de-Googled phone. 3-12 month 4gb plans with unlimited talk/text come in as low as $15/month which I find quite reasonable, either for trying a new phone, or for your main service later.

Once you are satisfied and confident enough to switch, simply drop your current daily driver SIM card into your de-Googled phone, import your contacts (easily done via USB and/or cable, copying and pasting the .vcf file by exporting and then importing contacts), install a few apps, and you are up and running pretty quickly. Your number stays the same, the new phone will soak up the contacts easily, and you might be surprised at how easy a transition it is for you. If you get frustrated or lost, simply drop your SIM back into your old phone, but I did not have any desire to do that myself, based on how easy the new device is to use. Another option is to run your old phone without the SIM if you need to use a specific app, but use WiFi or hotspot off of your de-Googled phone, some apps may not work if based on the cell number since your SIM is not inserted, or you might just need to confirm an SMS code.

Just to recap, you start with the current phone/SIM you have now, then adding a GrapheneOS phone with a trial prepaid SIM card, and then swapping your current SIM into the GrapheneOS phone to make that your daily driver phone. In order to use any of the apps on your old phone (without a SIM card now, because it's in your GrapheneOS phone) simply turn on Hotspot on the GrapheneOS phone and connect your old phone via WiFi.

Bottom line is that transitioning from one phone to another does not have to be instant, and there is *no* *'point of no return,'* but rather done gradually by using both phones for a period of time as you get comfortable with the new device. Another inadvertent thing that we accomplish by doing this is redundancy, a favorite topic of mine; you now possess two devices, and potentially two SIM cards if you continue to pay for service on the trial SIM. Should one fail or be lost, stolen, etc, you can quickly get back up and running with your second device that is loaded already with all of your apps and contacts. Even a phone without a SIM inserted can make an emergency 911 call.

Since we are discussing privacy, and de-Googled phones, I'll throw in one quick trick if you must, or want to carry around your old Google or Apple phone; keep it off and in a **Faraday bag** when not in use. Without a Faraday bag, your standard phone can be remotely accessed for not only location, but Apple/Google can install software changes/updates even with the phone off, so long as it has power and connectivity. The only way to defeat this unsolicited connectivity, is 'putting your tin foil hat' over your phone (keeping it in a Faraday bag.)

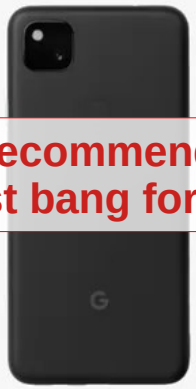
Of note...

toolkit@privacy:~$ GrapheneOS is privacy and security oriented by default, and without Google services, many push notifications will not work on the device since they are dependent on Google, which is removed from the phone. Your native call and text message apps will work normal with sound/vibration/visual alerts in real time, but email and most other apps will not. Not having your email and other apps beat you up with notifications constantly may be a deal breaker for some, but I find this a good thing, since you go to the phone when YOU want to or need to, instead of your phone sucking you in non-stop. Signal and some other apps can be allowed to run in the background to get real time alerts just fine, but if the specific app you need depends on Google services, it will not provide such notifications.

If you do require a Google based app, and to provide notifications, scroll down to the ‘Using Sandboxed Google Play’ page in this guide for how you can use Google dependent apps in a sandboxed environment to achieve this.

The other major change from a standard Android is that to stay ‘de-Googled,’ you will not have Google Maps app, which most of us rely on for vehicle navigation. Keep reading to see the alternatives to replace Google Maps, Magic Earth is my top recommendation, but there are a few others to try out. While we don’t have Google Maps on the phone, you can still use it in a browser in a pinch, you just lose some convenience factor.

Your phone can be backed up to a USB flash drive easily, and is divided into two different types of storage. By default, your ‘app-private’ (internal) storage is what is backed up when you use the System-Backup feature in Settings by connecting the flash drive to the phone and selecting it as the target for the backup. However your ‘Shared’ storage (files, photos and videos in DCIM, Ringtones, etc) must be saved separately- plug your flash drive and phone into your computer and copy the phone’s Shared storage to the flash drive. Do these two steps often to ensure you have a solid backup of your entire phone should it get lost or damaged, you can recover all of your data and apps. Signal app and some other messenger apps will not load previous messages by default (as a security feature,) but your app and the contacts will still be there.

Pixel 4	Pixel 4 XL	Pixel 4a	Pixel 4a 5G	Pixel 5
				
5.7-inch	6.3-inch	5.8-inch	6.2-inch	6-inch
Pixel 4	Pixel 4 XL	Pixel 4a	Pixel 4a 5G	Pixel 5
				
4K (30 fps), FHD (30/60 fps), Slow-mo (FHD @ 120fps, HD @ 240 fps), OIS/EIS	4K (30 fps), FHD (30/60 fps), Slow-mo (FHD @ 120fps, HD @ 240 fps), OIS/EIS	4K (30 fps), FHD (30/60 fps), Slow-mo (FHD @ 120 fps, 720p @ 240 fps), OIS/EIS	4K (30/60 fps), FHD (30/60 fps), Slow-mo (FHD @ 120fps, HD @ 240 fps), OIS/EIS	4K (30/60 fps), FHD (30/60 fps), Slow-mo (FHD @ 120fps, HD @ 240 fps), OIS/EIS

Currently I recommend the Pixel 5 as the most bang for your buck

Pixel 6 and 6 Pro are very large screen, similar to the 4 XL, and offer a big leap in camera quality, especially the 6 Pro model.

Pixel 6 Pro

Pixel 6

New

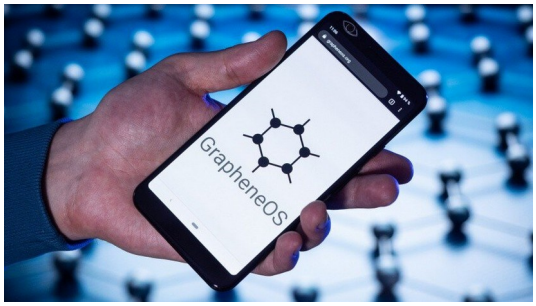
Pixel 6a

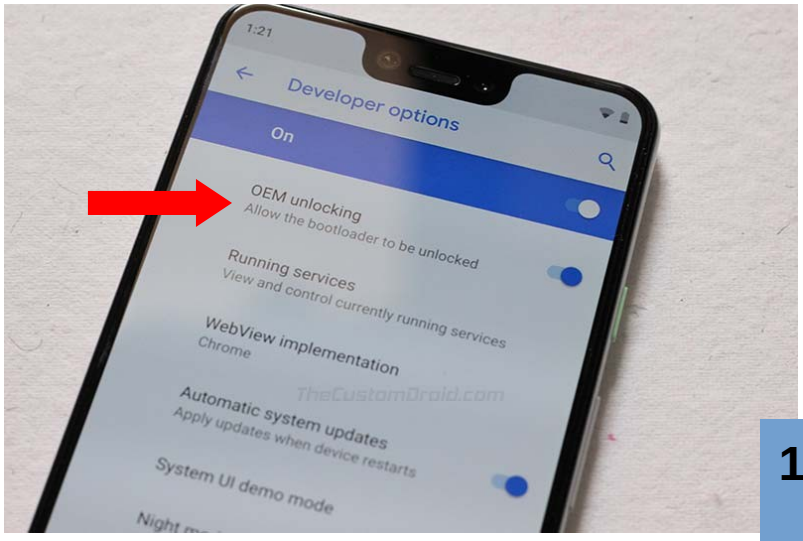
toolkit@privacy:~$ My biggest message to those who think that they don't have time to learn about these new systems, or think that they have to 'take the plunge' and go all in, know that you can easily dabble with learning de-Googled phones and Linux Operating Systems. There is no 'point of no return' on any of this, if you don't wish to use a de-Googled phone or Linux OS after trying them out, you can easily keep what you currently have, or revert back to stock OS at any time. If you get too busy, just walk away and come back, it will be waiting for you where you left off. These are completely free to try and use minus the device cost. If you choose to go the DIY route for GrapheneOS de-Googled phone, you must first find an unlocked version of a Google Pixel 3 or higher, I recommend the Pixel 5 for most currently due to being fairly new still, but about half the price of the Pixel 6 or 6 Pro models. Buy the most current one you can afford as best practice. Pixel 4a's and 4xl's are still great phones, do know that they are getting old enough now where battery life may be starting to suffer a bit on some, however mine still function just fine, and the Pixel 4a/XL's can be found for as little as $200 in good condition. Pixel 5's are going for around $350 in good condition which is very reasonable for what you are getting.

It is important to not only have a **carrier unlocked phone** that's not on a contract, but the bootloader **must be 'unlockable'** which can be determined quickly by interacting with the phone as outlined on **https://grapheneos.org** by attempting to toggle on 'OEM unlocking' option in Developer Options menu. If OEM unlock button is grayed out/disabled, do not attempt to flash the phone with a custom ROM. For those less technically savvy, consider purchasing a phone with GrapheneOS already installed, just be sure to buy from a reputable seller.

Since Pixel phones do not have any additional SD card slots, you may choose to store a microSD card placed in between the back of the phone and the case, with an adapter handy in your bag, or simply carry a USB drive with a USB-C adapter to plug into your phone for extra storage space.

Using email, cloud or a local USB drive, transfer your contacts as a **'.vcf'** file onto the GrapheneOS phone, a box should pop up asking if you want to add the file to your Contacts. Select 'Yes' and in a few seconds your phone will be ready to call and message all of your current contacts.





Officially supported operating systems for the web install method of GrapheneOS:

Windows 10

Windows 11

macOS Catalina

macOS Big Sur

macOS Monterey

Arch Linux

Debian 10 (buster)

Debian 11 (bullseye)

Ubuntu 20.04 LTS

Ubuntu 21.10

Ubuntu 22.04 LTS

ChromeOS

GrapheneOS

Google Android (stock Pixel OS) and other certified Android variants

Officially supported browsers for the web install method**:**

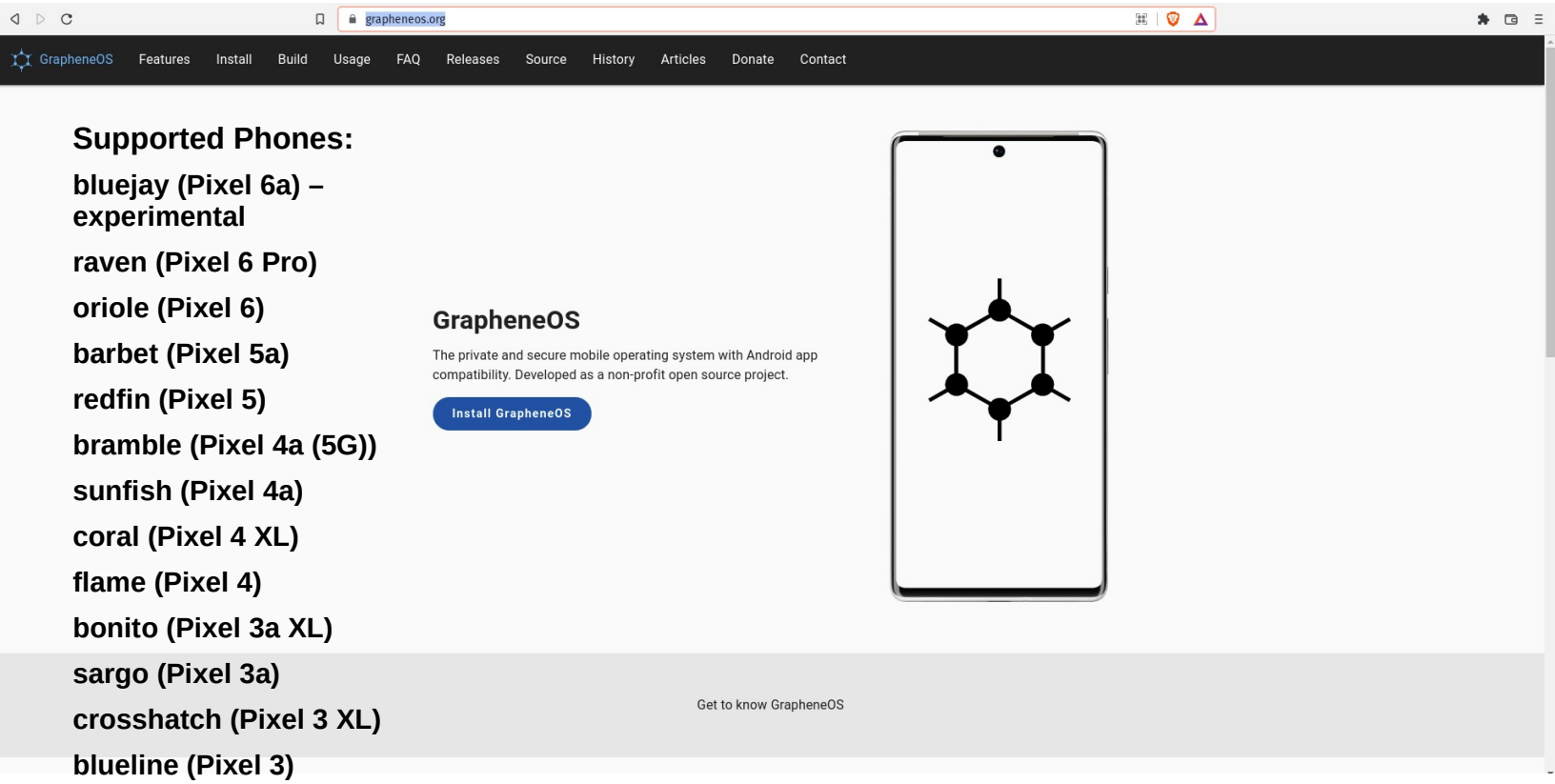
Chromium (outside Ubuntu, since they ship a broken Snap package without working WebUSB)

Vanadium (GrapheneOS)

Google Chrome

Microsoft Edge

Brave



DIY GrapheneOS Install

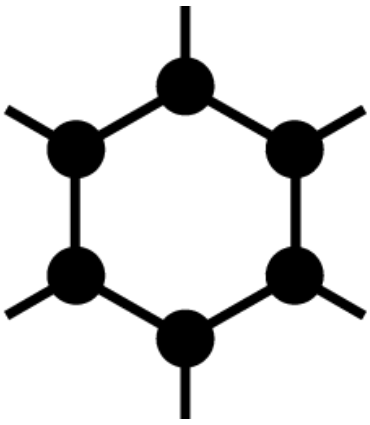
Using Sandboxed Google Play

GrapheneOS isn’t for everyone, but those on the fence that still need certain Google apps have an option to ‘Sandbox’ apps that require Google Play within the phone. This process allows Google apps to function but not have access to the rest of the phone, only the permissions you grant it specifically. Not ideal for privacy, but leaps and bounds better than a standard Google Android or iPhone.

From **https://grapheneos.org/features#sandboxed-google-play**

“GrapheneOS has a compatibility layer providing the option to install and use the official releases of Google Play in the standard app sandbox. Google Play receives absolutely no special access or privileges on GrapheneOS as opposed to bypassing the app sandbox and receiving a massive amount of highly privileged access. Instead, the compatibility layer teaches it how to work within the full app sandbox. It also isn't used as a backend for the OS services as it would be elsewhere since GrapheneOS doesn't use Google Play even when it's installed.

Since the Google Play apps are simply regular apps on GrapheneOS, you install them within a specific user or work profile and they're only available within that profile. Only apps within the same profile can use it and they need to explicitly choose to use it. It works the same way as any other app and has no special capabilities. As with any other app, it can't access data of other apps and requires explicit user consent to gain access to profile data or the standard permissions. Apps within the same profile can communicate with mutual consent and it's no different for sandboxed Google Play.”



Google Play

Shift the Tech Paradigm

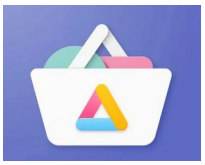
toolkit@privacy:~$ When we talk about shifting the paradigm of how we view and use our tech, here is a great example to consider. When we buy phones, many of us simply go to our local Verizon or T-Mobile stores and receive a new phone by purchasing it under a contract, under our account. With this method, there is little out of pocket cost at the time, instead you pay a small monthly fee, for many cases, years. While under this contract, they lock the phone so that no other carrier can be used, and no custom ROM can be installed, they have a large amount of control of the device. They also do a credit pull, and your full set of information is now attributed to that device (full name, SSN, DOB, etc.) You also are in a 'post-paid' account, which are typically much more expensive than pre-paid service accounts.

Instead of being locked into an ecosystem, we should instead seek to avoid those stores entirely. We buy our unlocked, carrier agnostic device from a trusted seller, either new or used, in which case we own the phone entirely. This is a bigger up front fee, however as mentioned earlier, there are many Pixel devices within reach price wise for most all of us. Load up your service using a pre-paid SIM card, most will offer a discount if you pay for a longer period of service, say 12 months. Go a large step further, and install GrapheneOS onto a Pixel phone, and if you really wanted private, you could choose to purchase the phone and the SIM card anonymously. Know that the cell carrier sees the phone's location, so true anonymity will be effectively impossible if that device is at your home frequently. However, even just transferring your daily mobile device to a GrapheneOS phone with pre-paid service, you have not gone through a credit check, your information associated with the device is much less, near zero if you choose, and you are not locked into any contracts. You pay less overall. You own your device. You have control of turning on and off your microphone, camera, location (to a degree) which is what our mobile phone experience should be. The phone does not come installed with a ton of 'bloatware' with unwanted apps that in many cases, cannot be easily uninstalled, meaning they are using and displacing precious data and memory, even though we don't want or need those bloatware apps.

Whether we care or not, our phones are our defacto microchips for most of us, the way we carry them with us every moment. They are constantly listening, watching and recording our every move. When you lift your phone to check to see if you have a message, Facebook, Google, Apple and others connect and pull that information-just from you touching your phone-very creepy and unwanted. So do something about it. Shift the paradigm. Tell your friends.

App Stores
Google Play Store Alternatives

toolkit@privacy:~$ Using a De-Googled phone means we need to pull our apps from somewhere other than the Google Play Store. There are two main app stores, although plenty of other options exist for many apps, although not all are available from one source as the Google app store functions, and not all are considered safe to download.



F-Droid is a free, open source software app store, these are considered safe, and the number one place I look for apps.

Aurora Store is another Google Play Store alternative, using this method essentially spoofs Google and downloads most Google Play Store apps anonymously. This is usually my second stop when looking for apps. You can set the filters to filter out ‘GSF dependent’ apps, although downloading a GSF dependent app won’t install Google, the Google dependencies simply won’t work.

Besides F-Droid and Aurora Store, you will find APK files for various apps on their respective websites, just exercise caution and research them a bit, not all respect privacy by any means. General things to look for are ‘Open Source’ code, reading the Terms of Service and/or Privacy Policies to see what type of information they use and collect, and simple internet searches to see what other privacy minded people or developers think about the app.

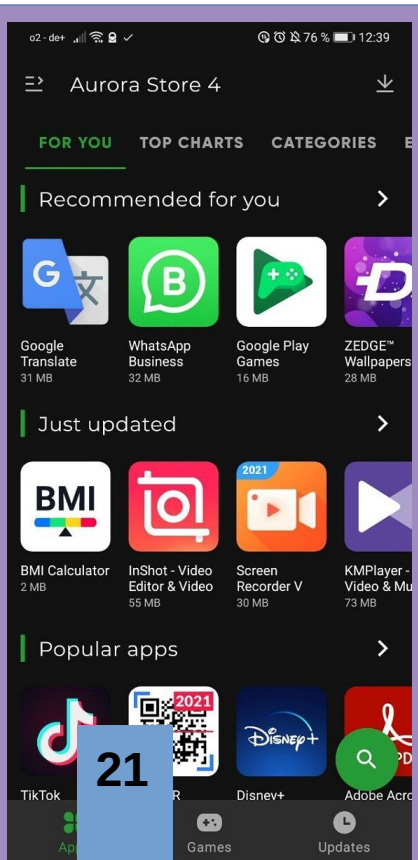
Anytime you install a new app, you will get a prompt to confirm that you wish to install the app, once downloaded, long press on the app icon and click the information icon and review the ‘Permissions’ section. Only allow the app to use the permissions that it needs to function. GrapheneOS also allows you to choose to deny the app from any permissions you wish when the app is not in use, this can prevent battery drain by restricting the app from running in the background, and also prevent some data leakage.

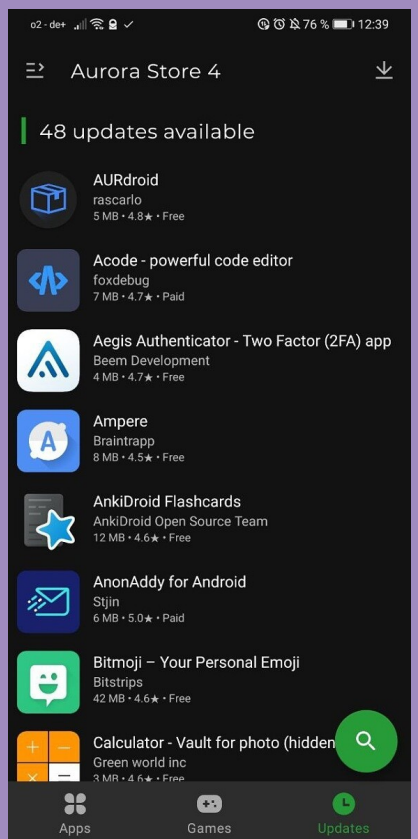
F-Droid and Aurora app stores

toolkit@privacy:~$

F-Droid is an app store with software that is all free and open source (FOSS) and is my first go-to in order to find apps for a de-Googled phone. You can still use this app store on any Android phone however, not just de-Googled phones. Apple forces you into their own ecosystem, so this will not work on iPhones.

Use F-Droid to download a second app store called **Aurora Store**





Aurora Store is an easy to use app store for anything you cannot find in F-Droid. Do not sign in with Google, use the ‘Anonymous’ option when using the app. This essentially spoofs the Google Play Store to pull the apps you need on your de-Googled phone. (Again, these app stores also work on regular Google Android if you haven’t de-Googled yet)

Map Navigation Apps

toolkit@privacy:~$ With a de-Googled phone, you can install Google Maps if you so choose, but this defeats the purpose of the phone. Not using Google Maps is likely the biggest change you will notice when switching to de-Googled life, so we need an alternative map app to take its place. There are at least a few good options, each with their own pros and cons, and specific strengths.

Magic Earth, available for download in Aurora Store is my top recommendation for a direct replacement for Google Maps app, I find this app to be the easiest to use out of the box for vehicle navigation with turn by turn voice and visual directions. Magic Earth indexes on addresses better than the others, and offers the ability to download maps state by state, country by country, for offline use when not within cell service.

OsmAnd, available for download in F-Droid Store is my second recommendation, this is an excellent and more detailed settings app, the main drawback for this app is that is won't index on addresses as well as Magic Earth, but will precisely navigate you to any location you point it to. The other issue I've found is that it requires more manipulation of settings in order to get this app to function exactly how you want it to, but if you are willing to take the time to familiarize and customize settings, it will give you very detailed information on route including elevation analysis and many other features. OsmAnd also has offline maps available to download, the entire US offline maps takes up about 9GB of space which is fairly reasonable. This app will calculate ETA and accurate route even without cell service, an excellent useful feature for when in poor, or no cell service areas.

All-In-One Offline Maps is available through Aurora Store and APK Pure, this app is best for on foot navigation for activities such as hiking, biking, climbing, hunting, etc. While it has its use for vehicle navigation, it is not meant for turn by turn directions as does Google Maps, Magic Earth or OsmAnd. Many topographic layers are available, and like the others, allows for downloading a specific area for offline use which makes this an excellent app for outdoor adventures out of cell service. I've used this app for many years for precise mountaineering navigation and find it my go to for anything I do on foot.

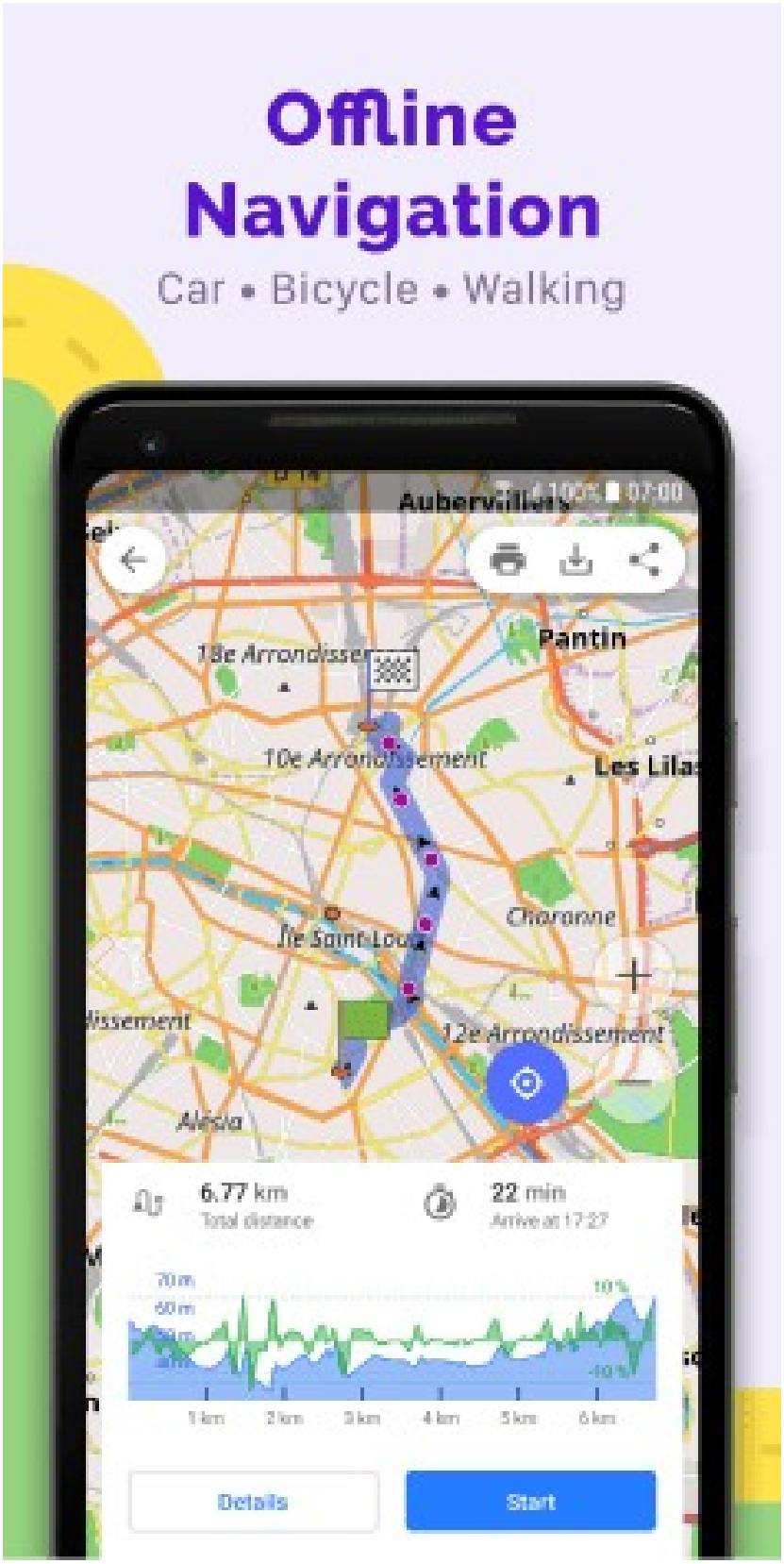
Magic Earth

toolkit@privacy:~$ A sample view of Magic Earth navigation

You can adjust the settings to set speed limit warnings, change the voice, set units to Miles/Feet or Kilometers/Meters, 2D or 3D view, and even use it as a dashcam in addition to navigation.

AI Dashcam integration: https://www.magicearth.com/ai-dashcam/

OsmAnd+ Maps



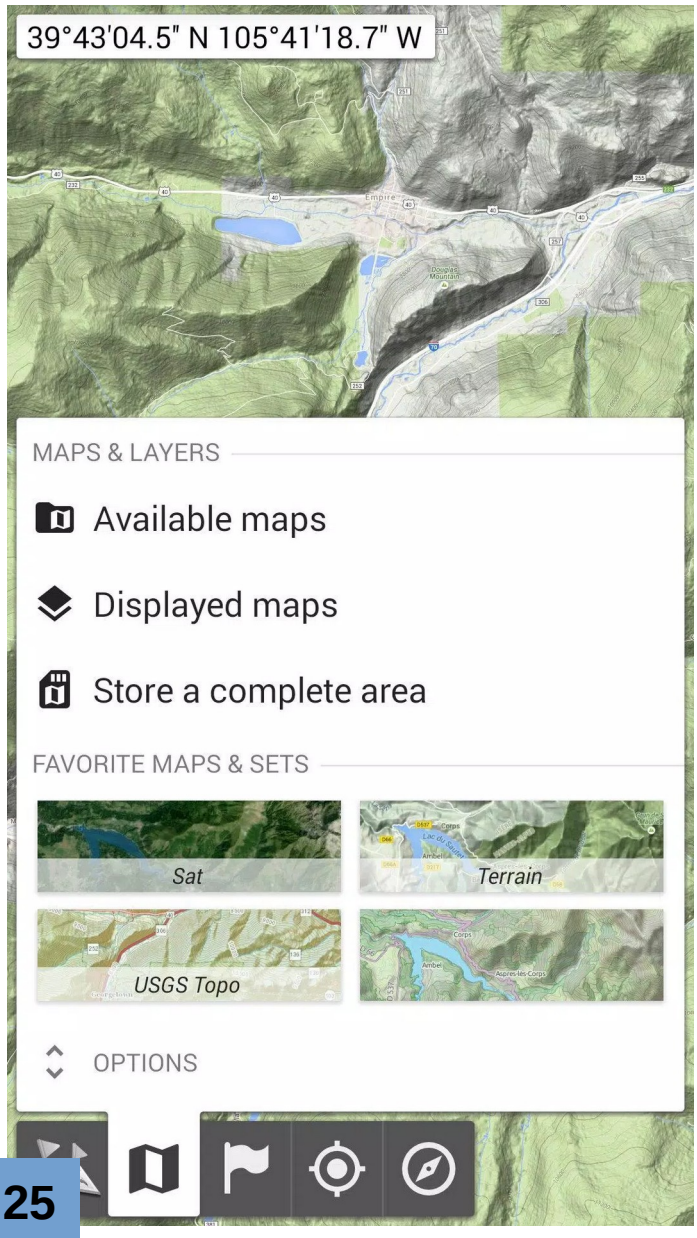
toolkit@privacy:~$ OsmAnd~ is much more feature rich than most others, the settings menu seems endless. This may be overwhelming for some to configure to your liking, but still a fairly intuitive and easy to use app with the default settings.

OsmAnd includes turn by turn directions including which lane you need to be in, and you can configure the display to show ETA, duration, distance remaining, and a ton of other details about your route. As with the other apps, you can add waypoints or points of interest easily and categorize them if you choose.

Default settings/modes for driving, public trans, and biking / walking available to use.

All-In-One Offline Maps

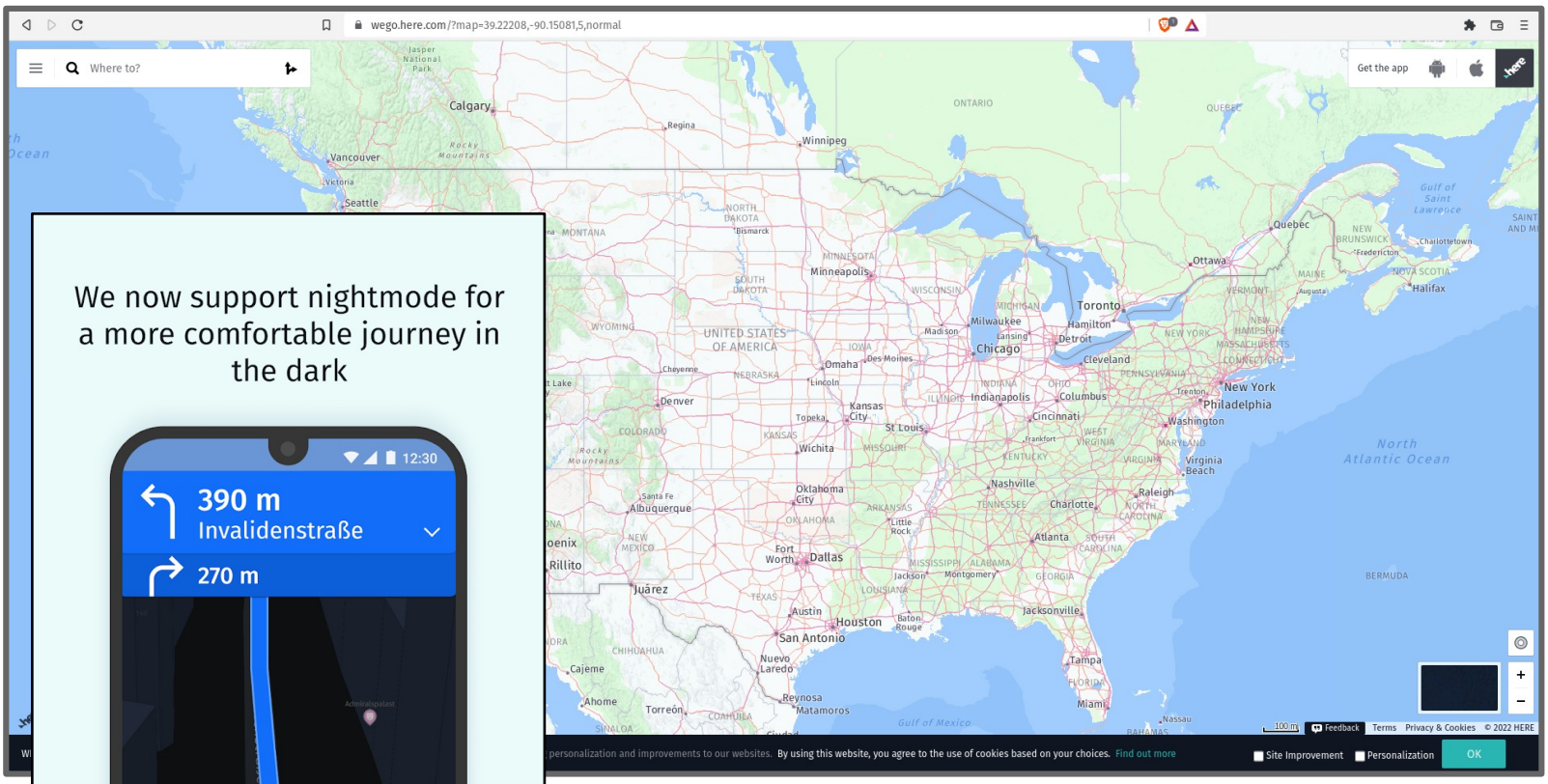
toolkit@privacy:~$ This app has been a must have for me for many years, even the free version comes with plenty of features. I find this app my go to for anything on foot, if you frequent the outdoors, you will want to try this out. There are various topographic and other layers that you can download and use, and like the other apps, you can select and save an area onto your device for use offline. With a de-Googled phone, you will not be able to use the paid version and maintain your anonymity. To be honest, I never really noticed a big difference between the free and paid versions, so I don't see this as an issue for most. All-In-One Offline maps has real time position, compass bearing to target, and many other settings to customize to your needs.



toolkit@privacy:~$ Other map options include using Google Maps, but from a browser tab rather than the app. Downloading and using the app defeats the purpose of our de-Googled phone, but by using a browser of your choice to use Google Maps will not give up your identity to Google. Some functionality will be lost when compared to the native app, but still quite useful if you get frustrated with the other apps and need to revert back to something more familiar in a pinch.

Another option is HERE WeGo maps app which you may find useful in a browser:

https://wego.here.com/?map=39.22208,-90.15081,5,normal

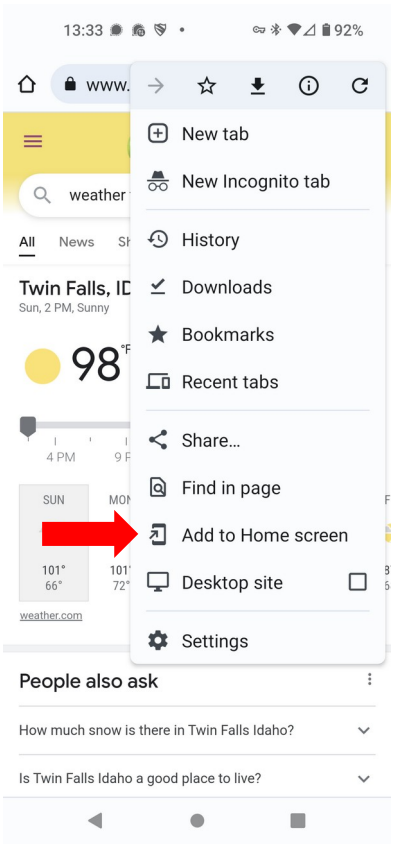


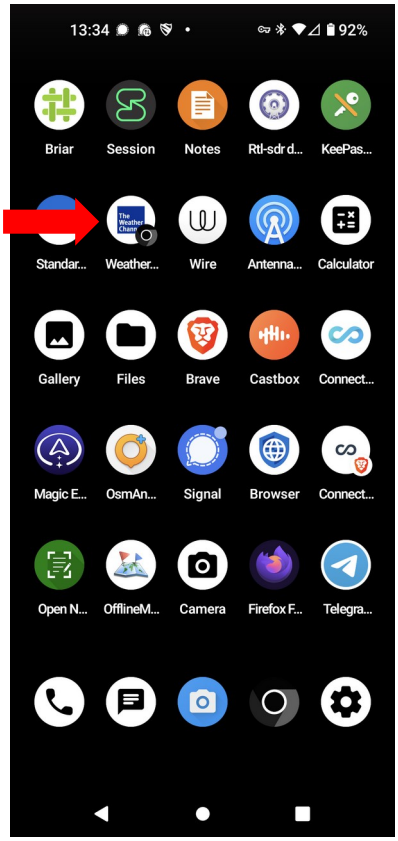
Or you can try the app on your mobile using Aurora Store

Weather Apps

toolkit@privacy:~$ Weather apps usually offer little extra, if anything other than a standard data pull from a larger national weather database, but they do collect a ton of user information about the device, and your identity. Instead of installing a weather app, simply navigate to a weather page in your browser, and then save the page to your home screen as a shortcut, this will function just like clicking on an app and provide you with the exact same information, but does not leak your own data through an app. This example is a Vanadium browser tab and saving a shortcut to the home screen of a GrapheneOS Pixel 5 phone.

Click on the Menu icon in the top right hand corner of your browser and select ‘Add to Home screen’





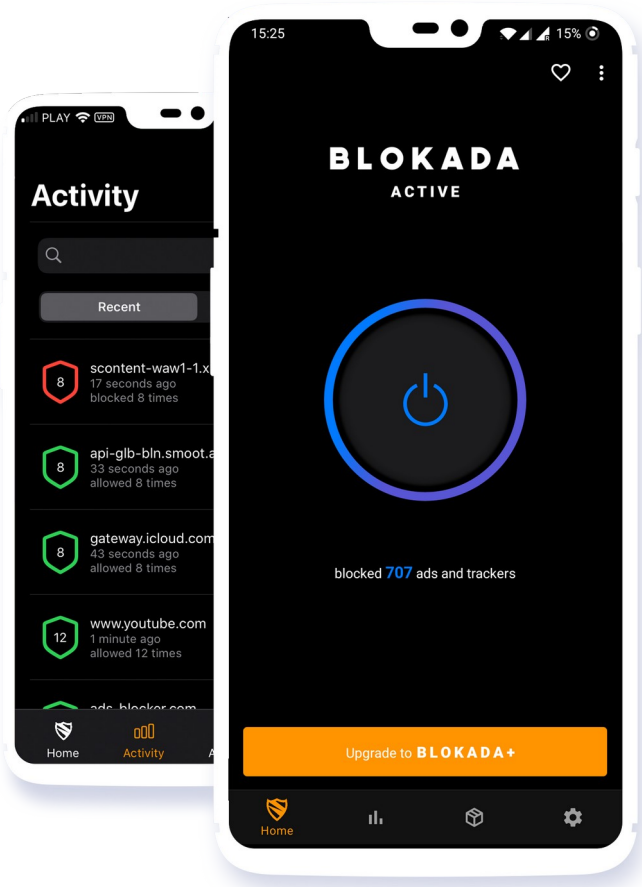
Setting up a VPN or AdBlocker

toolkit@privacy:~$ While there are various methods to help secure our internet connection on the mobile device, let's stick with a couple basics that work well. Install a VPN (Virtual Private Network) which I cover in it's own section later in this guide, and/or an Ad-Blocker app. Most will simply want the VPN app. (You can only run one of these at a time, but not both.)

ProtonVPN

ProtonVPN or a VPN of your choice – install onto your phone, sign in and adjust settings to only allow internet through the VPN. Using one hides your activity from the internet provider, whether that's your cell carrier, or when connected to WiFi. Avoid public WiFi whenever possible to maximize your privacy and security while using your mobile phone, tablet or computer.

Blokada – This can be used to view and block connections to your device that you do not want connecting such as ads and telemetry. Blokada has a free tier that works well and doesn't soak your battery, but filters out a lot of trash and gains you some privacy. View the connections periodically to get a visual on the endless things trying to connect to your device. You can also setup 'block lists' in the settings to help you filter out common known garbage. For full VPN protection, upgrade to the paid tier to Blokada Plus / Blokada 6. The main app can be downloaded from F-Droid app store, with options to upgrade to a paid tier if you choose for better protection.



I keep both of these options on my mobile device- if at home behind my home VPN firewall, I don't need an additional VPN service running. But if out and about, I can toggle on ProtonVPN to keep my internet browsing private from the internet provider/cell carrier. If you don't use a home VPN firewall, then leave your VPN connected while on your home WiFi.

‘Privacy Phone Club Rules’

Of course do what you wish, but these are some general rules I practice, and things that have become habit for me. With of course, the hilarious moniker of ‘Privacy Phone Club Rules.’

-Use a **custom Android ROM** such as GrapheneOS.

-Use a carrier **unlocked** phone with **no contract**.

-If you are not using **Bluetooth**, turn it off.

-If you are not using **WiFi**, turn it off.

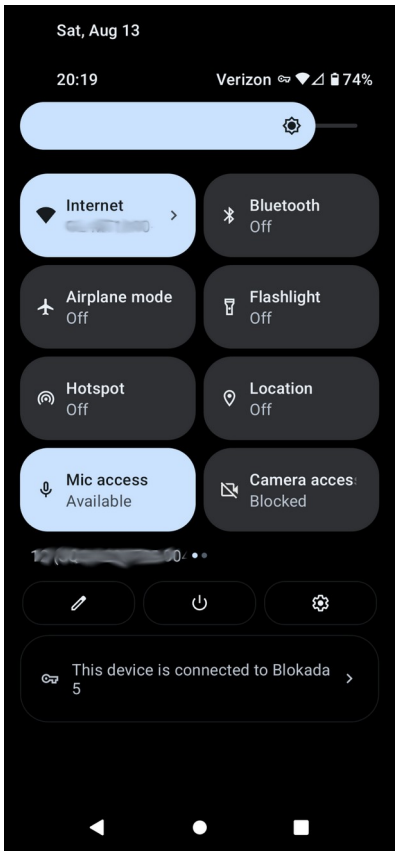
-If you don’t need your **Location** for an app, turn it off.

-On GrapheneOS, you can also quickly disable / restrict microphone and camera access with one tap. If you’re not using a call or video app, camera or other app that requires **Microphone** or **Camera** permission, I turn those permissions off, restricting any app from using them.

-If an app doesn’t need a certain permission, disable that permission.

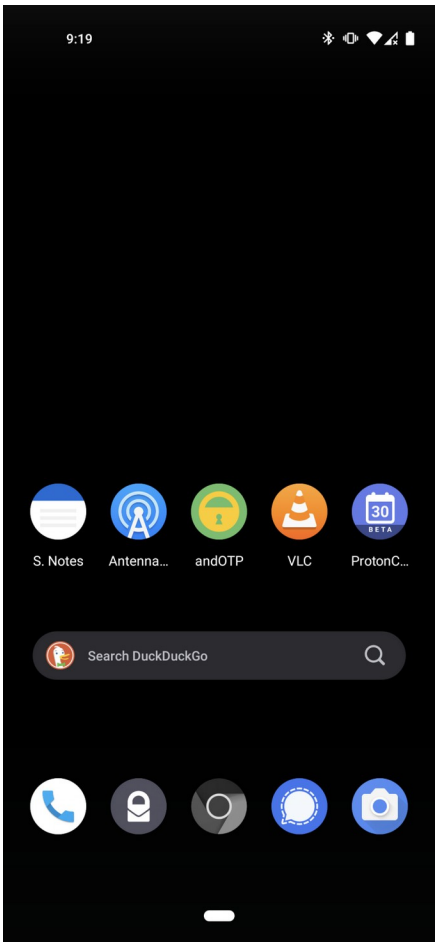
-If the task can be accomplished on a computer, then don’t use your phone, use your computer!

Example screenshot of GrapheneOS ‘swipe down’ menu hot buttons, fully customizable to your needs for quick toggling of permissions and functions on and off



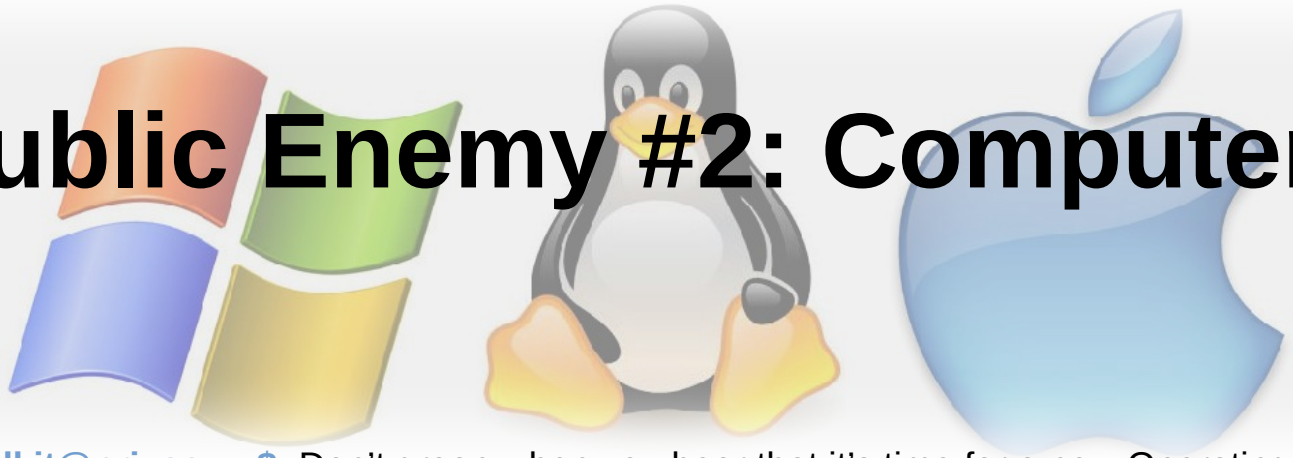
toolkit@privacy:~$ Here is a fairly comprehensive list of apps for your De-Googled phone to get you started, of course your needs will be much more custom, but these are good common ones to consider to at least get you started. Use F-Droid, Aurora Store or direct from web or APK files:

- VLC Media Player
- Metro Music Player
- Odysee / LBRY
- Rumble
- NewPipe
- Signal
- Wire
- Briar
- Element.io
- Session
- Jitsi Meet (video chat)
- **Proton Mail** / Drive / VPN
- Blokada 5
- Brave Browser
- FireFox Focus Browser
- Vanadium Browser
- Bromite Browser
- Tor Browser
- Mojeek Browser
- Standard Notes
- Syncthing
- Magic Earth (maps)
- OsmAnd Plus (maps)
- All-in-One Offline Maps
- Antenna Pod (Podcast app)
- Collabora Office (MS Office viewer)
- KeePassDX (KeePassXC file reader)
- Calibre (e-Book reader)
- LibreOffice Viewer
- Simple Calendar Pro
- Simple Voice Recorder
- OpenCamera
- AirGuard (search for Air Tags nearby)
- PDF Scanner (from F-Droid)
- OpenNotes Scanner
- OpenCV Manager



Public Enemy #2: Computers

Public Enemy #2: Computers



toolkit@privacy:~$ Don't groan when you hear that it's time for a new Operating System (OS) in your life if you are still stuck in the Microsoft Windows OS or MacOS ecosystems. Many have never heard of or given much thought to Linux systems, our large tech friends at Microsoft and Apple ensure that we are only exposed to their own closed source, proprietary systems. Bypassing the history, which I encourage you to research later, let's consider what Linux is and why we want to use it, and ultimately what we achieve when we use this option for our daily computing tasks. This is one of the five OS's available, and arguably the best as far as privacy goes, there are many liberating things about using Linux.

What is FOSS?

Free and Open Source Software, or FOSS, is non-proprietary software that as the name reveals, is free to download and use, and all of the source code is open for anyone to look at to see what is under the hood. Users can modify the software and see what is happening, unlike MS Windows or Apple products. Microsoft has admitted to logging keystrokes and scooping up data in email, and MS Office products such as Word, Excel, etc. Apple and Google scan our content as well, and as we discussed earlier, this data is sold back and forth behind our backs, the code to gather this info invisible to the user. What is Windows 11 doing in the background? Why does it take forty minutes to update, without warning? Is it recording audio? Is the camera taking pictures? Is it logging my IP address, location data, browsing history and other telemetry on how I use my device? With closed source code, you simply don't know what is happening on your machine, Microsoft and Apple have the keys and full control of what your machine does (or doesn't do.)

You clicked 'Accept' without reading the Terms of Service and Privacy Policies, and I don't blame you. I've blindly accepted far too many apps and software, entrusting these companies to simply provide us a product that we need for work, for entertainment, for creating content, viewing others' content. Gradually over the years, we know that these devices and apps are collecting more and more data about us, and selling that data. Shift the tech paradigm, and gravitate towards FOSS, where you are in control.

Did you know that roughly 90% of webservers (sites you visit online) use Linux? Your automobile likely uses AGL (Automotive Grade Linux) and many other tech that you wouldn't really guess. Linux is a large part of our world currently, even big tech companies have their own custom Linux OS's. Don't fall victim to thinking that you are stuck in Windows or Apple! Linux is free, like freedom.

Public Enemy #2: Computers

toolkit@privacy:~$ Enter Linux. Without overwhelming you with the endless Linux OS options, or distributions, let's just get familiar with a few to start with, keeping in mind that there are many other distributions that may appeal more to you later on, and many others are for specific purposes. Linux in general comes with little or no 'bloatware' (extra unwanted programs that are installed by default from manufacturer, even if you don't use them, they take up resources and space on your machine, and in many cases, cannot be easily uninstalled.) Linux in general is very fast and efficient, even really old machines thought to have been unusable with Windows, roar to life and function just fine using Linux.

One great way to get started is to dig up an old desktop or laptop that may be sluggish, try installing Linux onto it (wiping Windows or macOS away) and begin learning, with no consequence. If it blows up, start over and try again, or try a different distribution of Linux to see what you like. Pick just one of these at a time, such as Ubuntu, and go from there.

Ubuntu is an extremely common, if not the most common, and user friendly Linux OS for beginners with tons of support online to help you tackle any issues.

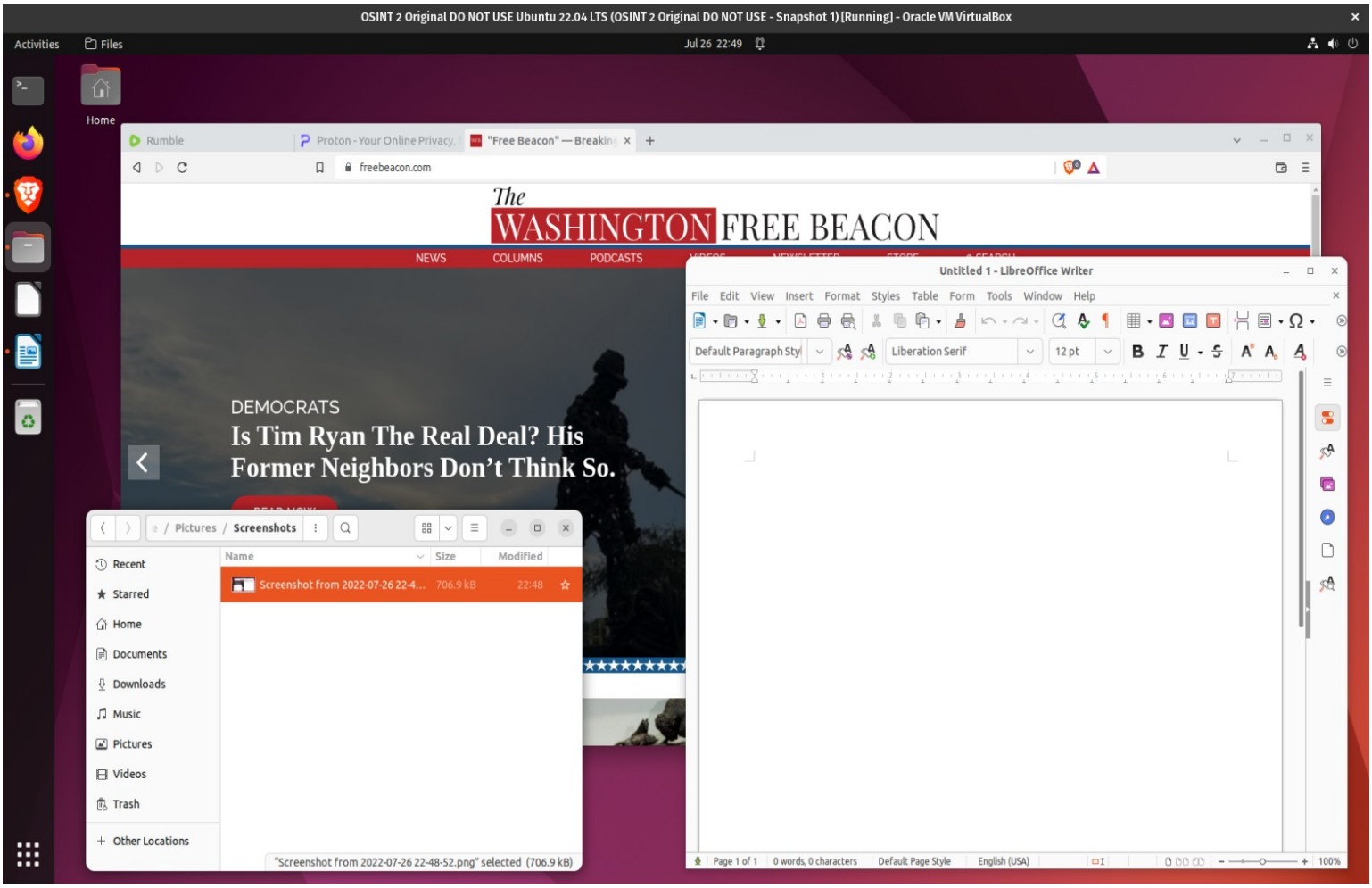
Linux Mint is another very common and easy to use Linux OS, with Desktop Environments (DE's) that mimic the look and feel of either Windows or macOS to help new users adapt. Tons of online support exist for this OS as well.

Pop!OS is currently my daily driver OS, it is similar to Ubuntu with some unique features and good support. → **System76** ← offers Pop!OS or Ubuntu with their computers, an excellent company if shopping for a new, fast and privacy minded machine, made in US, and HP is beginning to offer a Pop!OS option on some of their laptops as well this year.

Manjaro Linux is an Arch based OS that many new users start with, (the first three being Debian based-Ubuntu, Mint, and Pop! OS) [Arch and Debian are like trunks of a whole tree of other Linux distributions and OS's.] Plenty of online support is available for this one as well, although not quite as common as the first two Debian based OS's.

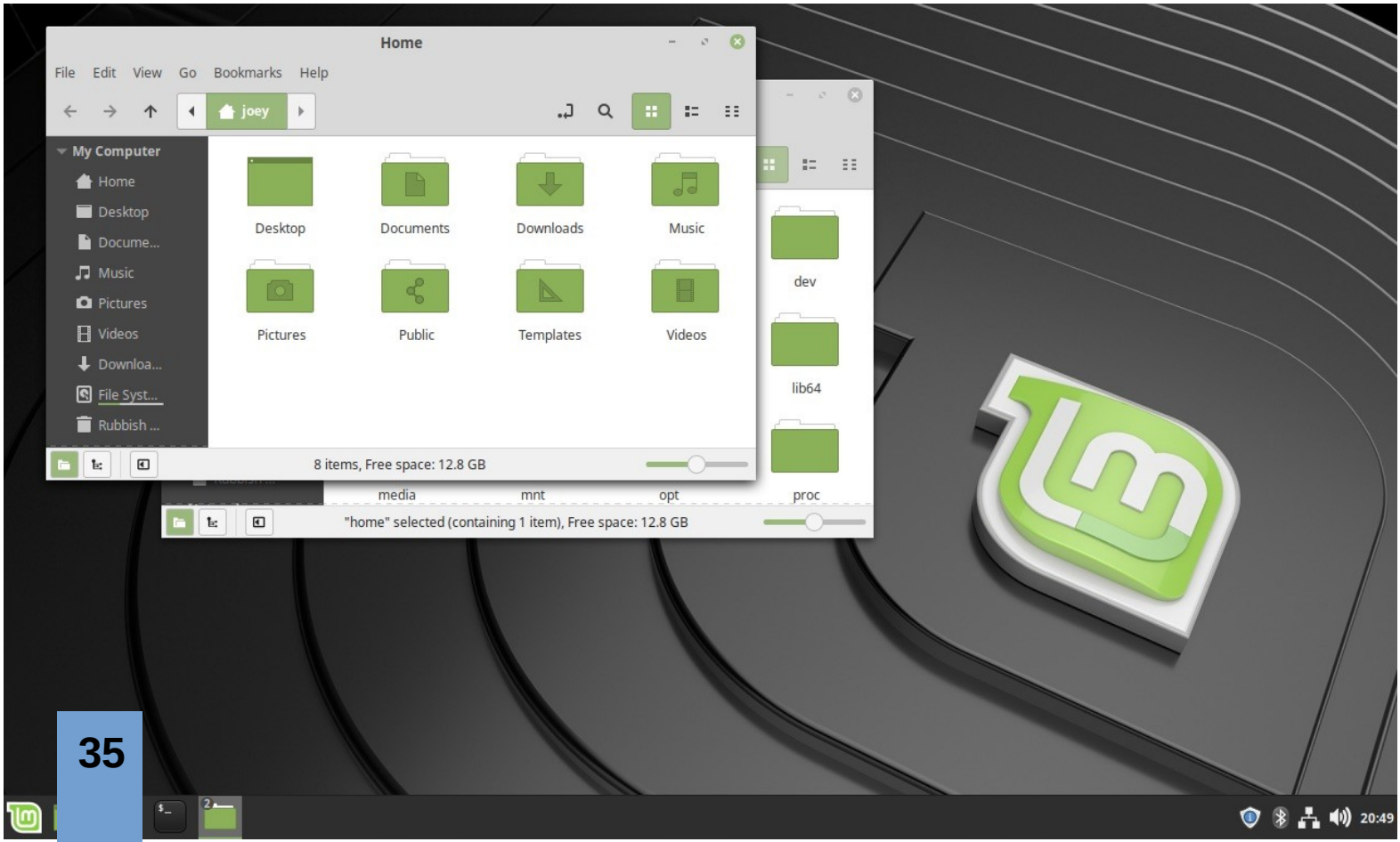
Ubuntu is a great starter Linux OS for most, it's free and easy to use

toolkit@privacy:~$ Example of Ubuntu 22.04 LTS Linux Operating System:

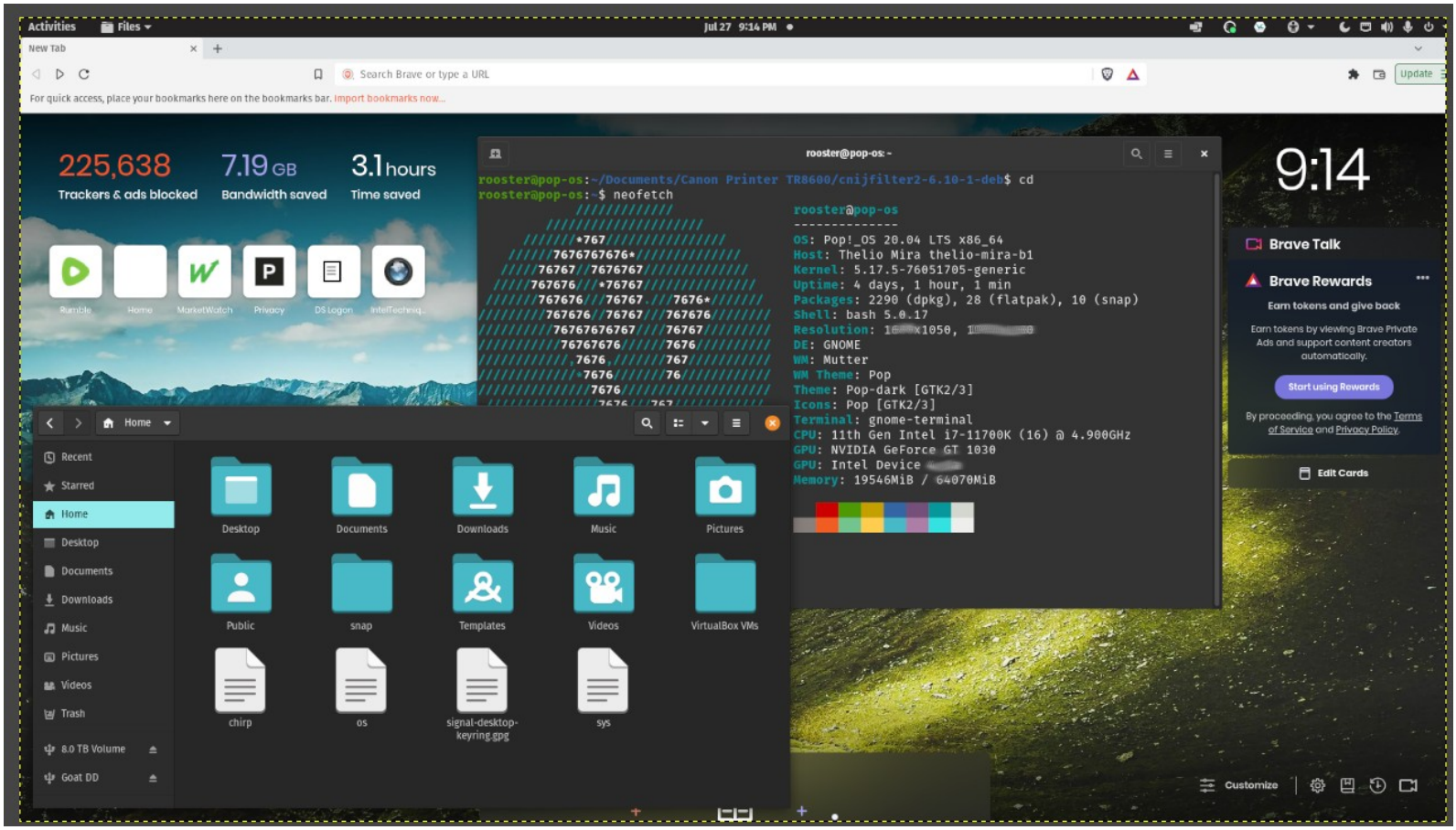


The appearance and icons/tray can all be customized to your liking for both appearance as well as function *(Example, if you want the icons on left to appear on the bottom tray instead, you can change that)*

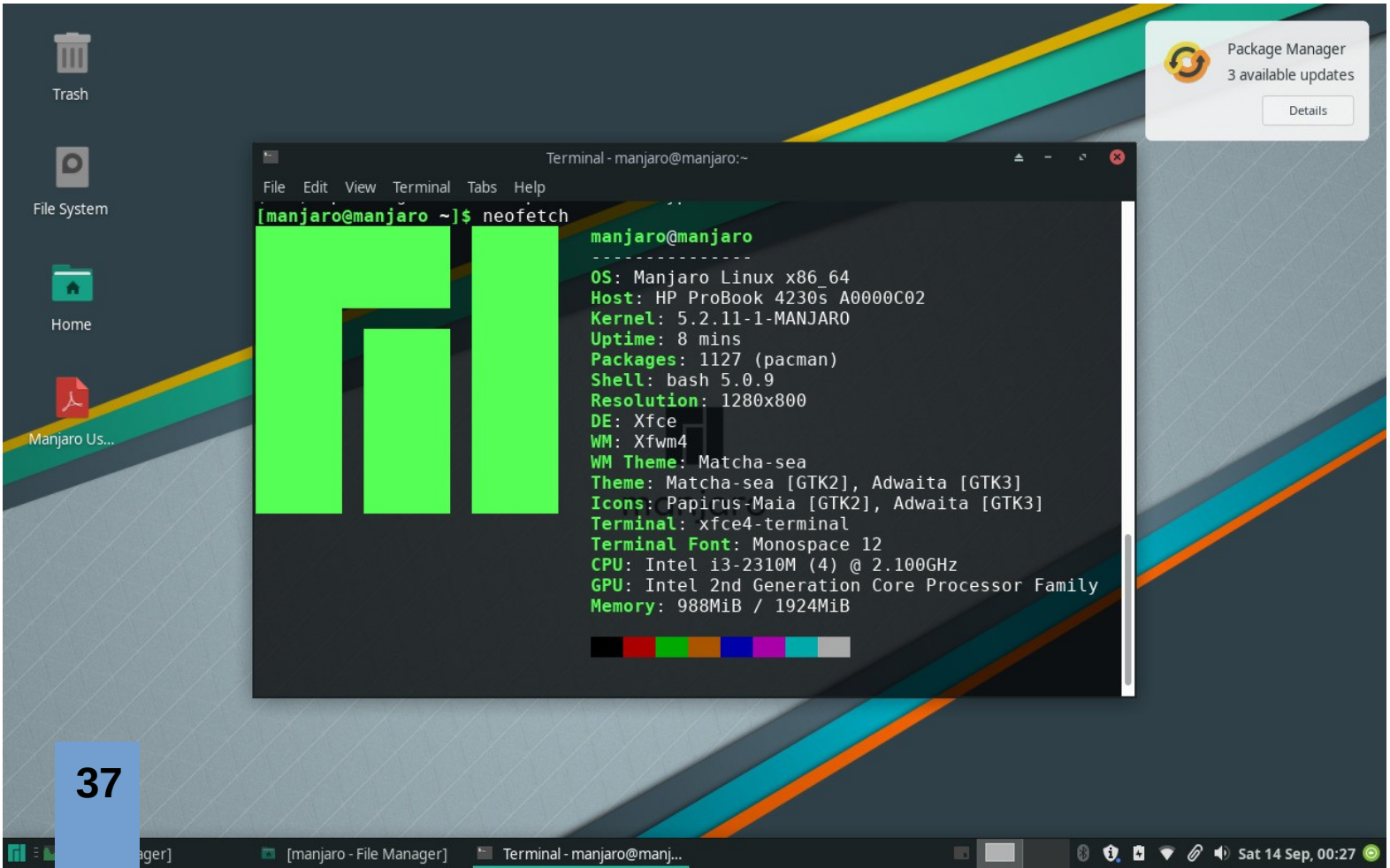
toolkit@privacy:~$ Linux Mint Screenshots, many beginners start with Mint with one of three Desktop Environments, Cinnamon, MATE or Xfce. The difference is mainly just personal preference and how many resources and options are available, Cinnamon being a common choice, give each a look to see what you like.



toolkit@privacy:~$ Pop!OS Linux Screenshots, my personal favorite Linux OS at the moment. Very efficient and easy to use, with good support available through both Pop!OS and many of the Ubuntu issues also apply to this distro.



toolkit@privacy:~$ Manjaro Linux OS screenshots, like most Linux distributions, your desktop can be customized and configured to your liking. Manjaro is based on Arch Linux (the others are Debian based.)



Hold on! - Backup your data

toolkit@privacy:~$ Before proceeding with any installation of a new Operating System, **backup all of your data first!** Make sure you collect all of your wanted documents and media off of your existing device before installing anything new, or making any major changes or upgrades to any machine. It's also not a bad idea to create a boot disk of your current machine just in case you ever wish to use that specific one again for some reason.

Some general advice, I store all of my data on an external hard drive, that way I can bounce from computer to computer at will, without the need to transfer anything, or risk losing data if a machine crashes for good.

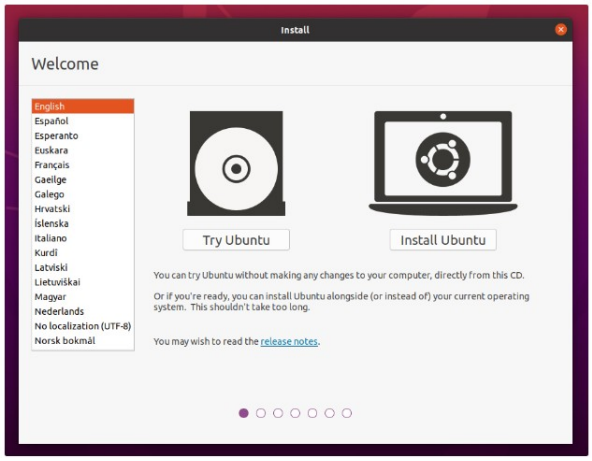
Backup your data always! One cannot backup often enough, most of us put this off way too long, until we get pinched from a digital glitch and lose a lot of important data. I run most of my day to day life off of a 2TB SSD external drive, but I keep a backup of that entire drive on a separate drive, and update/backup frequently. If you have a reliable and trusted cloud service, or local NAS (Network Attached Storage) or network, you can store a copy there as well for safe keeping. We want to prevent losing our data should a drive fail, get damaged, or stolen, backup always. Did I mention, you should backup your data? Don't lose a lifetime of photos or important documents due to poor storage strategy (or lack of one.) Best practice is to have copies in your physical control, remember that a cloud is just someone else computer…

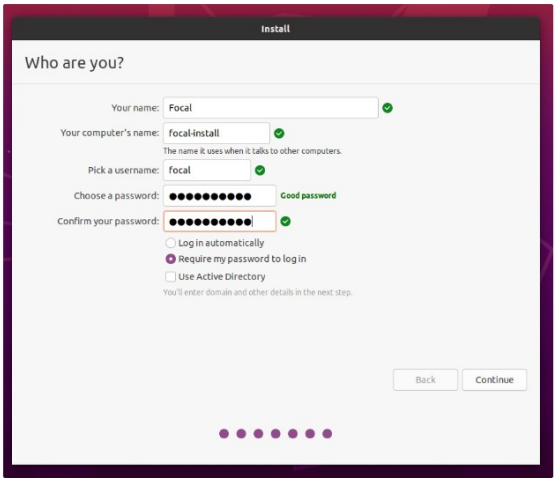
Small SSD drives offer an excellent on the go storage solution for daily needs, and can be quickly removed for secure storage when necessary.

Large internal drives can be a cheap way to store backup data, they can be plugged in with an inexpensive USB adapter and power supply, and often require you to format them before they will work as an external drive. (FAT32 format is usually a good one) The HDD have physical spinning media, and are slower, but are still fairly reliable, and less expensive than SSD drives which use less power, are smaller, but much more expensive.

USB drives are often big enough for storing large amounts of photo, video and documents, you may find adequate solutions using inexpensive USB drives.

Ubuntu installation guide



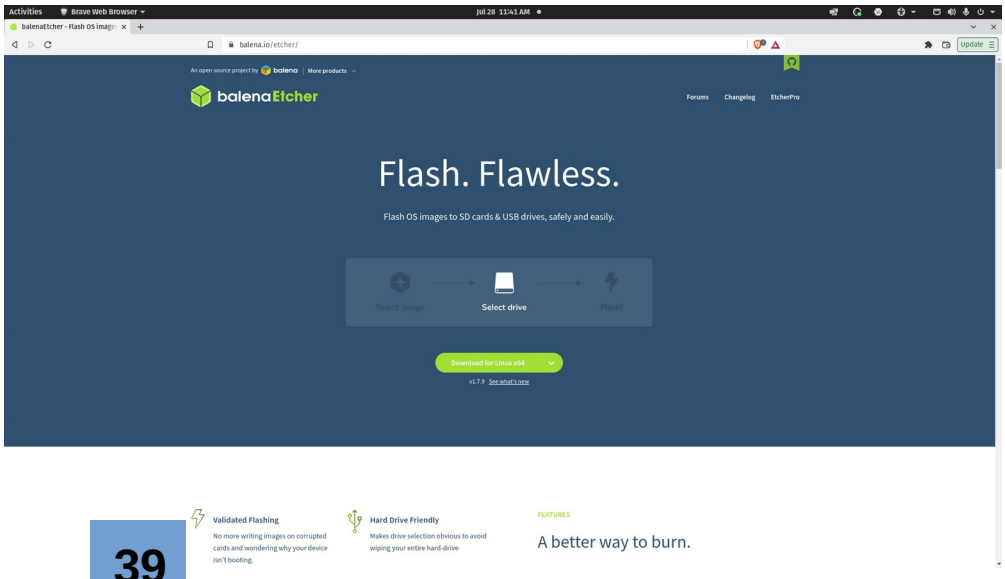


toolkit@privacy:~$ General instructions on how to download and install a Linux OS of your choice, see more detailed instructions **here** (Ubuntu in this example, but applies to others as well.) The only things you will need to install or try out any OS are:

- **Computer with at least 25GB of storage remaining**
- **USB drive 8GB in size or higher**
- **Decent internet connection**
- **20-30 minutes to install and update the new OS**

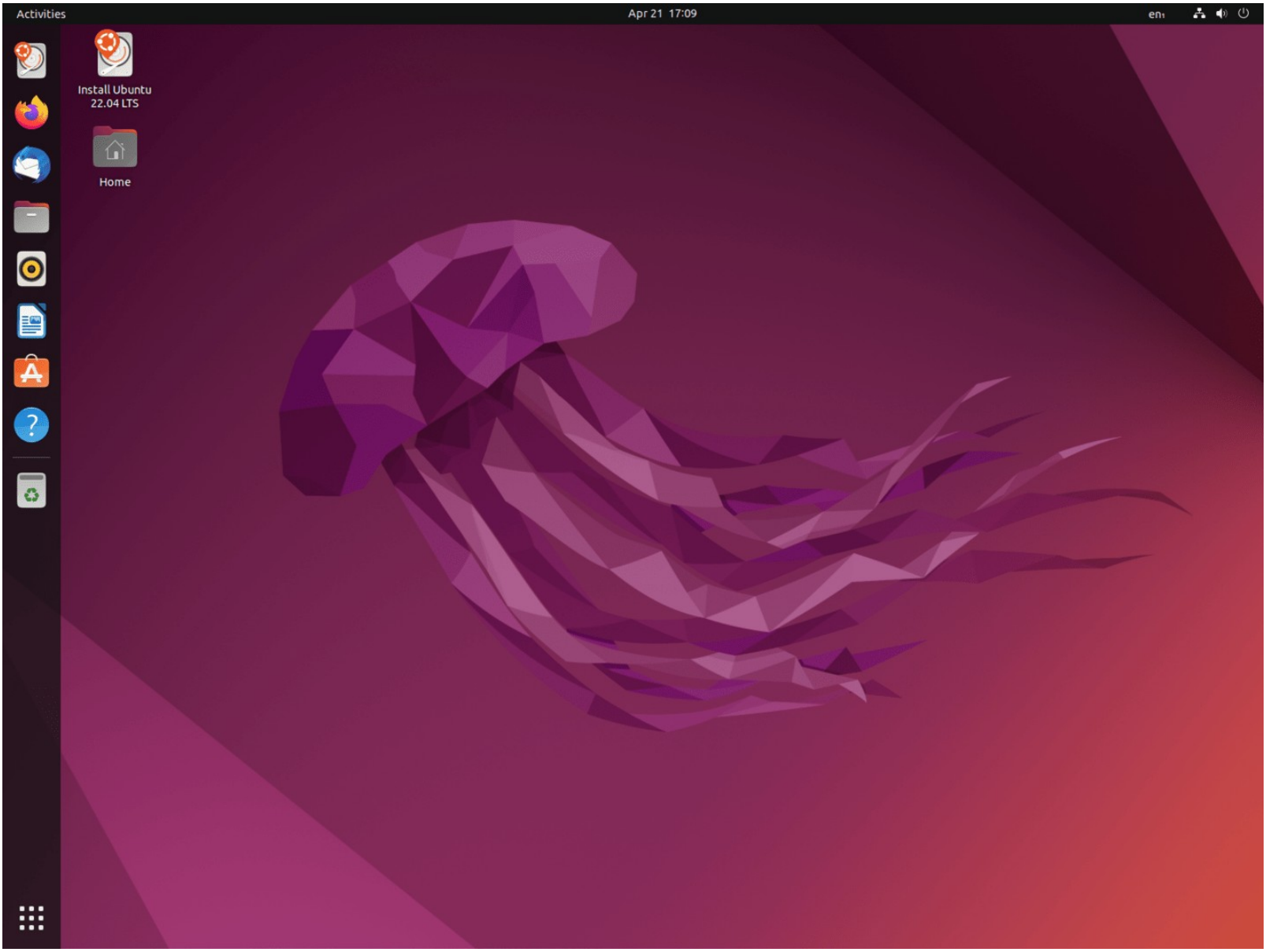
First, create a bootable USB with the Linux OS of your choice, you will need to install a program called Balena Etcher, or similar. This program works on Windows, macOS and Linux and is extremely easy to use. **Follow the steps in the first paragraph** on installing Ubuntu to see detailed step by step guide to create a boot disk and how to install the new OS using that boot disk (USB.) If insure, you can 'Try Ubuntu' instead to test drive the new OS before committing. Once you install, remove the USB drive when prompted and reboot, and begin using your new Linux OS.

- Download Balena Etcher to create your boot disk **here**



*Note, depending on your current machine settings, you may need to enable 'Boot from USB' in the BIOS or UEFI menu, which can be reached easily by powering computer off, then turning back on while holding the Windows super key, Shift bar, or F2 (look up your specific machine to find out how to boot to BIOS menu if one of those won't work) Often the system will recognize bootable USB on startup which you can select for a few seconds during boot process, boot to the USB with Ubuntu .iso on it. If it won't boot, go into BIOS / UEFI and check setting there.

toolkit@privacy:~$ If you chose Ubuntu (22.04 LTS is the latest,) here is an image of your default desktop, you can add/remove apps on the left tray with ones that you use frequently. Switching to Linux can be done in small, bite size chunks, and a small amount of time investment here and there using the new OS will have you comfortable using Linux for all of your daily tasks within about a month or so for many people.



toolkit@privacy:~$ Now that you have a new OS, how do you get apps? With Linux, you have many options, not just Windows or Apple stores, so in short, there is no real one stop shop for everything. I try to steer people away from using Snap store, and towards others, here is a good quick explanation of what app repositories and packages are for Linux: https://fosspost.org/app-packages-linux-snap-flatpak-appimage/

With Linux, you have full control over your system unlike Windows/Apple ecosystems, and with that power comes the ability to install apps from untrustworthy sources without the typical warnings from Microsoft or Apple, so before installing anything unknown, do a basic search to ensure you get the app you need from a trustworthy source.

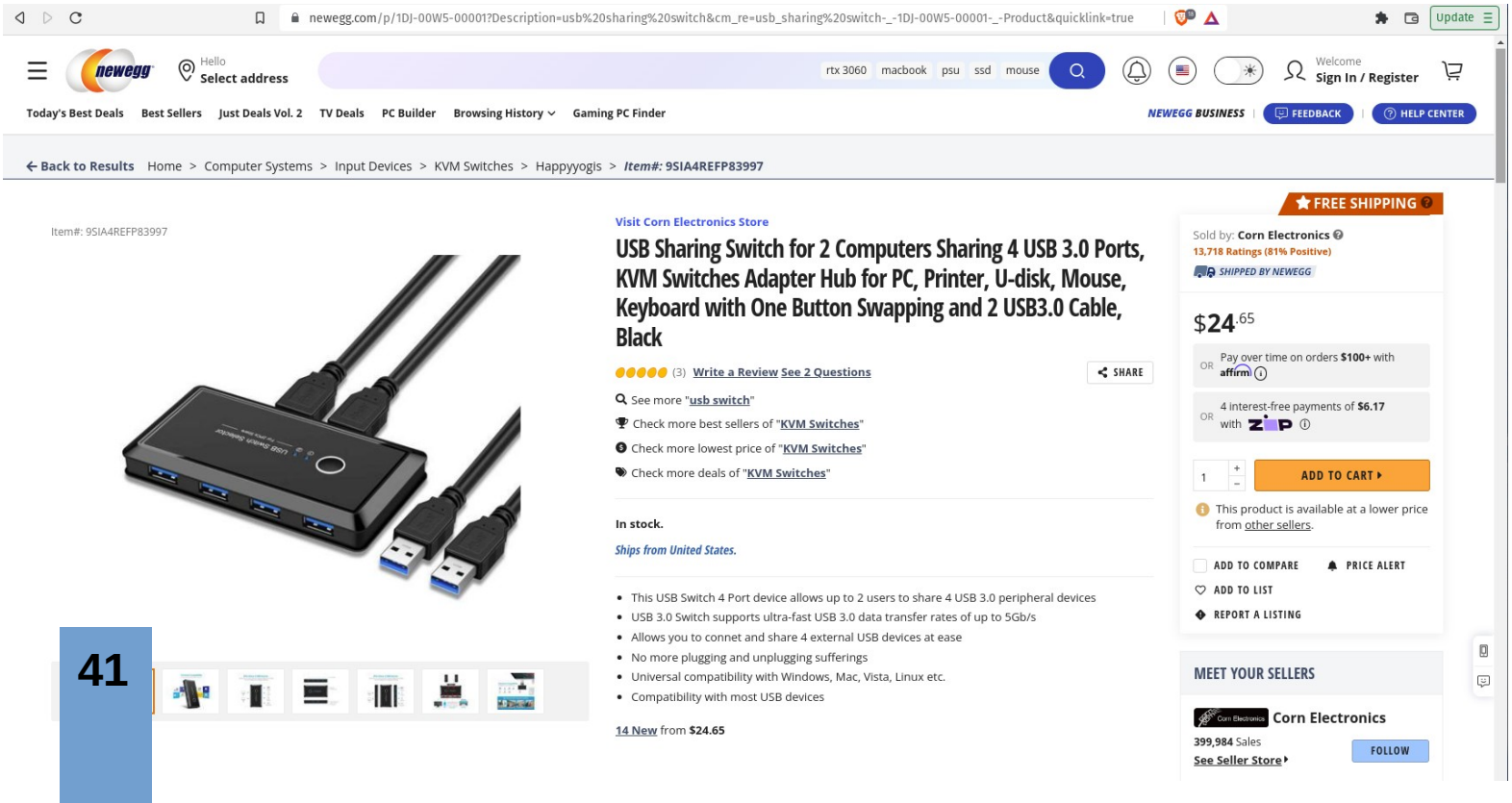
Here is another more advanced collection of information on this topic: https://www.makeuseof.com/tag/migrating-from-windows-7-to-ubuntu/

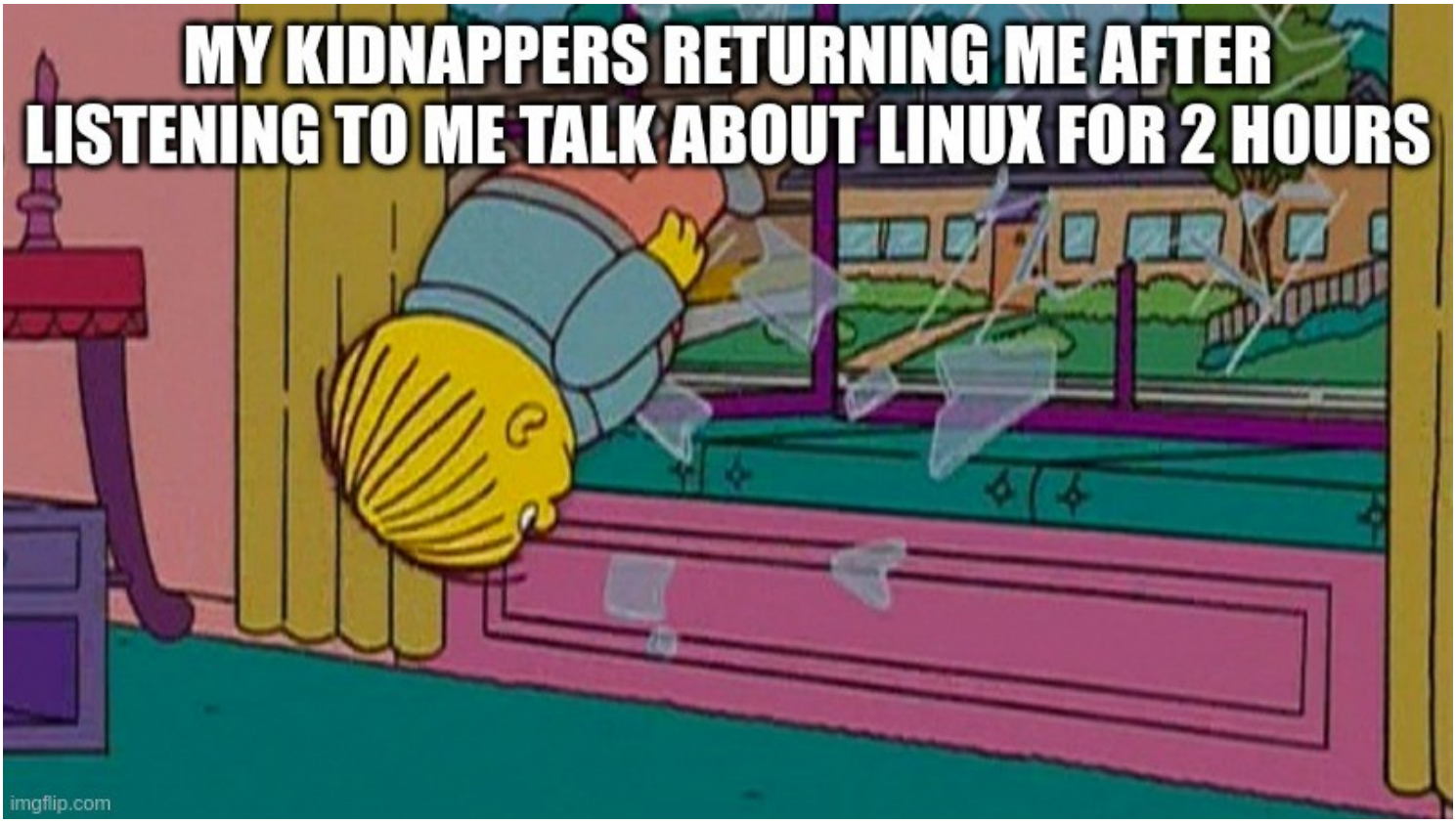
toolkit@privacy:~$ One method that I use and highly recommend to those choosing to make the switch to Linux, is to use a **USB switch.** The single monitor versions of these are extremely cheap. For dual monitor, you will have to spend much more. This device allows you to quickly cycle between two different computers with a push of a single button. When starting out myself, I installed Ubuntu on a cheap laptop, and plugged it into this switch, as well as my Microsoft Windows 10 desktop. You plug your mouse, keyboard, printer, monitor, and anything else you need into the switch, turn on both machines, and you now have a very easy way to have your daily driver machine and your new Linux OS up and running. Try to do as much as you can on Linux, and if you get in a hurry, or get frustrated, simply push the button and revert back to your regular machine instantly.

Using this trick helped me immensely, and allowed me to learn without interrupting anything important, or urgent/time sensitive. Within about a month, I installed Linux onto the Windows desktop (dual boot) and have never logged onto Windows since. The first things I noticed was how fast Linux ran, it is much more efficient just due to the fact that it's not running near as many unwanted programs in the background. Just like with a de-Googled phone, you are now in control of the device. No more forced updates, everything is on your terms. You shift the tech paradigm towards free and open source software, knowing what your machine is doing, and away from proprietary and abusive big tech operating systems. Whoever controls the operating system controls the device. With Windows/Apple, the one in control *ain't you.* With Linux, you are in control and can see everything that is happening on your machine, this should be the accepted standard.

Of note, you don't need a hardware switch to do this, it can be done with software instead. However, using a hardware switch is much easier to set up two computers for someone who is less tech savvy. Read more about using a software switch if you want to try that out:

https://www.makeuseof.com/tag/why-you-no-longer-need-a-kvm-switch-for-your-multi-pc-setup/

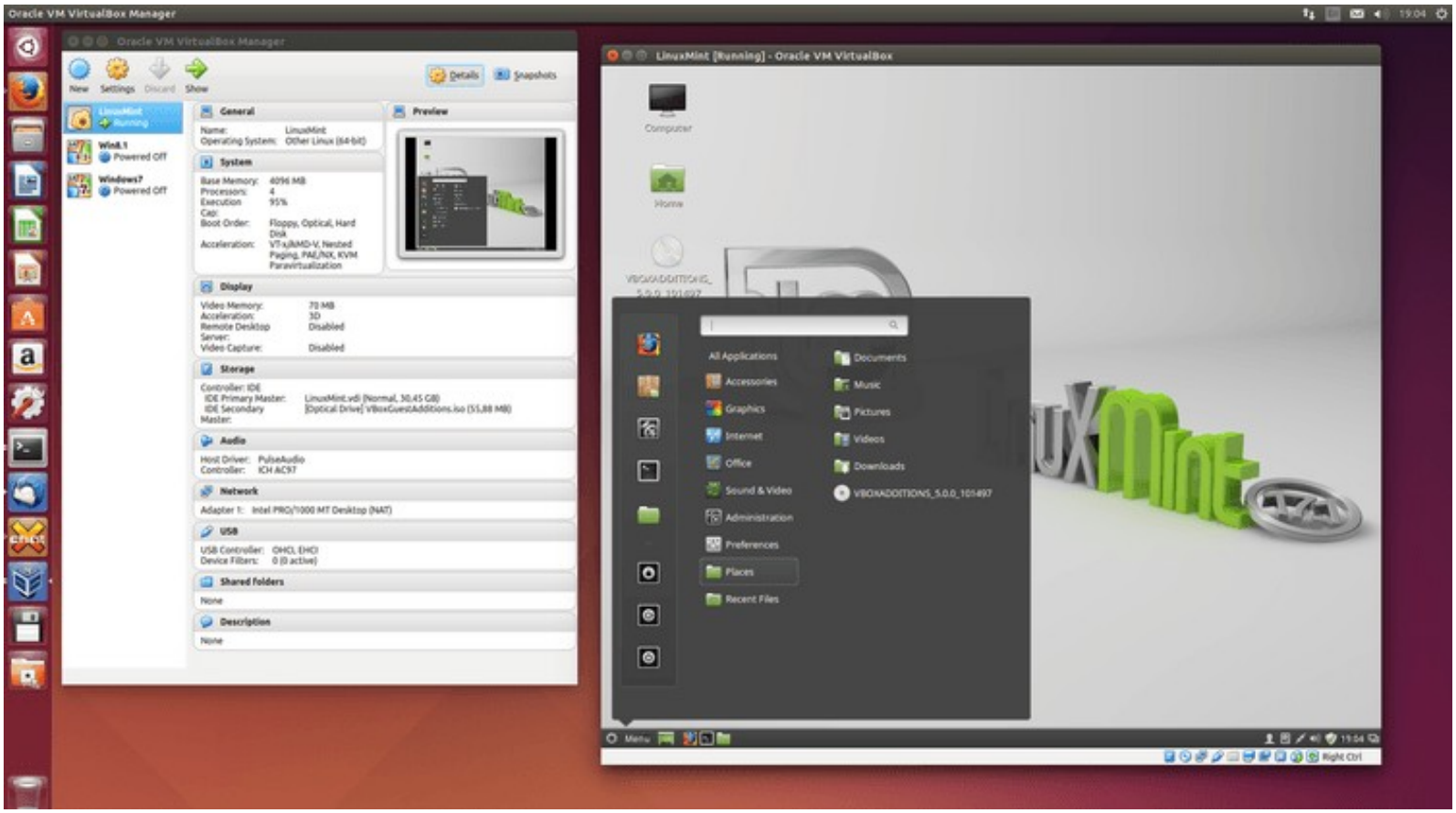




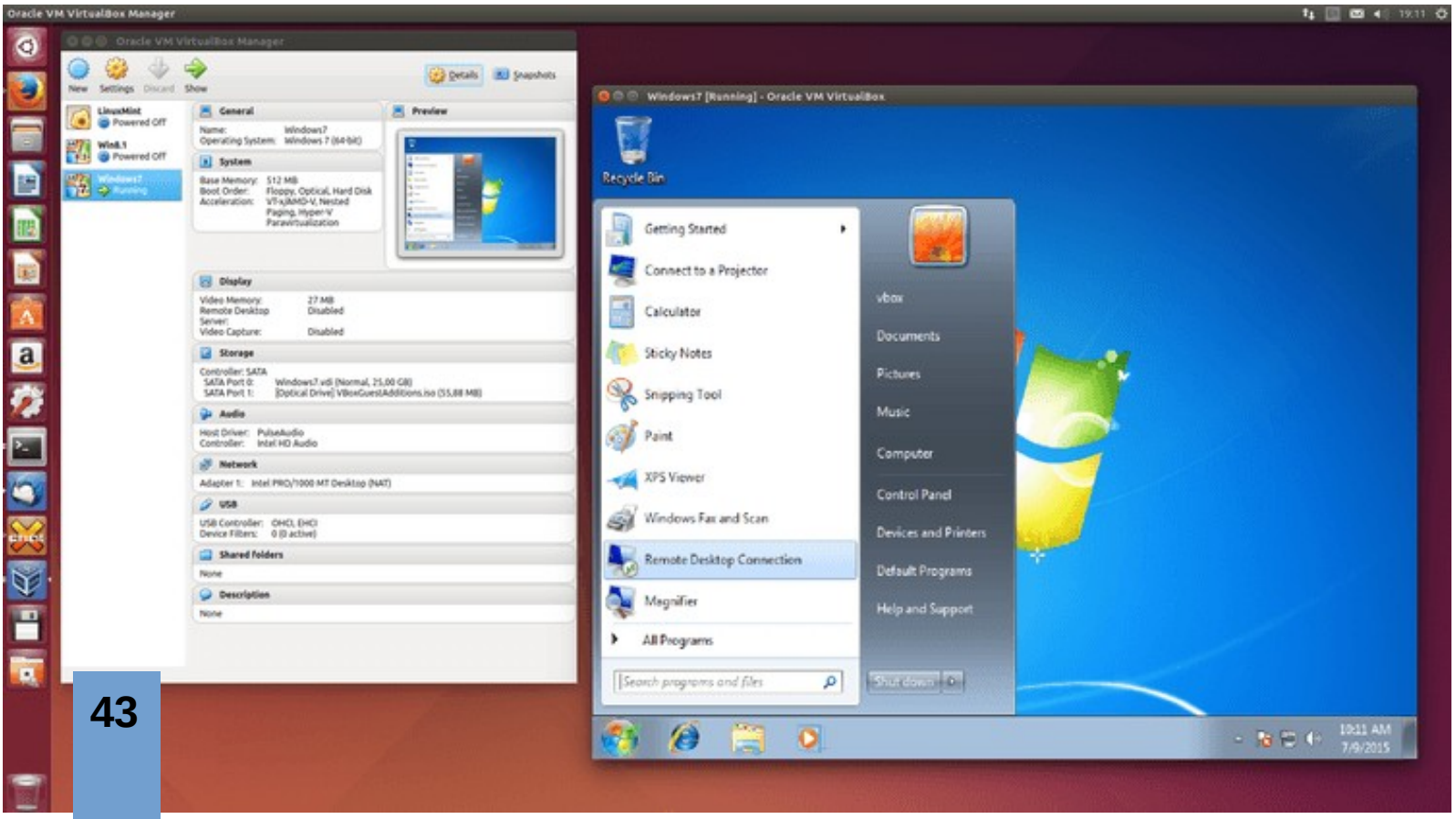
toolkit@privacy:~$ If you want to kick off a hornet's nest on any Linux forum, chat, channel, etc… simply state that [fill in the blank] OS is the best Linux OS there is. Watch a firestorm ensue as people rush to defend the honor of their favorite systems. While we can easily get overwhelmed with the number of Operating Systems and Desktop Environments available in the Linux ecosystem (growing even more numerous as more continue to be introduced, and existing ones updated) you'll start noticing many similarities among the various versions. Start with one, stick with it for a little while, and as you get time, consider exploring others. You are no longer trapped into one of two big tech OS's, you now have complete freedom to customize and use whatever suits your needs.

One way to do this quickly and easily, is to use **Virtual Machines (VM's)** which are essentially a computer, inside of your host computer. In other words, you can use one of several available VM software programs to create unlimited amounts of 'guest' computer OS's on your existing 'host' hardware machine. One of the more popular ones is **Oracle's Virtual Box** software, install it on your host machine, and then 'roll your own' guest OS. I currently use Pop!OS Linux for my daily driver, and within that using Virtual Box, I have about a dozen various computers for different purposes, these are excellent for isolating identities with online accounts/use, and for testing various things. This is a great way to quickly try out a new OS to see if it's worth your time, before installing it on 'bare metal' (onto your host machine.) The beauty of VM's is that they are easy to simply 'light on fire' (delete) and make a new one at any time, while still having your host computer up and running normally. The VM uses your host system's resources such as the processer, memory, internet, etc, but does so in an isolated fashion so as to keep them completely separate. I do setup shared folders between the guest and host machines, and enable 'bi-directional' copy/paste function to quickly transfer files or username/passwords between systems, so there is some interoperability possible.

toolkit@privacy:~$ Here we have as an example, several screenshots of Oracle Virtual Box software, the first one with Linux Mint running on the host computer which is Ubuntu.



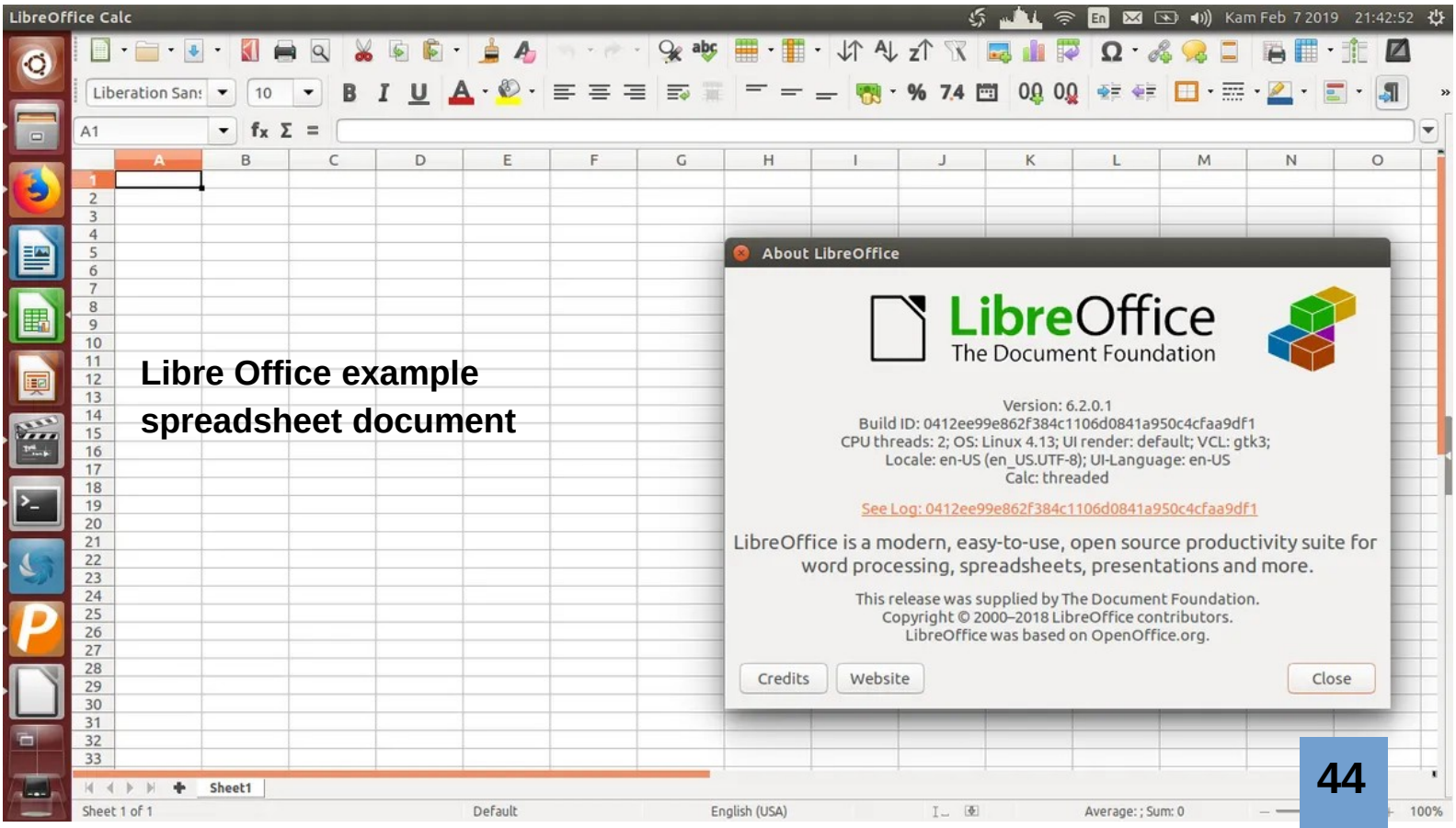
toolkit@privacy:~$ Here we have the same host computer (Ubuntu) running Windows 7 as a Virtual Machine, you are not just limited to Linux with VM software. Virtual Box software will let you create any type of OS, Linux, macOS or Windows.



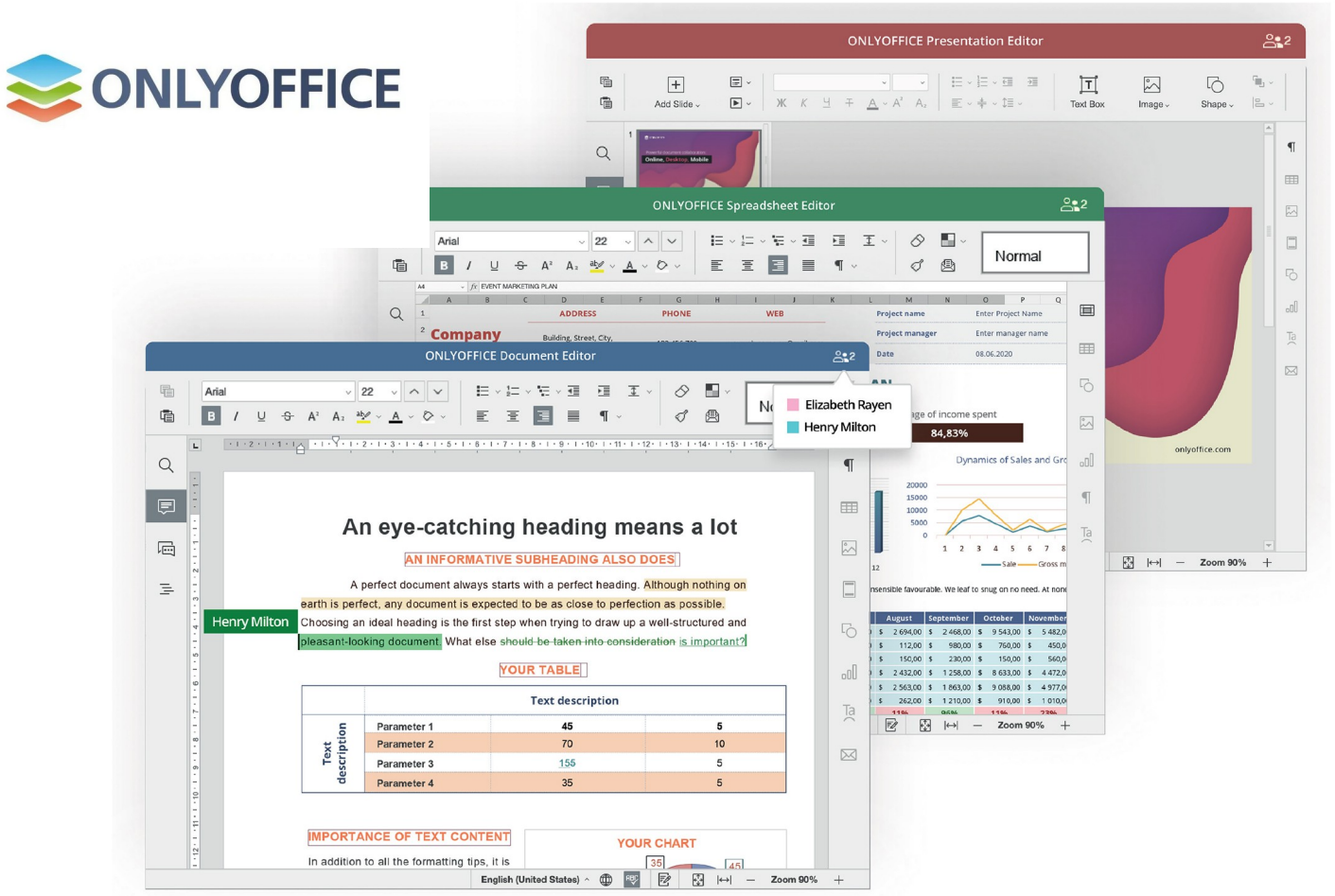
Libre Office and Only Office

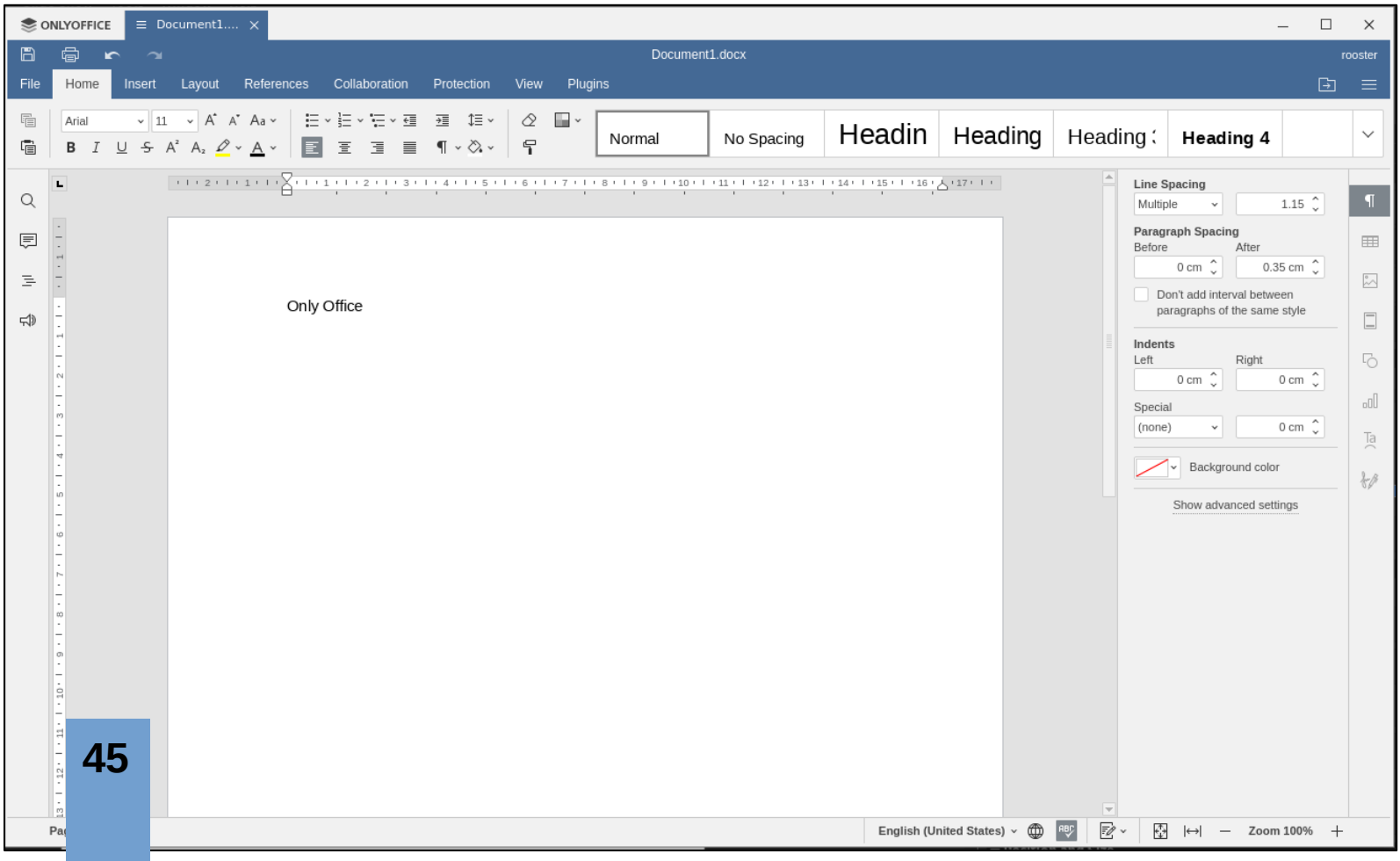
toolkit@privacy:~$ If you start using Linux systems, you will need a replacement for **Microsoft Office 365 (Word, Excel, PowerPoint, etc.)** The two best alternatives are Libre Office and Only Office. Both programs are free and open source software (FOSS) that will not spy on you, analyze your keystrokes, or execute any other unwanted privacy intrusions. The great news is that Libre Office likely is already installed on your Linux machine, it comes standard with many distributions. Tap the Windows logo key (superkey,) and type “Libre” and you should see several options for document, spreadsheet, impress, etc. Libre Office is my go to, but Only Office functions very well also, and looks even more like MS Office 365 products, give them both a try. Not having Microsoft collecting all of the things and ways you type and use their products leaves me wanting both of these apps to gain a huge leap in privacy from these abusive tech giants, and with absolutely no subscriptions or fees. You can open and edit MS Office 365 documents as well with these software products. No cost.

Only Office download

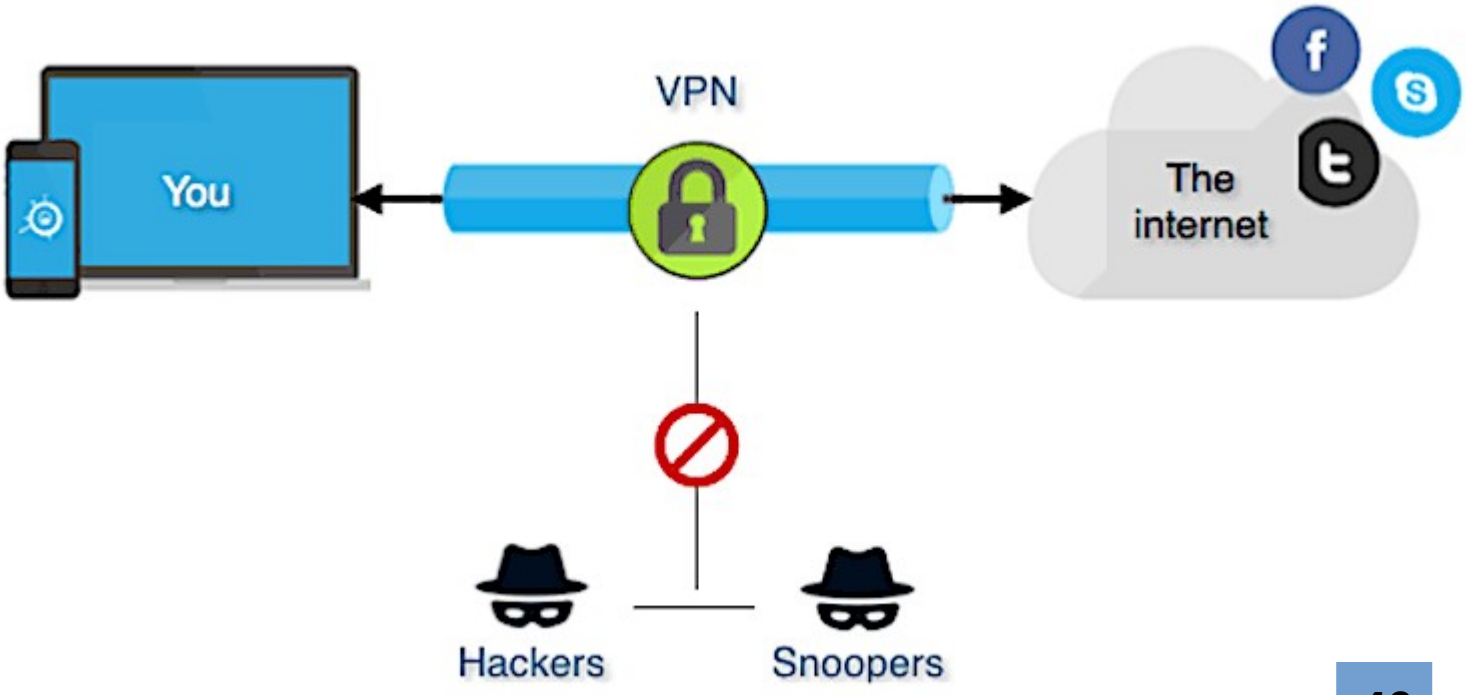


Libre Office example spreadsheet document


ONLYOFFICE
ONLYOFFICE Presentation Editor
ONLYOFFICE Spreadsheet Editor
ONLYOFFICE Document Editor
An eye-catching heading means a lot
AN INFORMATIVE SUBHEADING ALSO DOES
Henry Milton
YOUR TABLE
Text description
IMPORTANCE OF TEXT CONTENT
YOUR CHART
Elizabeth Rayen
Henry Milton

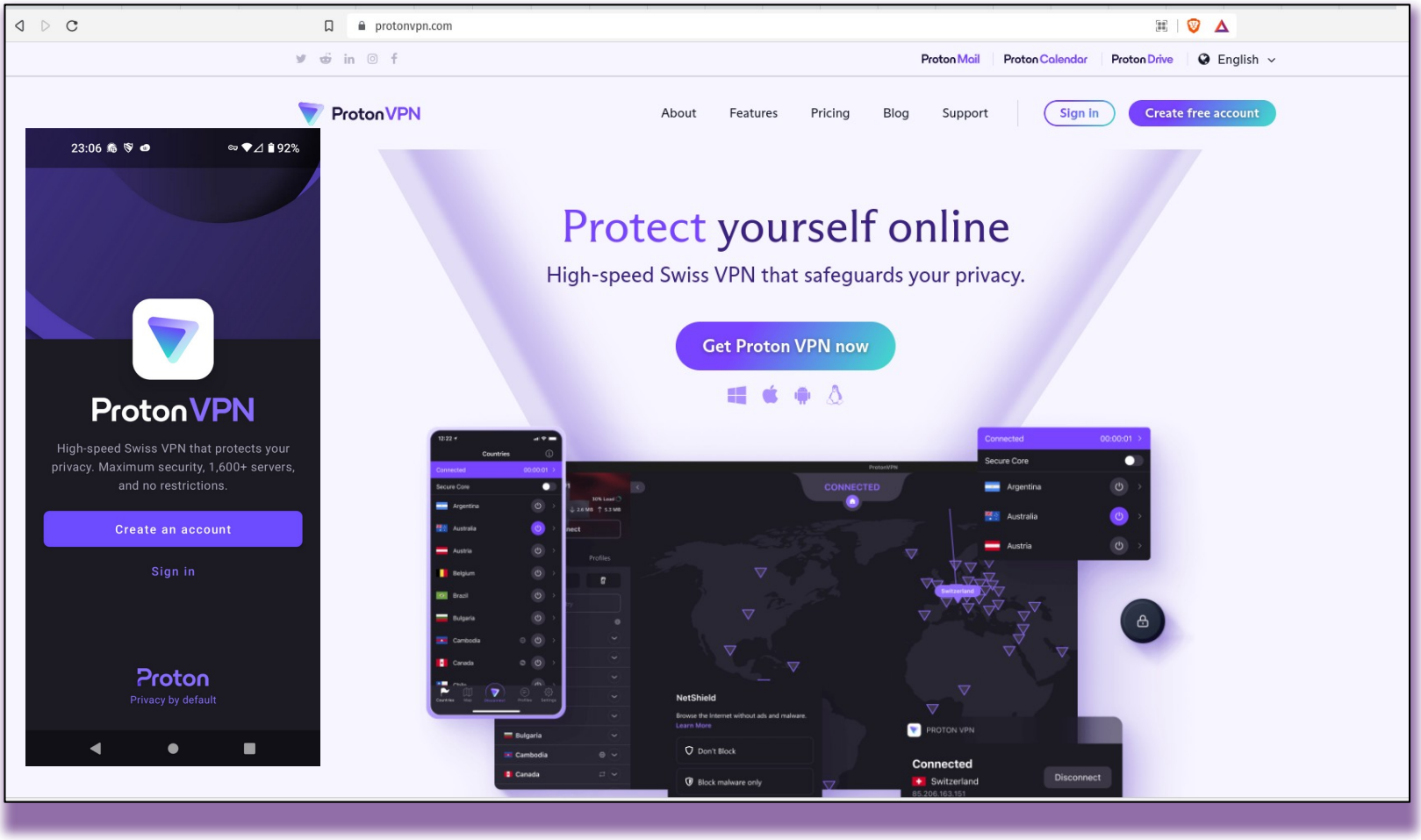

ONLYOFFICE
Document1....
Document1.docx
rooster
File
Home
Insert
Layout
References
Collaboration
Protection
View
Plugins
Normal
No Spacing
Heading 4
Only Office
Line Spacing
Multiple
1.15
Paragraph Spacing
Before
After
0 cm
0.35 cm
Don't add interval between paragraphs of the same style
Indents
Left
Right
Special
(none)
Background color
Show advanced settings
English (United States)
Zoom 100%

Virtual Private Networks (VPN's)



ProtonVPN, Private Internet Access (PIA)

toolkit@privacy:~$ **ProtonVPN** offers an excellent VPN service for a wide variety of reasons, including fair price, excellent service, they are based in a country with little ability for US to force Proton to give over any information on their users, and do the best they can to limit the amount of necessary data required to be collected on a user's account. Many folks choose Proton or **PIA**, but others exist such as Mullvad where they will actually accept cash in the mail for an account to keep your stuff anonymous the old school way. No matter what, always using a VPN will greatly protect you from the ISP seeing and recording (and likely selling) your browsing history forever and ever. Give them nothing ! Use a VPN. This is an excellent quick read to understand who owns various VPN services: https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/



You need a VPN!

toolkit@privacy:~$ Many of you already use a VPN to connect to the internet and mask your online activity but if you are not already using a VPN, read on for why you need one. Without one, all of your online activity is visible to your ISP (Internet Service Provider) and they also may store and sell that data. A VPN hides your traffic, using one creates a tunnel between you and the sites you visit to mask your activity from the ISP, otherwise they see every single site you visit. If you visit a site with your true IP address, the site also sees exactly who you are and may log your activity. To keep this section short, whether you want to hide your activity or not, you should, as best practice. While you may not do anything nefarious online, one day the things you search for, or the sites you visit could easily be labeled nefarious, or outright or defacto illegal. How far back will that reach? Months? Years? Say you searched for a topic five years ago, it's been logged, and suddenly that topic is off limits. Who is to say that an over reaching company and/or government won't look backwards to get an idea of who to put on a naughty list? We are not just thinking about the present, but forward thinking to avoid our present activity being used against our future selves in any way.

One thing to keep in mind also is that most VPN companies also will log your IP address and activity/connections, but hopefully keep that information private unless demanded by law enforcement. For maximum privacy, VPN's can be purchased completely anonymously with cash, cryptocurrency or anonymous credit cards to make it more difficult to trace that VPN connection back to your true identity. Should an entity gain access to the VPN company's logs, your identity is preserved. Some VPN companies sell their clients' activity to other parties, so do your homework on the provider you choose to trust.

Hiding your internet activity is only to your benefit, there is no disadvantage other than the cost of a VPN (relatively inexpensive though) and perhaps some slower speeds, but usually not enough to be an issue for most of us. Some may fall back to the "I have nothing to hide" mantra, which we've already touched on to some length. In a free society, we have the distinction between a public and private self, where we enjoy privacy. In an authoritarian society, there is little privacy. Do you want to be put onto lists, just based on your internet search history?

Need more reasons why you need a VPN? Not only does using one gain you privacy from the ISP, but also government, hackers, when using public WiFi, but also from many apps such as Facebook which harvest your activity and track you across the web. VPN's also provide a layer of security for working remotely, I used one provided to me while working in government to access and share data remotely. The VPN encryption helps boost the security of sending traffic over the internet. Another reason is to simply have the ability to view content that may be prohibited in your country. Some countries ban various apps and websites that are legitimate, using a VPN server from another country circumvents some of that censorship control, and allows the user to access more content.

You need a *paid* VPN!

toolkit@privacy:~$ Avoid free VPN services, they pay the bills by selling your data. This is a good way to increase your chances of a breach of privacy or security. Always use a paid service, most cost less than $7/month, often less, especially when you pay for a longer period. Buy a plan that supports enough devices that can be used on one account. (a family of four may want at least ten connections for phones, laptops, etc.)

If I had to pick just one for most people, Proton VPN would be my first choice, they offer a free account but the paid version offers better speeds and more server choices, although I still maintain a PIA account as well. Mullvad is another good one for anonymity, they actually still accept cash as a payment method, although speeds vary for people with each of these choices. One advantage with PIA is that they offer a 'dedicated IP address' which can be useful for online shopping or banking to satisfy some of the anti-fraud software systems in place, although this option is slightly more expensive.

On my own home internet, I protect my traffic with a **pfSense** firewall box, this is free software installed on a small machine between the incoming internet and my devices. Instead of having to install VPN's on each device I use, it is installed onto the pfSense box, and anything that connects to it is behind my VPN. This also helps prevent IP address leaks, in the brief moments where you have internet, but before your VPN service starts, the ISP can see a surprising amount of your data. There exists a wide variety of options for using a pfSense home firewall, for moderately savvy users, I highly recommend trying this route out for securing your own home internet traffic.

****Learn more about pfSense home firewall here for more advanced users**

You can also build your own VPN:
https://forums.lawrencesystems.com/t/getting-started-building-your-own-wireguard-vpn-server/7425

https://techcrunch.com/2017/04/09/how-i-made-my-own-vpn-server-in-15-minutes/

4-Port Protectli firewall box

Internet Browsers

Internet Browsers

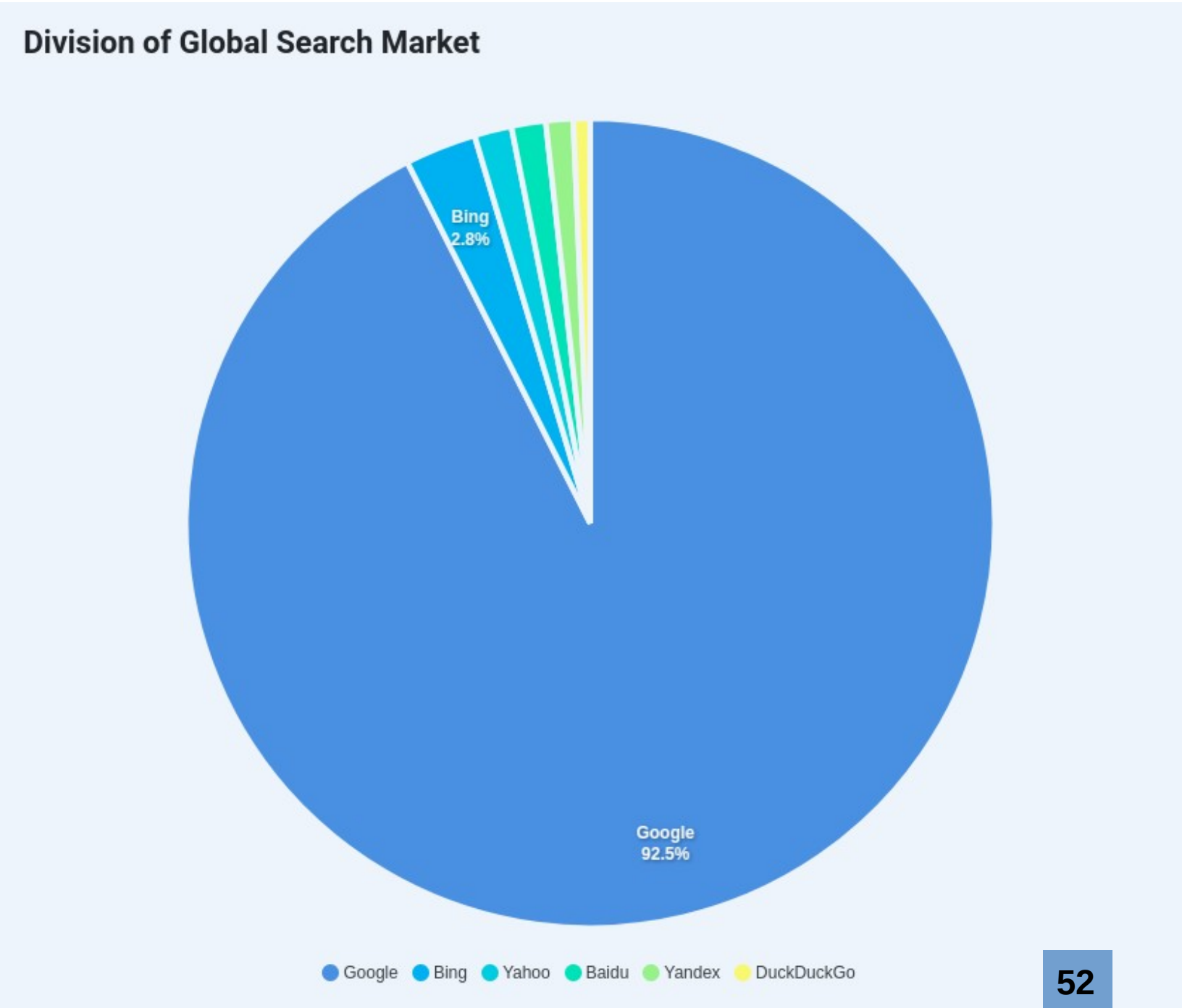
toolkit@privacy:~$ What does your internet browser collect about you? Which browsers censor content from you as you search? Without going into too much technical detail on each one, here is a brief list of browsers that offer increased protection from data collection as well as better search results for various topics, although many argue about which one is better, or which one is better for privacy. Google dominates the search engine space, something like 93%, however they collect a ton of data on your usage and use that information to throttle certain content, and promote other content. This manipulation of search results has gotten quite frightening. Google has used things like FloC (Federated Learning of Cohorts) and has supposedly moved onto a different version, Topics, learn more about this not so comforting profiling of us is **here** and **here.**

Note that a browser is not a search engine, they are two different things. Many people will swear that they left Google and only use DuckDuckGo now; only to visit their search engine in the settings and discover that they are still using Google. Select your browser, and then be sure to check settings under 'Search' and select the search engine of your choice, I prefer Brave/Brave, or FireFox/DDG or Tor for the majority of my internet usage. Tor (The Onion Router) is a different type of browser, I highly recommend using this more often as this offers a huge layer of anonymity when browsing, although know that it takes longer to load. Speed on Tor may get bumped up for the better soon though. Mojeek (UK search engine) offers vastly less biased and censored search results than Google in my testing, try both side by side and see the stark contrast.

Aside from which browsers you use, practice a technique called 'browser isolation' where instead of using one browser window with a ton of tabs, open certain accounts in a separate browser. For example, Amazon and Facebook collect a ton of data about the other sites you have visited, or have open currently in your browser. If you choose to use such intrusive services, open them in their own isolated browser, and do your other computing tasks such as email in a separate browser. Even better, use a different type of browser, example, open Amazon in Firefox, and browse your email in Brave, or vice versa. Rob Braxman explains this tactic in more detail in **this video.**

- **Brave Browser / Brave Search Engine: https://brave.com/**
- **FireFox Browser / DuckDuckGo Search engine: https://www.mozilla.org/en-US/firefox/new/**
- **Tor Browser - https://tb-manual.torproject.org/about/**
- **Privacy Browser / Mojeek Search Engine: https://www.mojeek.com/**
- **Vanadium Browser (Default on GrapheneOS) / Google or DuckDuckGo**
- **FireFox Focus (Android) / Google or DuckDuckGo**
- **Vivaldi Browser: Vivaldi Browser**
- **StartPage (uses Google anonymously): https://www.startpage.com/**

toolkit@privacy:~$ Here is a visual to demonstrate just how much Google search engines are used for the vast majority of traffic, especially in the US. Brave,Tor, Mojeek, and DDG are my favorite answers to help shift this paradigm, away from Google and towards search engines that work for us. None are perfect, and sometimes I do use Google for specific types of searches. Not only is what you see on Google and Bing curated, and based on any attributes it can identify with you, but even more powerful is the search results that you don't see. Lies of omission. This is outright manipulation, and explains the information silos we find ourselves in as a culture. On the next page there is a short 13 minute clip that helps explain these lies of omission, and offer you an example that you can quickly test out for yourself on your own search engines. Couple this with Rob Braxman's videos on Google FLoC concepts, and we can get a feel for how these big tech oligarchs are watching and learning about you. Giving them less data by not using their products, is the simplest solution.

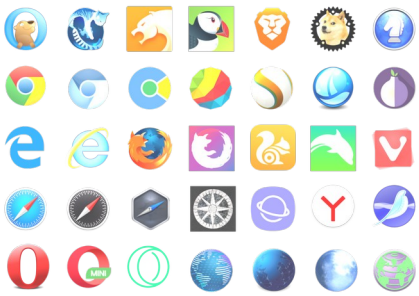


toolkit@privacy:~$ Browsers and search engines have a large influence of how we interact with content, and even can control what we see, or don't see. Using Google is almost sickening to me when I see the search results, often they have little if anything to do with what the search term is, and the amount of results are extremely limited now. Also obvious is the lack of certain information on browsers like Google Chrome, Microsoft Edge, Safari, Bing, etc. Try out Brave, DDG, Mojeek and of course Tor, to see the difference for yourself. (Make sure to try different search engines, not just the different browsers.)

Also worth testing is doing identical searches while connected to various countries using VPN's, you'll quickly see just how much content is changed based on the country where the VPN connection is.

For some provocative thought that is somewhat frightening, and a glimpse of how our searches online are extremely manipulated and limited, watch this 45 minute presentation called **"Where Did the Rest of the Internet Go?"** by TruthStreamMedia:
https://www.youtube.com/watch?v=6zyJB45ewvU

Shorter video here if you don't have much time, watch this 13 minute video that illustrates this: **https://rumble.com/v1fs007-disturbing-proof-theyre-quietly-deleting-the-internet....html** This video shows us some alarming trends in search results, and an explanation for the apparent information silos we find our fellow humans in. With FloC we see how search results can be manipulated and fed to us based on our past online searches and behavior.



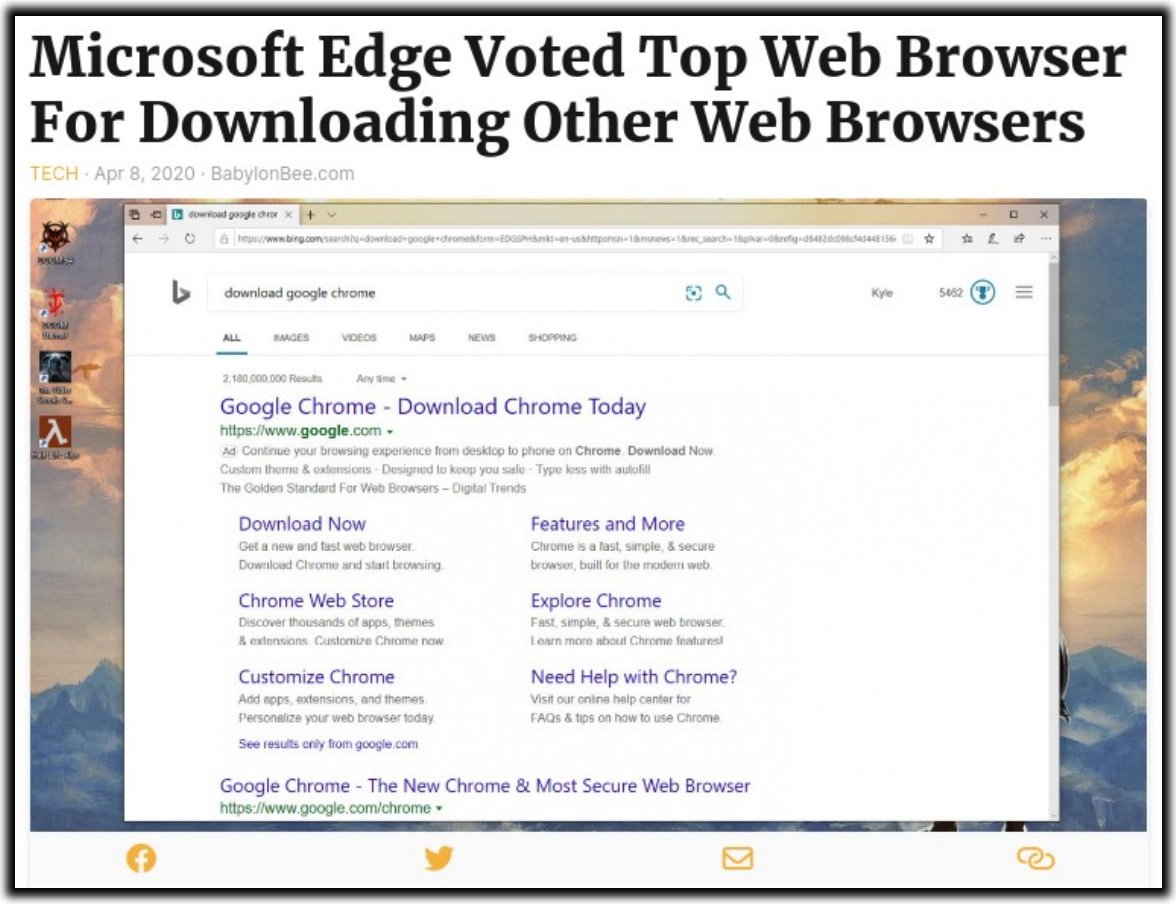
toolkit@privacy:~$ On a desktop, simply navigate to the browser you wish to download and install it to your machine. Click on the Menu icon in upper right within the browser and go to Settings menu, and scroll through to adjust any settings to your liking. I block camera / mic / location, un-check Autofill options for credit card or address type entries, enable HTTPS only, select the search engine of choice such as Brave, DDG, etc.

On a mobile device, Mojeek (search for Privacy Browser) can be found in F-Droid, Brave can be installed via Aurora Store or directly from their website as an APK file if you know which version you need for your device, FireFox Focus is another good option also on Aurora Store, and Vanadium is the default with GrapheneOS. Even if using a stock Android, you can still use these search tools from their respective sources listed above. Be sure to visit the settings menu and set the features you want or don't want on each.

As mentioned, you'll rarely see many agree on which browser and search engine is 'best' for any given topic such as search results or privacy, but these alternative options offer a much better solution than using the big tech search tools. There are many other configurations, these are ones that I have used and tested, find out what you like.

Another hot topic is browser extensions. While there are many great add-ons to enhance privacy and block ads and other unwanted junk, such as u-Block Origin and Privacy Badger, know that those also make you look more like a needle in a haystack of people using stock settings. I don't proclaim to know what is best for anyone, but food for thought. You can test your browser with this handy website from EFF:

https://coveryourtracks.eff.org/



[00:00:00] 1 keys tested (1020.67 k/s)

KEY FOUND! [Cisco123]

Master Key : 4C C0 3F 98 91 C4 4B F3 33 51 C2 8F 2B 43 F2 02
73 19 38 12 C1 8B 1D E6 B9 15 AE 23 36 2D 7F 6A

Transient Key : 80 F5 7F F5 18 F8 E5 41 EA 99 DD 15 3E 12 DB 6A
61 2A E7 8B A4 3B FB 5E E0 80 AB 20 C9 01 59 1B
14 25 BE 52 F0 17 83 C6 0A AE DB B7 A0 25 6E 65
B6 D5 4A DD C9 1D 27 CC 02 05 CC E8 A8 02 35 42

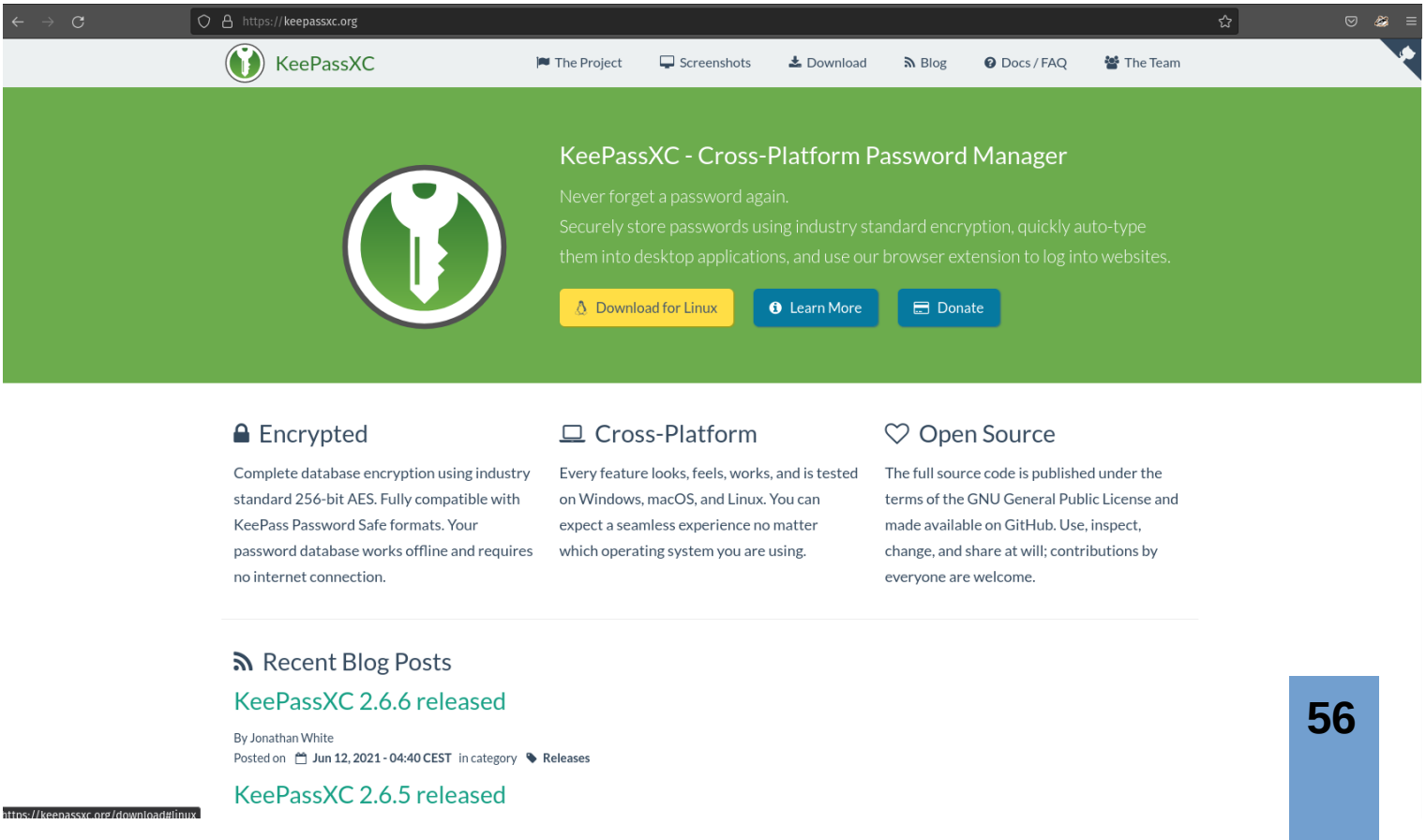
EAPOL HMAC : 69 36 BF 90 43 46 07 20 46 87 26 46 3A 59 A8 26

Password Managers & 2FA

KeePassXC

toolkit@privacy:~$ Be honest, is your workspace cluttered with sticky notes containing your login information for various sites? Perhaps you're like me once upon a time, I used Microsoft Excel to centralize all of my passwords foolishly, only to learn that Microsoft could have complete unfettered access to that data if they wished. Not that I was all that concerned that they would actually abuse it, but certainly there are rogue employees that could at least in theory take advantage of such data. Even if the various entities that have access to your machine don't have dishonest employees, they are frequently targets of successful cyber attacks, which spill our data and credentials into the wrong hands. I also toss this question at folks; if your sticky notes, laptop and phone disappeared for some reason, such as fire or theft, **do you have a file saved somewhere to recover or access all of your digital life?**

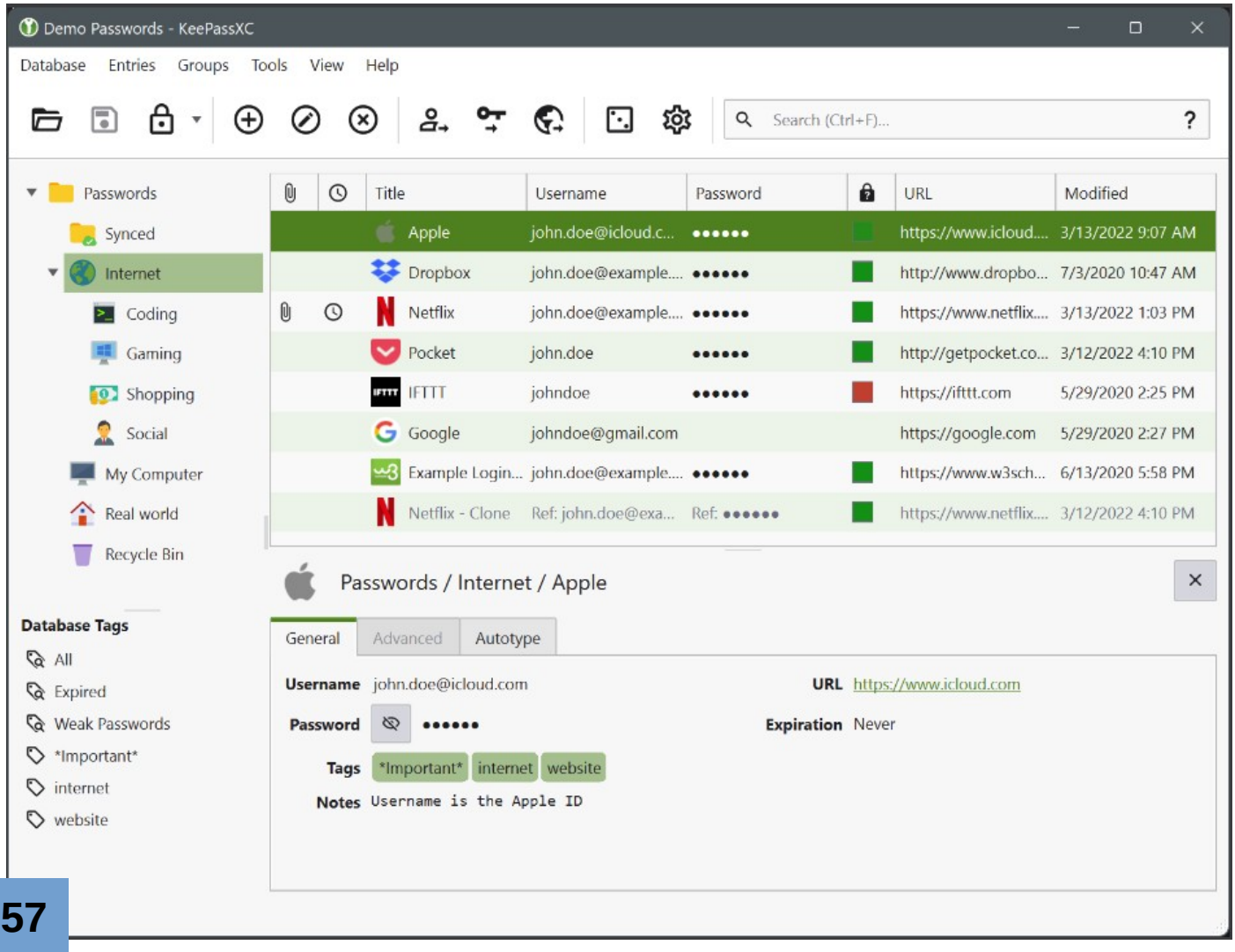
Today I use a dedicated password manager, a software program that stores your login credentials for you in a single database file, that file being locked with a password of its own. Today I only have to remember one password to access my entire digital life, I don't even know what my passwords are for my hundreds of accounts. I rely on the password manager, in my case a program called **KeePassXC**, to do the work for me, and centralize all of my login credentials. On the next page I'll go over some basics of passwords themselves, and some strategies for using a password manager in an effective way that should suit most of us for our digital lives.



toolkit@privacy:~$ **KeePassXC** and other similar password managers are very easy to install and use on all of your desktop devices. Navigate to **https://keepassxc.org/** and download the version of the manager for your system. This will allow you to create as many databases as you wish, and provide you the ability to open KDBX files containing your passwords. These databases can be stored on your local machine, however I keep mine stored on a USB stick which I keep with me, and can then use on any of my devices to access my accounts at any time. I also maintain a backup USB drive with a copy of the database file, never rely on a single piece of hardware or single file. You could also keep a backup on a secure cloud service, such as Proton Drive, which would help protect your database from physical damage or loss, but only use a service you trust.

KeePassXC can also store notes, attachments, URL's and anything else about your accounts, not just login credentials. I'll frequently add entries to my database for various devices, such as my phone, with the PIN and passwords for the various apps on my phone, notes about when I signed up for a service, when payment is due, or which email/phone number I used to sign up for that service or app.

A KeePassXC database example:

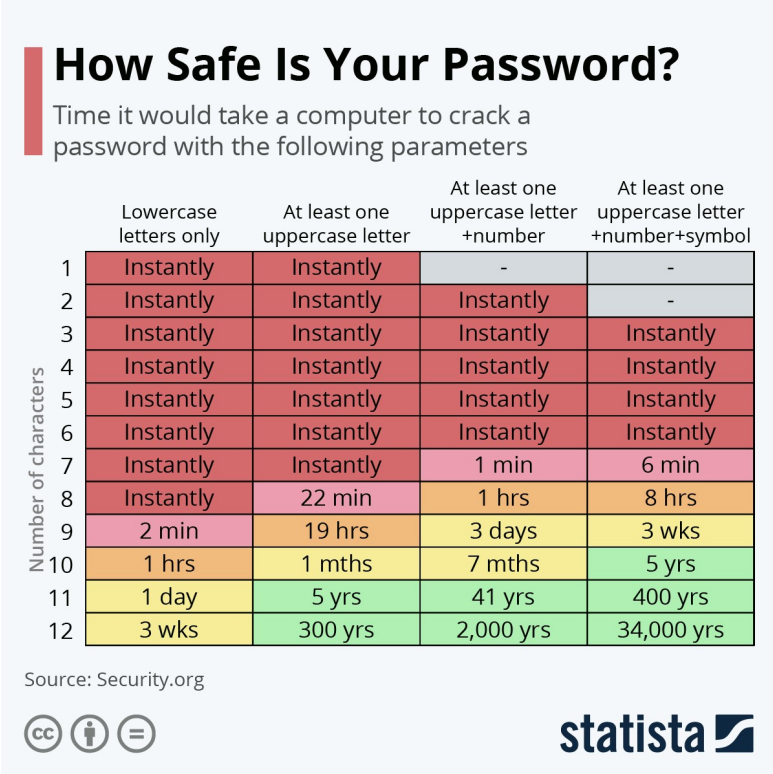


Password guide for maximum security:

toolkit@privacy:~$ 1. **Guard your password database both physically and digitally.** If someone gains access to the locked file, they still need to know the password, but should anyone gain access, they will have free reign of your digital life. Having a good strong master password, and storing the file on a removable device (USB drive, SD cards, etc) kept in secure locations are good practices to avoid the worst case scenario. When not in use, remove the media and keep with you or lock it up to avoid theft and damage.

2. **Always back up your password database.** You are putting most of your eggs in one basket here as mentioned above, so make copies on separate removable media devices and keep in several different secure places. Consider giving an encrypted USB with a backup to a friend that you trust. (See 'Data Encryption' section for combining encryption strategies with password managers.) Update them often as you change and add new passwords, setting up a routine may be helpful to remember to do this. Example, I store a copy in a VeraCrypt container on my daily driver external hard drive, and keep three separate USB sticks that also have copies of the database, and different physical locations.

3. **Use long character passwords** with the typical use of upper case, lower case, number and symbol combination (using at least one of each.) The longer the password, the more secure, assuming all else equal.



4. **Never use the same password on different accounts.** By using a local password manager, you only have to remember one password to unlock your database, and then copy/paste the unique password into the login box for each account. This adds a good layer of security to your accounts, as hackers can use breach data to quickly attempt known passwords attributed to you on other accounts you own, to attempt access. Example, you use the same password for Facebook and your Gmail account; if a hacker gains access to one of the accounts, they can quickly discover the other account with little effort, and attempt the same or similar passwords, don't get owned by using the same password, **or recycling old passwords**, even on different accounts. Use the random password generator in KeePassXC if you have trouble creating a strong password on your own.

5. **Add the date you updated your database in the file name to help keep track of things.** If you choose to separate and do multiple databases as outlined below in section 6, it is helpful to name them in a way to easily differentiate them as well. Example, your database for daily/common use for email and social media could be labeled ‘DAILY DRIVER Database (13 Nov 2022)’ and another one for less used accounts as ‘Database 2 (13 Nov 2022)’ and continue to change the date as you update/save them. I frequently will not delete old databases for a while until I’m certain I’ve updated them properly across all USB sticks. Instead, I will simply save the old one in a folder labeled ‘zz.Archived’ and click ‘Save Database as…’ with the updated date. This way, if you accidentally update entries incorrectly across your USB sticks, you can fall back on older ones to ensure the current entries are up to date if you make a mistake on an entry, or forget to save the file correctly. The ‘zz.Archived’ naming strategy is to put the folder at the bottom or end of your string of files, out of the way, this is just a personal habit I use.

6. **You can create and manage as many database files as you want.** This can be used to compartmentalize various accounts. Example, you could have a database file for all of your social media accounts, a separate one for banking, and so on. They would ideally have different master passwords, but you may wish to simply use one password for all databases, but keep certain ones detached from your computer unless in use, such as banking accounts. The stuff you use daily/continuously, you could store in its own database on your machine, with backups on USB drives kept elsewhere, and/or in a trusted cloud service.

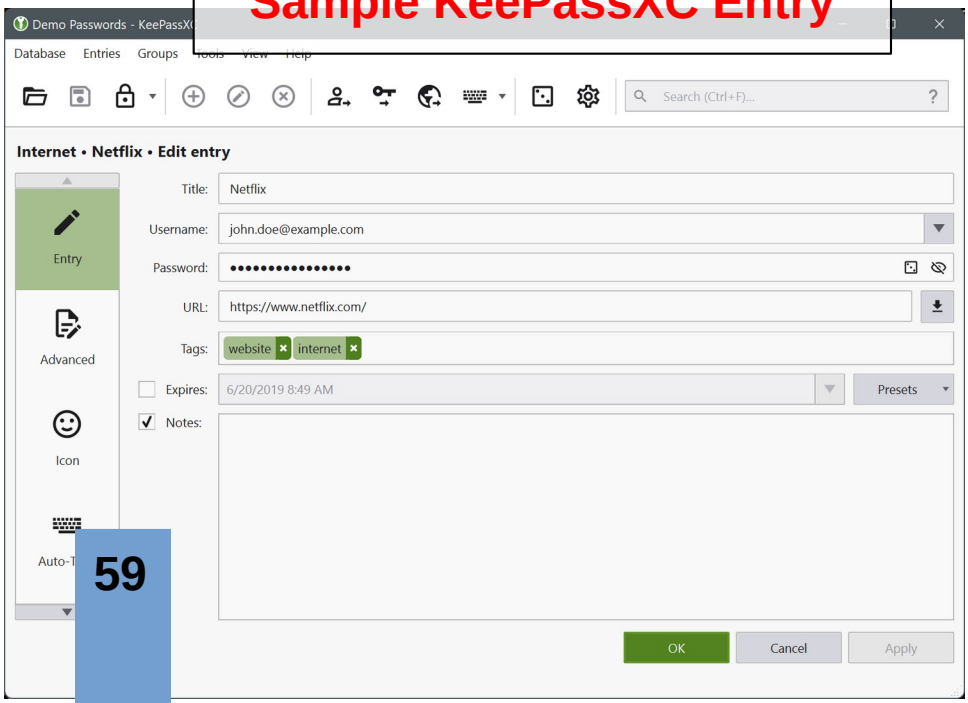
7. **Change your passwords periodically**, and as mentioned, never recycle old passwords, use new ones. With a password manager, this is a one click, easy task by using the password generator within the app.

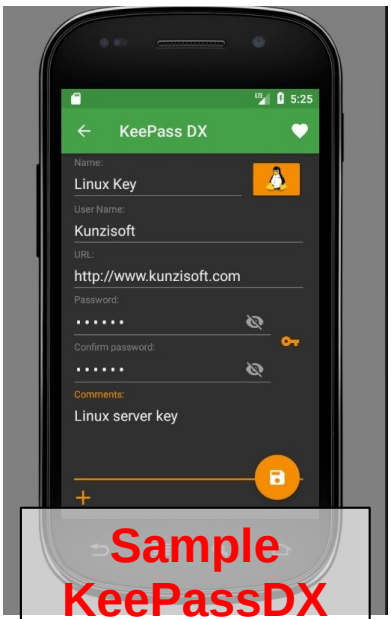
Download KeePassXC program for Linux, Windows or macOS **here**

View the User Guide for detailed instructions and FAQ’s **here**

The program works across Linux, Windows and macOS, and can be opened on a mobile with a separate application called **KeyPassDX here**

Sample KeePassXC Entry





Sample KeePassDX Entry

2FA (Two Factor Authentication)

(Also referred to as MFA, Multi-Factor Authentication)

toolkit@privacy:~$ So you use a username, and strong login password to access your online account, one that is very important to you. A bank, cryptocurrency account, or something you really cannot afford to have compromised. While a good strong password goes a long way, 2FA is exponentially stronger at keeping unwanted 'visitors' from gaining access to your important accounts. 2FA adds a second method of authentication in order to gain access to your account, so, in addition to username/password, you should set your accounts to also require a second method, such as an SMS text (poor choice but usually better than nothing), security questions (OK), another password or by use of a TOTP (Temporary One Time Password) (good,) Software Token, or Hardware Token (Excellent.)

SMS Text verification has the possibility of being hijacked by a 'SIM swap attack' which can be possibly thwarted by putting a PIN lock on your SIM card with your cell carrier. Using a SIM Text or Link Verification code will link your phone to your other device, if you want to avoid that privacy intrusion, try one of the others listed below instead for better privacy and security. Best practice is to not link your phone to anything you don't have to.

2nd Password verification is decent, but not a very common method in many apps.

TOTP is offered by more apps, but many are tied to SMS messaging, however those through email are considered better, and a good option for 2FA.

Software Token, this is another program that you install on your machine such as Authy, or Authenticator among others, which requires a TOTP for each login after you enter username/password, and offers excellent increased account protection.

Hardware Tokens are the holy grail of 2FA for the average user, this requires a physical digital token device that is plugged into a USB port when logging in, without this hardware key, even if someone hacks your username/password, won't be able to access your account without physical access to this hardware token. **Yubikey** is an industry leader in making commercial grade hardware tokens for computers and smartphones, but other methods exist, such as credit card looking RFID reader cards as the token. Yubikey is my suggestion, and if you go this route, buy at least two of them, if not three, to ensure you have backups to avoid locking yourself out should one key get lost or destroyed. Yubikey allows you to clone up to five keys for each account(s.)

Yubikey

Data Encryption

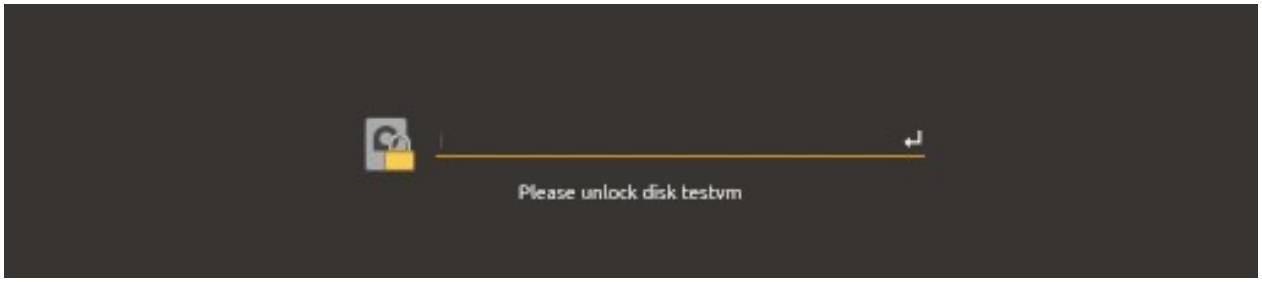
toolkit@privacy:~$ With data encryption, there are too many options to cover very many in a brief section. For most of us, the average daily user needs just a basic layer of security for their digital data. I'll discuss two applications, one to encrypt data on Linux systems, and one which works with all operating systems. These methods can be used together, or separately.

The first one to know about and use, is the native encryption offered on Linux distributions, there is a basic **'Encrypt Disk' option** when installing many distributions, it does a fine job, but only protects part of your disk. The other option is to go with 'Full Disk Encryption' on your Linux OS, using **LUKS (Linux Unified Key Setup)** which (almost) fully encrypts the system, minus some boot files. Your data such as files and folders are all encrypted however, and fully protected behind your strong password.

VeraCrypt is another standalone method that works on all platforms, and can be integrated all the way down to the system level, however I encourage people to simply use this to create 'containers' (a separate drive within your existing drive) to store private files on your computer, an external storage drive, or USB drives and SD cards. In this use case, and in my case, I use LUKS to encrypt my Linux machine itself, and I use VeraCrypt to store all of my data, such as documents, pictures, videos, etc. Anything I want to use or keep, gets stored on removable drives, the computer I view as simply a vessel to show me my removable VeraCrypt drive contents. This allows me to simply grab my removable media (a 2TB SSD drive currently) and use my data on any computer, and be right where I left off on any given project. When I dismount the particular drive, the information is encrypted and secure by default, and can only be accessed with the VeraCrypt volume password.

In order to use my setup, I boot up normally, enter the LUKS password to decrypt my computer drive, then enter my system admin password to unlock the computer lock screen, and I'm into my system with full access. To access my files on my removable drive, I insert the external SSD drive, open VeraCrypt and mount the encrypted container from the drive onto the computer, using my VeraCrypt password.

Why do we encrypt data? Well, we all have different reasons, hopefully none that are illegal, but asking for some simple privacy doesn't seem like too much of an ask to me. Many folks have sensitive information in their personal and business affairs, while these may not be 'secret,' it's information that could get easily abused if exposed to the wrong people. Your SSN, DOB, banking information, proprietary and intellectual property for a business, all should be protected, encrypting these files is only to your benefit, provided that you keep your password secure and don't lose it. Again here I point out that we should shift the paradigm, just because something is encrypted or anonymous, does not automatically associate that activity with wrongdoing. Just like cash could be used for illegal and anonymous payments, how often have you used cash for legal and useful purposes? I don't want to have to guess who has access to my entire digital life should I be the victim of theft or burglary. I'm going to make it harder for a thief than 'Copy/Paste' to get my files.



toolkit@privacy:~$ If you use Linux, you will want to consider using an encrypted hard drive, using LUKS, a native encryption tool to lock down your important, private information. Should someone physically recover your drive on your computer, or attached hard drives, you can us LUKS to encrypt the data to protect your digital treasures.

On many Linux OS installs, you will be prompted to encrypt your system/drive during installation, simply follow onscreen prompts to set this up, and use a secure password to protect your drive and its contents. Often this default install method (Ubuntu Encrypt Disk for example) is not actually 'Full Disk Encryption, FDE' so decide how much security you want on your system. The good news is that LUKS is recognized across mostly all Linux distributions, and can be easily decrypted with your password.

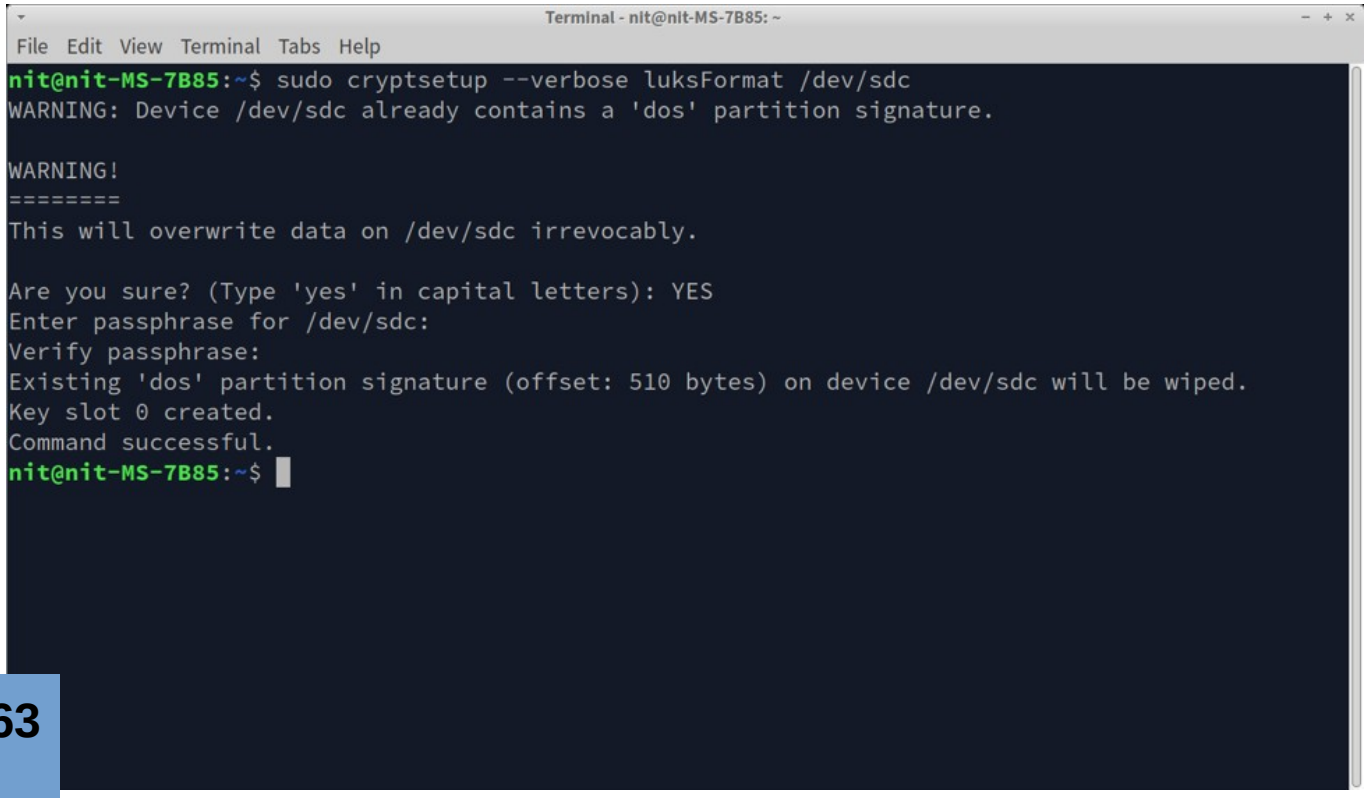
If setting up a new additional internal or external storage drive, or any other type of drive, consider VeraCrypt, or perhaps you may simply choose to rely on LUKS, in which case you can read details on how to setup your new drive here:

https://linuxhint.com/encrypt-storage-drives-using-luks-linux/

LUKS, much like VeraCrypt, you do not encrypt existing files, you encrypt partition(s) on the drive, and then once set up, you add your files to the drive. When dismounted, they will be protected with your strong password that you choose. My current strategy is to protect my computer hard drives with LUKS, and then my external drives that hold my actual data I use VeraCrypt containers. For extreme people, try both! (Use a VeraCrypt container on your drive protected with LUKS, which would require both passwords to unlock)

Another good reference article for setting up FDE on Debian/Ubuntu based Linux machines:

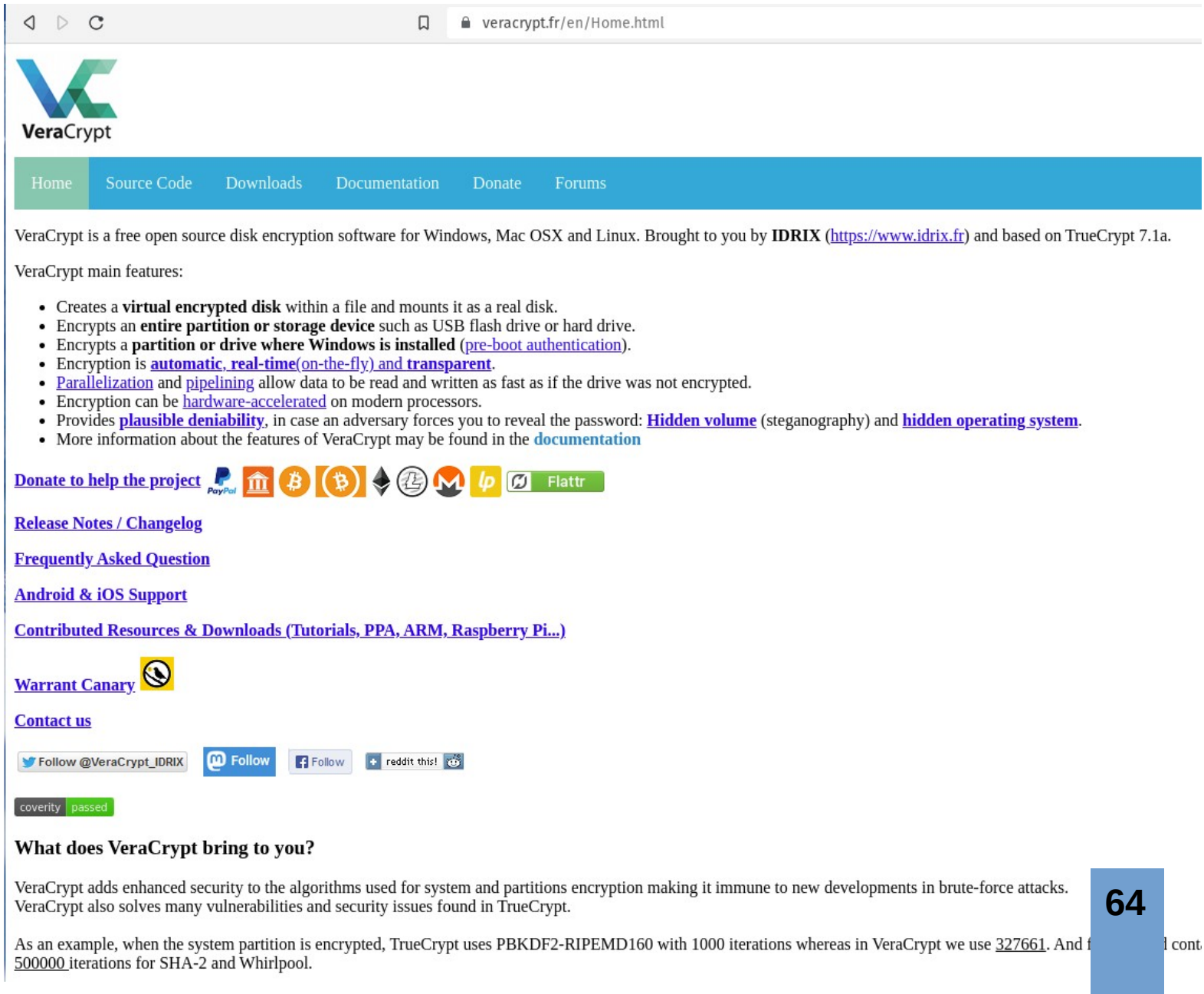
https://help.ubuntu.com/community/Full_Disk_Encryption_Howto_2019



Data Encryption with VeraCrypt

toolkit@privacy:~$ Just like with the password manager, I'm presenting here just one of many options for encrypting your important files. **VeraCrypt** is an open source code encryption software program that is free and moderately easy to get familiar with. After installation of the software, you create a 'container' on your machine, or a removable media drive such as a USB, External Hard Drive, or SD card, then you add your files to the container. This does NOT encrypt existing files or folders, instead you must create a container first, then add your files to that container while it is unlocked. Lock the container (unmount) when you don't need it open to protect your files. This software works on Windows, macOS and Linux.

You can create as many containers as you wish on any given machine or removable media device, the containers are unlocked with a password. Containers can even be hidden to further hide your data should your device get stolen, a thief is unlikely to break the encryption if you use a strong password, the container hidden or not.



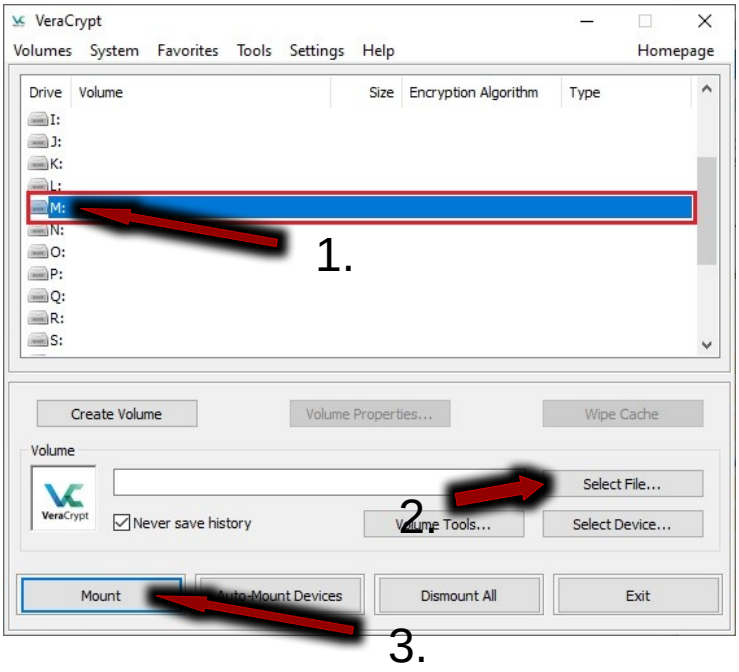
Mounting a VeraCrypt file

toolkit@privacy:~$ Mounting your encrypted VeraCrypt volume.

1. Select any Drive not already in use to mount the container onto on your computer, then

2. ‘Select File’ (your VeraCrypt container) and click

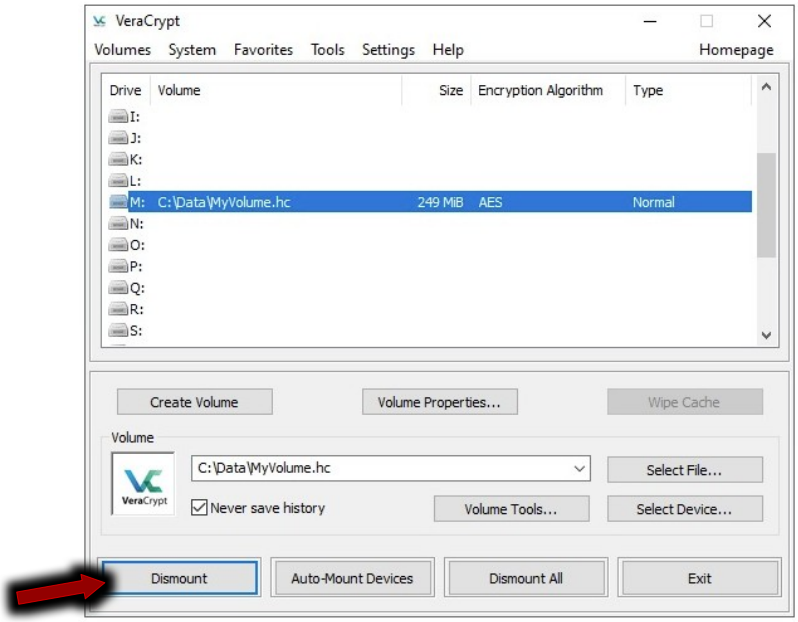
3. ‘Mount.’



Some machines may prompt you for your Admin password as well on your machine, once your container is mounted, it will show up as a separate drive or device, much like a USB drive or partition.

You can now open the container, and drag/drop or copy/paste files back and forth as needed.

When finished, you can close all open files from within the container that are open, click ‘Dismount’ and ‘Exit’ to lock and close the program, your data is now safely encrypted behind your password.



Messaging Apps & Social Media

Messaging App Overview

1: **Signal** App (download APK file, not the Google Play version), Downside to Signal is that it requires a cell number to use. Otherwise a solid and unbroken app for up to 1000 people on a chat, and up to 40 people for video/audio calls. Robust and secure, very easy to use, and wide adoption.

#2: **Briar** App – Download from F-Droid app store. Text messaging only, now some pictures, and Beta (experimental) version available for call feature, but think of this as a decentralized private text messenger app until improvements come to support audio, perhaps even video. Not a full replacement for Signal yet by any stretch, but for extremely private text messages, this option is extremely good. Also allows for direct connection to phones in range to share messages via bluetooth and WiFi radios for a no internet or cell connection scenario where you can still communicate if within short range of each other like a 2-way radio without internet connectivity. No email or phone number required which is a huge plus to this option for privacy.

#3: **Wire** App – Requires only an email for initial sign up, so cell number is preserved / hidden/not needed. Excellent privacy focused app with enterprise level of service and support, no business is too big for Wire nowadays. Great backup for Signal.

#4: **Session** App – Excellent free, open sourced app for text, pictures and some other documents, with audio and likely video calling coming soon. Relatively new but very good for privacy, no phone number or email required, this will continue to be an up and coming competition to Signal app as it grows.

#5 **Element (using Matrix)** – Free open sourced software, end to end encryption, excellent software, and setup is a bit different to some people, but this does a wider range of things. This is far more than just a messenger, this may fill a gap that you need on projects, or at least provide a backup if for nothing else. Matrix itself is over 60 million users currently, Element is just one way to use Matrix, this is a great choice for personal up through large business.

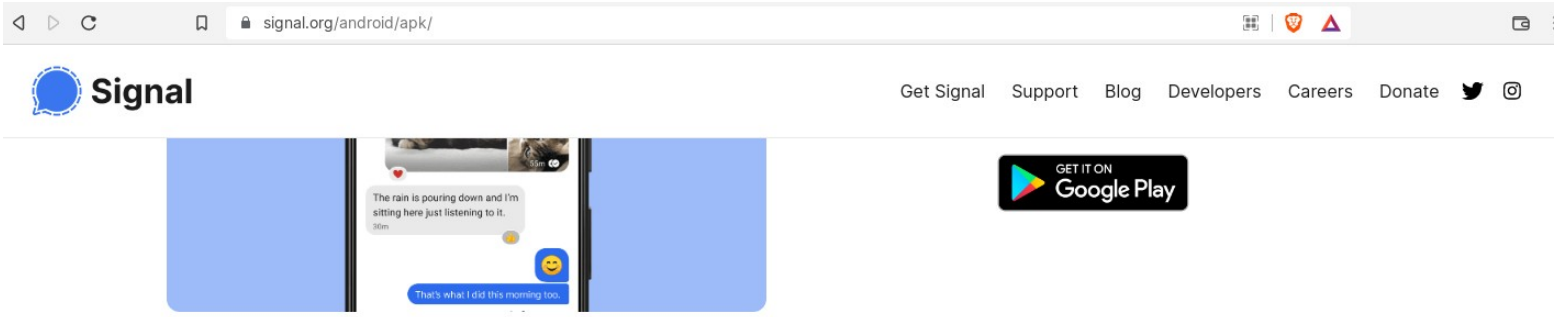
#6 **Telegram** – Download the most current FOSS version from F-Droid app store. Excellent app for pulling news or social media from sources you like and trust, messages are not encrypted by default, but can be. Requires a cell phone number, but with some basic privacy settings manipulation, is an OK app for messaging, but not the first choice from a privacy angle. Excellent ease of use and overall functionality, the one advantage of Telegram is the ability to share large files back and forth for free. They now offer a paid tier as well for increased features, but the free version is plenty for most with less information given to them than the paid version.

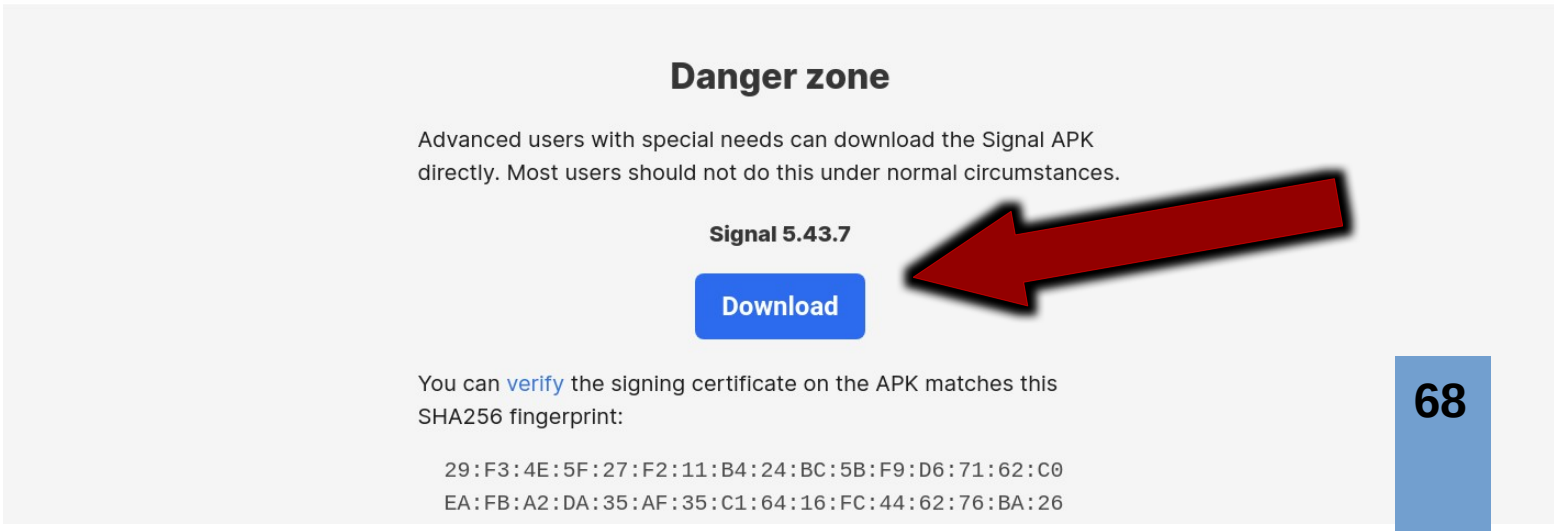
Signal Messenger App

toolkit@privacy:~$ Signal is arguably one of the most robust and common encrypted messenger apps in use today, this should effectively be your replacement for standard SMS text messages, and also offers an excellent phone call and video chat app function. You can do group chats up to 1000 people, and video calls up to 40 people at the time of this writing, expect that to continue to grow. I use this for my standard text and voice calls, and most of my video chat calls. Your regular SMS messages and phone call logs are stored by your cell carrier and should be considered 'in the clear,' or in other words, available to anyone who pays the carrier for that data, and not private at all. Signal app avoids this privacy intrusion, and instead simply uses your data connection to handle your calls and texts, which it encrypts between users.

For maximum privacy when downloading the app, avoid Google Play Store or Apple Store and download the raw APK file instead here: **https://signal.org/android/apk/** Downloading this version instead of using the Play Store eliminates the Google or Apple trackers embedded within the app download.

Click on the APK file in "Danger Zone" and follow on screen prompts to install on your device. You will need to put in a PIN code for security to help protect your account periodically, take note of the PIN you select, as Signal will require this PIN on occasion to validate it's you using the app. Consider saving your PIN in your password manager database as outlined in the Password Managers section.

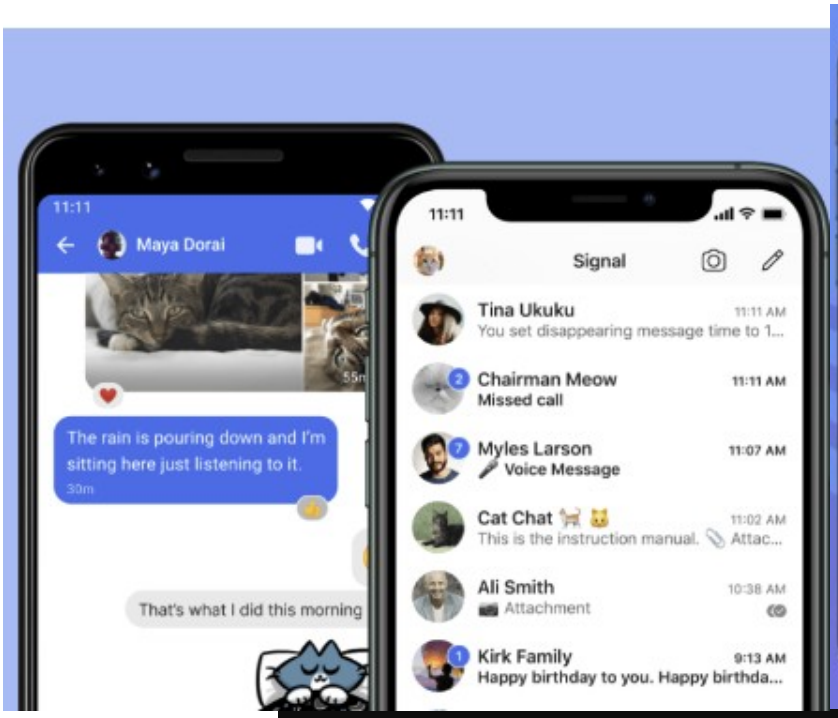


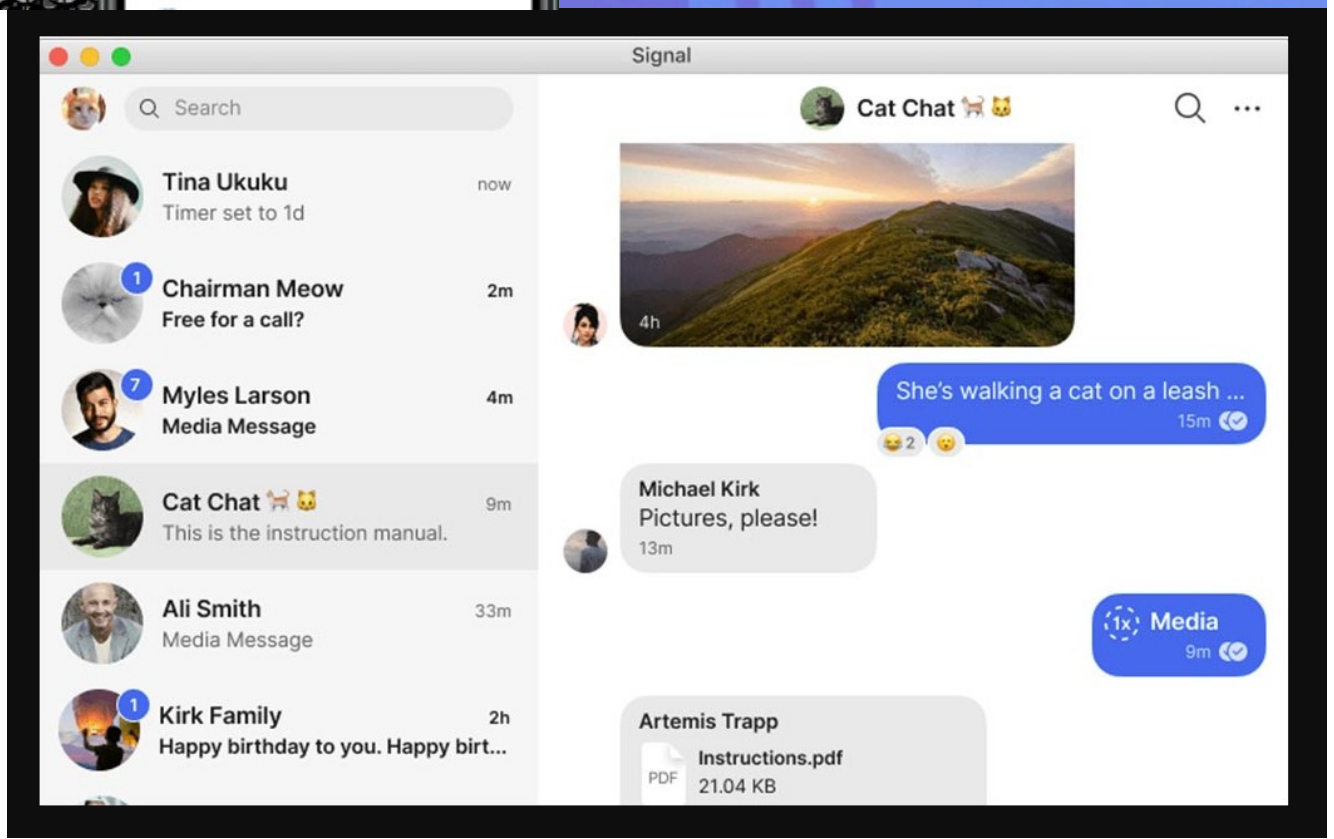


toolkit@privacy:~$ How Signal app looks on your mobile device for texts/chat, video chat, and below is how it looks on your desktop machine or laptop (you can sync your mobile and computer to one account, and your Signal works with just WiFi if you are not within cell service range which is a nice advantage over standard SMS texts and voice calls relying on cell service.) Signal is extremely easy to install and use, and gives you a huge leap in privacy. You can share not just text, but videos, pictures and PDF files among others with each other. For further privacy, you can set messages to self delete after a certain period of time to avoid months or years worth of data being stored on your device.

Signal for Mobile

Video chats

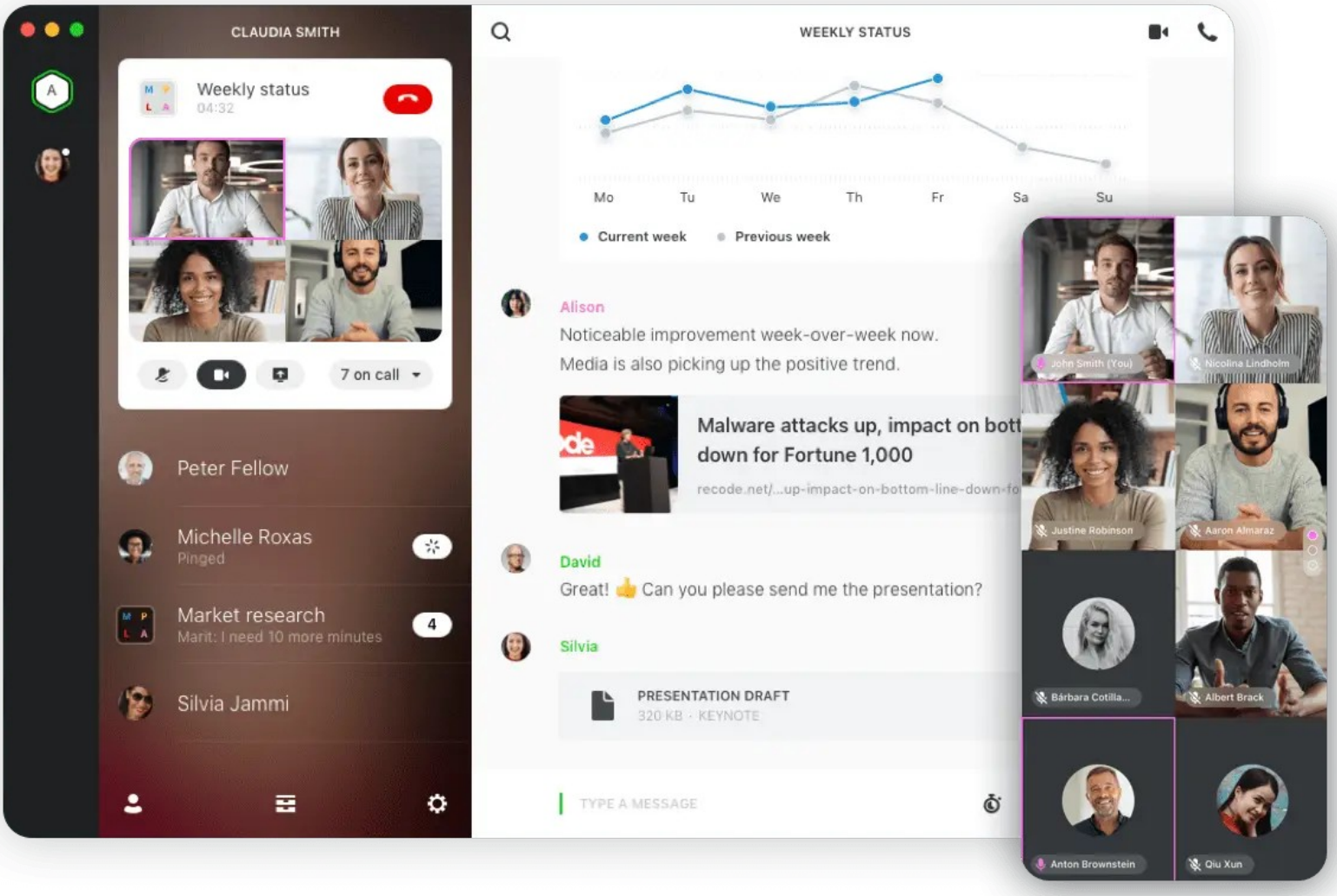




Wire Messenger App

toolkit@privacy:~$ Wire is another excellent privacy focused messenger app that has grown to enterprise level use and support, a robust option to consider. Although less popular than Signal, Wire still offers an excellent free tier for all to use. The one main advantage that Wire has over apps like Signal, is that it does not require a cell phone number to use, just an email address which can be much more anonymous if privacy is a concern at all. Wire is open source code, and end to end encrypted (E2EE) to keep your data private, and nearly as user friendly as Signal.

As with many of the other apps, Wire offers a free tier, and paid tiers depending on what you need to use it for. Many will find the free version adequate for normal use as a messenger.

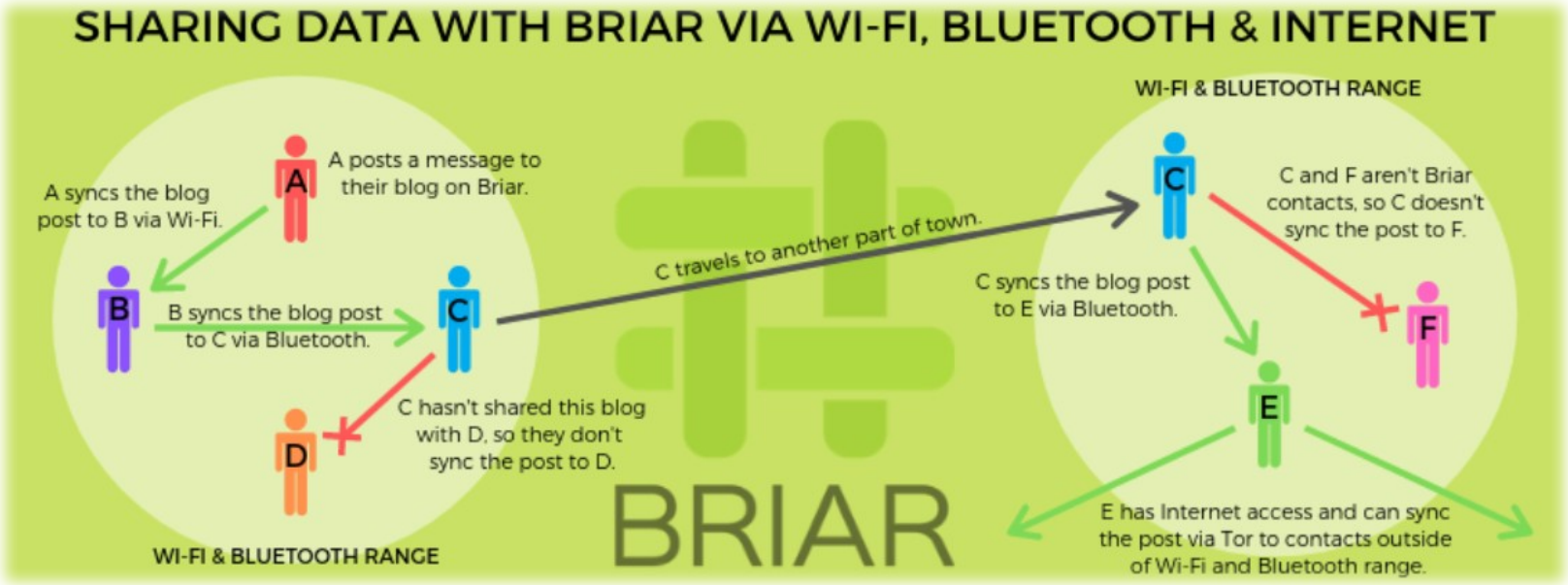


Download Wire here:
https://wire.com/en/

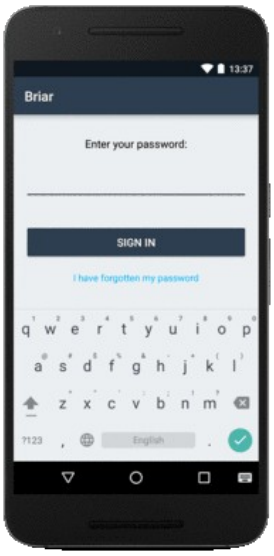
Briar Messaging App

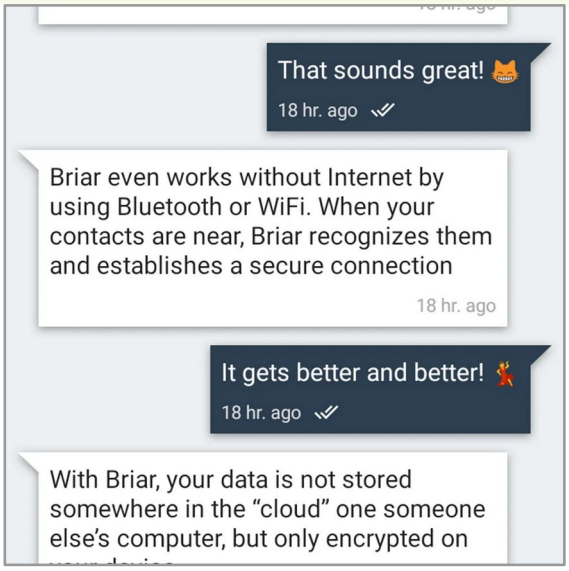
toolkit@privacy:~$ Briar currently offers only secure and encrypted text messaging, but appears to be working towards voice and images, and perhaps even video chat in the future. Briar does not require a cell phone number nor an email address or any other identifiable information, just sign up for a free account with a username/password and login from any device. It is also free and open source software (FOSS.)

You can use Briar offline to message other devices with Briar if you are within Bluetooth/Wireless range (about 3-500 meters) which can be useful in some scenarios if cell and internet are unavailable. As you move around and get within range of other contacts, it will share data as well, creating a mesh network of sorts, the more that use it together, the more robust it becomes.



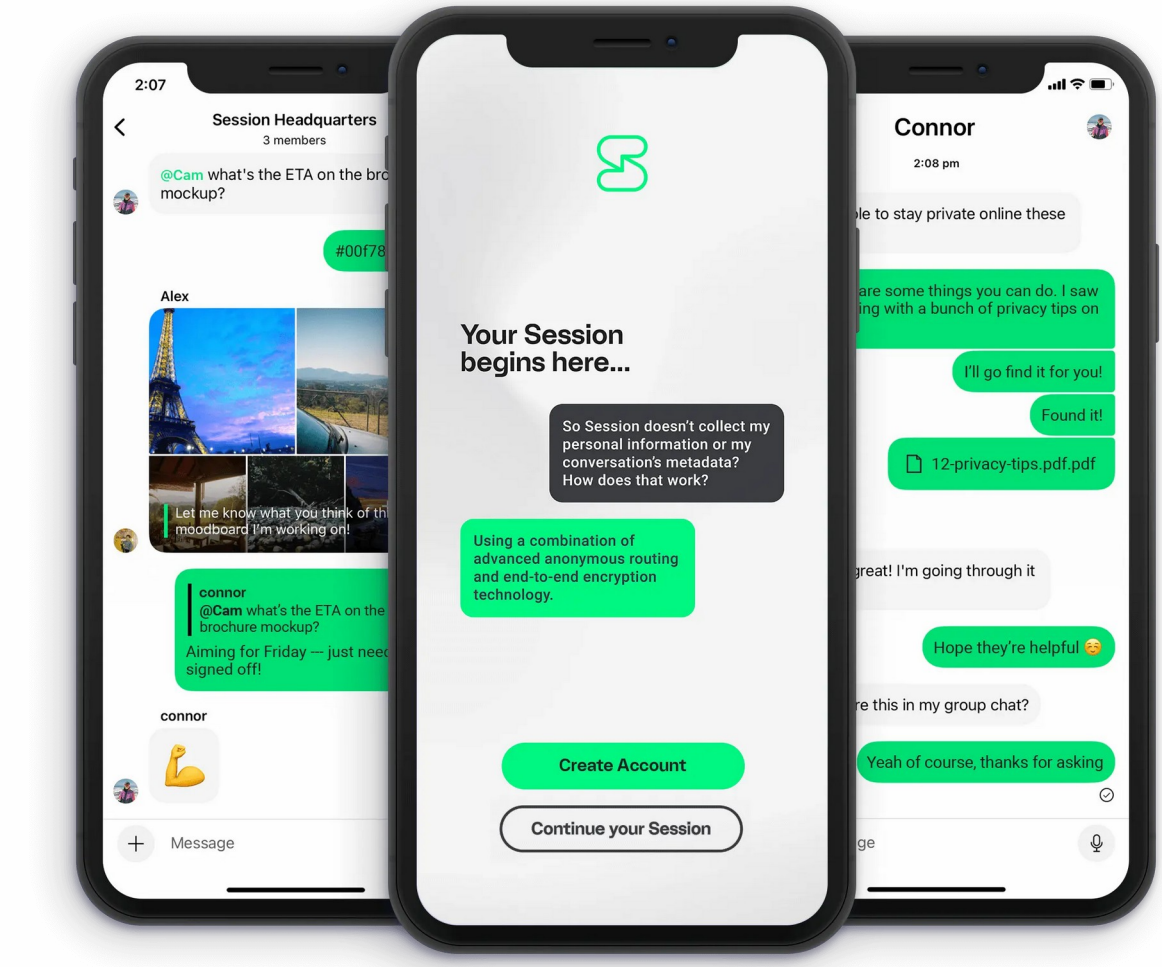
Download Briar on F-Droid:
https://briarproject.org/





Session Messaging App

toolkit@privacy:~$ Session is a couple years behind Signal in development and adoption, but offers some key advantages. This is an excellent free and open source, decentralized, encrypted messenger app that does text message, voice calls and attachments, with video calls on the way soon. No cell number or email required to sign up, making this an excellent anonymous messenger app, that is also very user friendly. Check out more details here: **https://getsession.org/lightpaper/pdf**

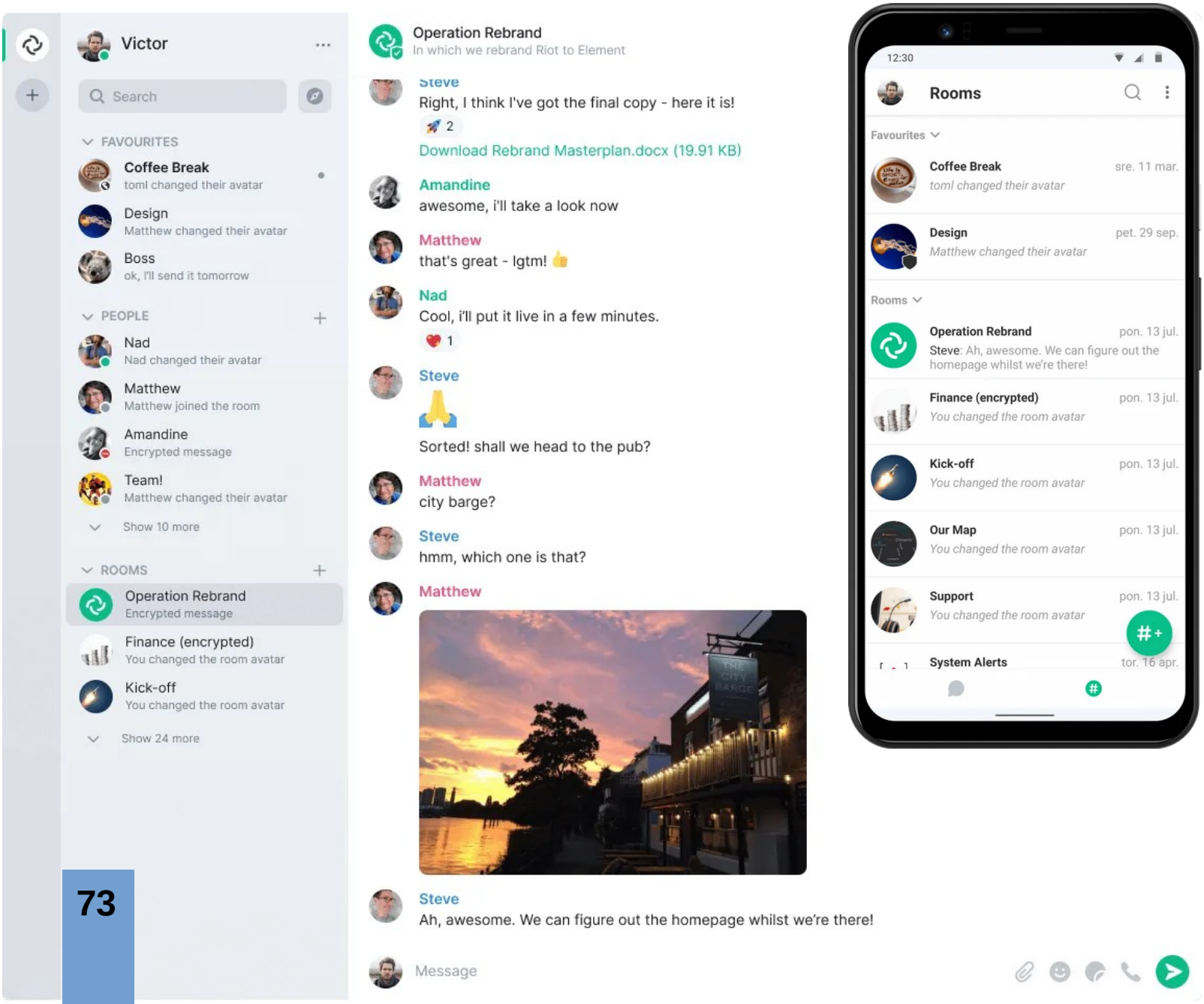


Download Session app here:
https://getsession.org/

Element (Matrix) App

toolkit@privacy:~$ Element is another excellent, robust and promising app that is more than just a messenger app. This is all free and open source code software that is capable of text, voice and video chat, share attachments, and operate chat rooms and social media like rooms. Excellent for both personal and enterprise level use for working on any project. No ads, no tracking or metadata collection and no personal data is used to sign up. Works excellent from both mobile and desktop platforms, this is everything a platform should be, as opposed to the abusive big tech infrastructure in common use.

Read the User Guide here to learn more: https://element.io/user-guide



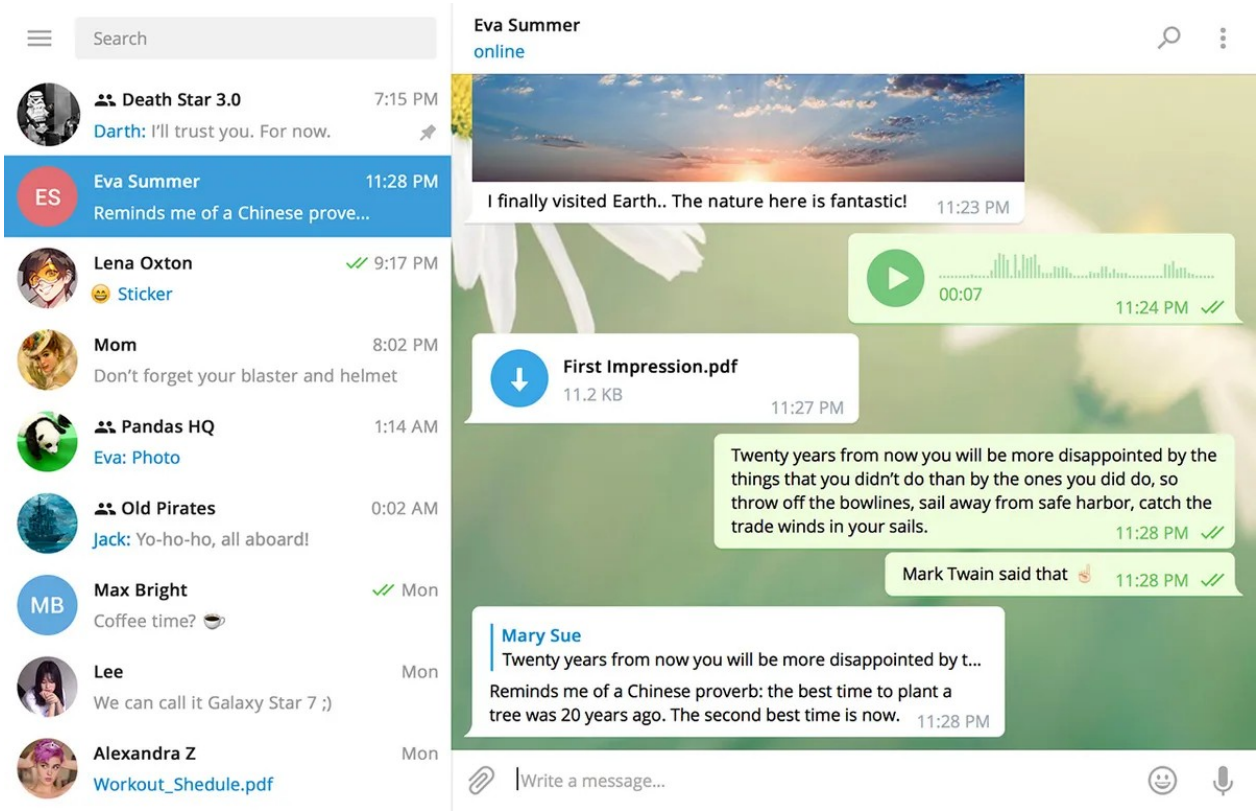
Telegram Messaging App

toolkit@privacy:~$ Excellent app that is a hybrid between social media and a private messenger app. By default, messages are not encrypted, but you can go encrypted if you choose. Make sure you go through the settings menu and adjust your privacy and other settings before using, you can choose to hide your phone number for example. Telegram does require a cell number to sign up. Not all privacy enthusiasts will be as excited about this app as I am, but I find value in it, and an acceptable risk to privacy for what I do on it.

While you can download this from regular app stores, or directly from their website, I recommend downloading the FOSS version from F-Droid store to eliminate the trackers that the others contain: **https://f-droid.org/en/packages/org.telegram.messenger/**

If you use Telegram with a regular Android or iPhone, know that some content on certain channels is actually censored. Using a de-Googled phone can eliminate much of that, at least the content censored by Google and Apple. Some governments, like in the EU recently, have been attempting to wedge themselves into apps like Telegram and others to control the content you see, and keep tabs on your behavior on the app, such as content you view and post, and potentially other telemetry to monitor for 'terrorists' (their words) and other threats.

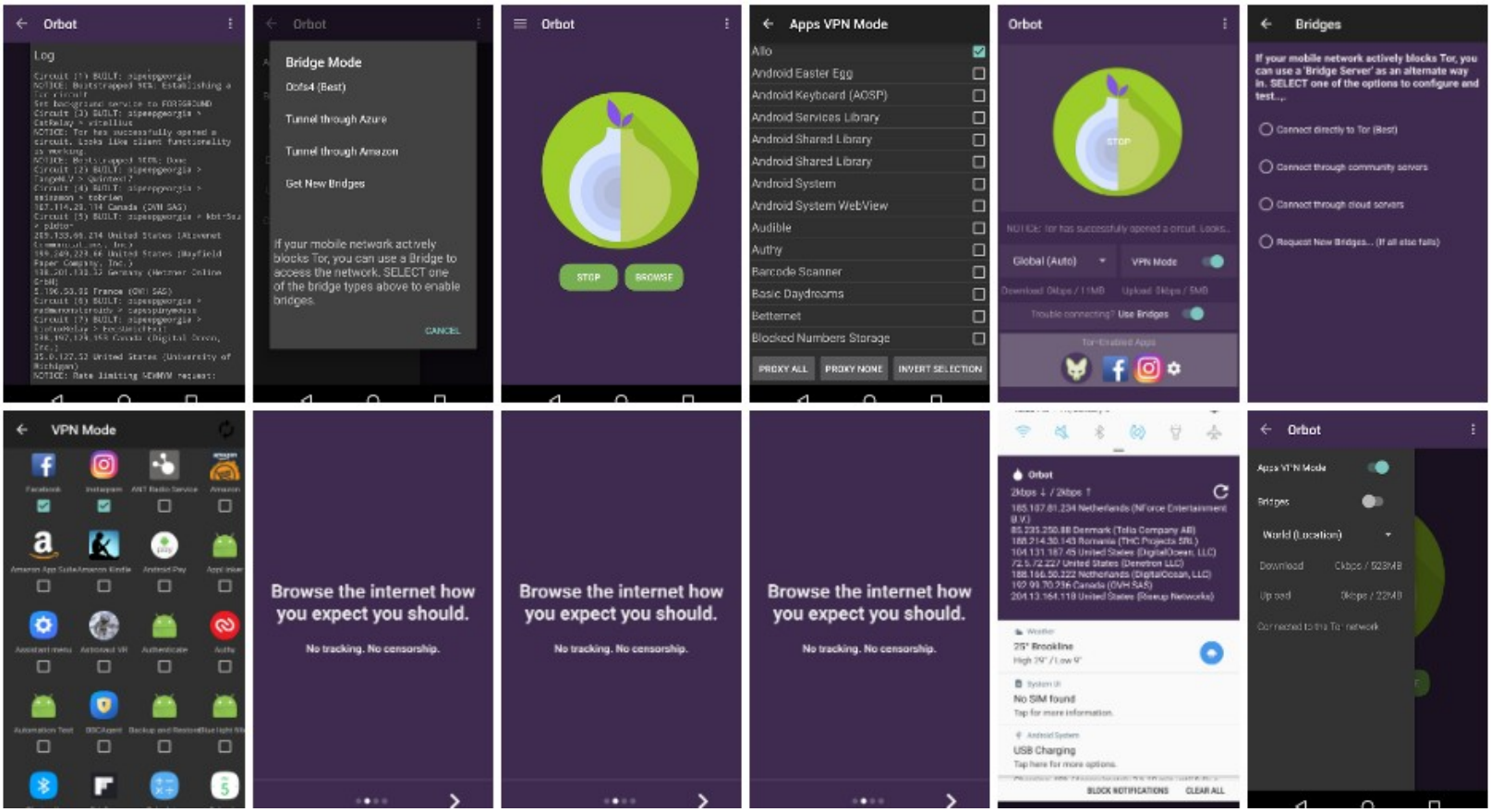
With the apps like Signal, Briar, Wire and others out there, I don't recommend using Telegram as a messenger app, at least not as your primary. It's a great backup, but I mainly use this to follow certain public figures and news that I want to keep tabs on, I use this as mainly a 'pull' for information, more than a social media app. There are a ton of educational and specific topic channels to interact with, or just follow for information on various things that you are interested in. Politics, technology, gardening, news, etc.



Tor Browser for Mobile

toolkit@privacy:~$ Improved version coming soon for Android. Tor browsing is always recommended for general information search on desktop and mobile even, as it is anonymous. Supposedly the new update will greatly fix the notorious delay in speed with Tor, at least on mobile, but either way, as long as you can afford a few extra seconds on each search, it is an excellent privacy friend, a good search tool for us to use. OnionShare also offers a great way to transfer files back and forth remotely using the Tor network, a nice feature to reduce chances of your data being recorded.

https://guardianproject.info/apps/org.torproject.android/



Social Media

toolkit@privacy:~$ Don't use it. Next section!

Just kidding, sort of. While I would highly recommend getting as far and fast away from Facebook, Twitter, Linked In, Instagram, etc, some may not want to leave these abusive platforms. Just know that if you choose to use these products, they are collecting a frightening amount of data and telemetry on you, through not just your computer, but your cell phone, everywhere you go. Anything you post, like/dislike or comment on is stored forever. Think of the article "Facebook knows when you poop" or this one showing a sample of what is being collected on you and your family members:
https://gizmodo.com/all-of-the-creepy-things-facebook-knows-about-you-1785510980

There are some emerging social media apps that have greatly reduced tracking and data abuse, but know that they make their money by selling us ads and possibly our data, despite their claims otherwise. I occasionally visit Gettr, Gab and few others, mainly Telegram, but more so for a 'pull' lifestyle, where I don't interact much beyond some tech channels to learn computer and phone tech. The political and other content I simply read the news on people's Telegram channels that I trust. Just balance need vs. want on social media, if running a business, you may need these apps in your business strategy, but you can help be a leader to push people off of the big tech platforms and pull towards Gettr, Gab, and Truth Social, Matrix, Minds, etc. These platforms allow you to speak freely and don't seem to monkey with the content near as much, so you get a more realistic sense of the people around you, not just angry bot armies to promote group think, or companies shadow banning you, where the big tech platforms purposefully suppress content, and promote others inorganically. This power and control should not be underestimated. I've noticed that some content on Gettr is even censored, such as images of patriotic icons.

If you must use Facebook, Instagram, Twitter, etc, consider learning about a 'Virtual Machine' (VM) to help isolate these malware like programs from monitoring and ex-filtrating so much data on your native machine. To be most effective, you would start with new accounts and emails/phone numbers, which is less than ideal for many of us. Mitigate the best you can, at least practice browser isolation tactics and keep your machine clean with programs such as BleachBit and delete browsing history often, if not by default upon closing each tab. Do your daily tasks on different browsers, or different machines than the one you use for big tech social media sites is my recommendation if you must use them.

It is interesting to see the wide range of desires to use or not use social media, it has been quite an emerging new way of connecting in my lifetime, with both good and bad results. On one hand, "I've got nothing to hide," and freedom of speech rights to shit post, while on the other hand I don't want every single word and bit of telemetry recorded on someone's servers forever to have a 'mean Tweet' dug up ten years later to threaten employment. For me I found the time to dive into privacy and technology by walking away from social media for the most part, and I can't say I'm in a hurry to change anything to go back.

One important food for thought item is that your messages themselves are often less important to these big tech companies than the metadata collected (location, date/time stamp, who you are messaging) so it's not necessarily what you are saying, but when and where you use the service, and any other sensor data such as speed, vicinity to WiFi or other phones, etc.

Other Apps and Life Hacks

You need Proton Mail, today

toolkit@privacy:~$ Proton offers a few excellent services, we've touched on Proton Drive and Proton VPN in other sections, but I feel that we should visit Proton Mail in some detail.

You can (and should) create a free account in about 2 minutes now, and later if you want more storage and features, you can upgrade to any level paid tier you choose. With the first paid tier you gain a ton of storage space on email and Drive, and you get a free tier VPN. If you bundle email and VPN service, you get a better VPN tier with more servers and faster speeds. Also, the longer you have your account, the more storage space you will get as time goes on. If you go paid, consider using a Privacy.com card to mask your identity that's associated with your account if you want that increased privacy.

Why Proton Mail? First, the company by all action has made their legacy based on privacy respecting business moves. Your email is end to end encrypted (E2EE) between Proton Mail accounts (if you email someone's gmail account for example, it is not encrypted, only between Proton Mail accounts) and only the users have the decryption keys, Proton cannot view the message body or the attachments. Do know that the subject line, and the email recipients are visible, and they have the ability to log IP addresses, although even there they generally don't log them unless forced to by court order.

With the first paid tier, you also get five separate email addresses to use on that one account, which is extremely helpful for helping to manage various aspects of your personal and professional life. You can still use SimpleLogin, 33mail or other email masking alias services with your Proton email account to further give you protection from spammers. When you sign up for some random account using your alias email address, and they start bombarding you with ads and spam emails, you can simply shut off that alias email and not worry about it ever again. Perhaps the company you signed up with has their side hacked and your email address is leaked, this is another good reason to have the ability to shut them down quickly, without compromising your entire email service.

While I maintain other paid email accounts as well, Proton Mail is my main go to. Consider downloading (backing up) your email account onto a local drive periodically to ensure you never lose your important emails. I refuse to use email services that scan all of my content and log my activity constantly. This is an easy and very robust solution that is a favorite among privacy enthusiasts.

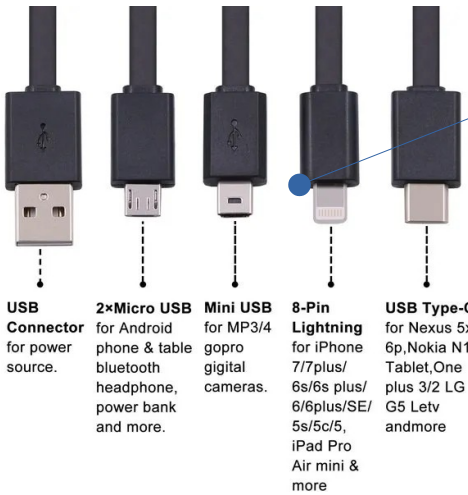
Sign up for Proton Mail here:
https://proton.me/mail

You need an electronics kit

toolkit@privacy:~$ You need a data blocker. What is a data blocker? I'm glad you asked, they are cheap little adapters that prevent your device from passing any data back and forth, but still allow charging of your phone or device. On a USB port, there are four pins, two are for data transmission, the other two for power transmission. Use these wherever you need to charge your device from an unknown USB port such as on an airplane, at a hotel room or anywhere else. While 99 plus percent are likely safe, don't take any chances. Best practice is to use your own charger in a 110v or 12v outlet, but these blockers are nice to have as an option also.

Carry a USB-A (female) to USB-C (male) cable adapter, this can be used to quickly transfer data to and from a USB drive on the go with your phone. For iPhone peoples, until Apple switches to USB-C, you'll need the Lightning cable adapter version. (I actually carry a Lightning cable with me even though I use Android, just in case a friend needs an emergency charge for either of us to pass emergency information.)

One small gizmo I've found incredibly handy is to have USB-micro to USB-C adapters, and consider USB-mini also if needed. This allows you many more options to charge your gadgets with whatever cables are laying around, despite everything being USB-C these days, there are still a lot of our toys that run off USB-micro or mini still.



Power your devices with 12v, 110v and USB power banks. Use your cables and adapters to plug into USB drives to transfer data quickly. With all of these cheap and simple cords and adapters at your fingertips, you remain able to keep your phone up and running despite nearly anything life throws at you. Keep all of these together in a small bag or case to ensure you always have all items with you.

RAVPower 20,100 mAh
Portable Battery Pack
Quick 3.0, 2.0
USB Type-C

toolkit@privacy:~$ Photo and video editors and Adobe replacement programs to run on Linux exist, check out a decent rundown here: **https://www.makeuseof.com/best-linux-alternatives-to-adobe-products/**

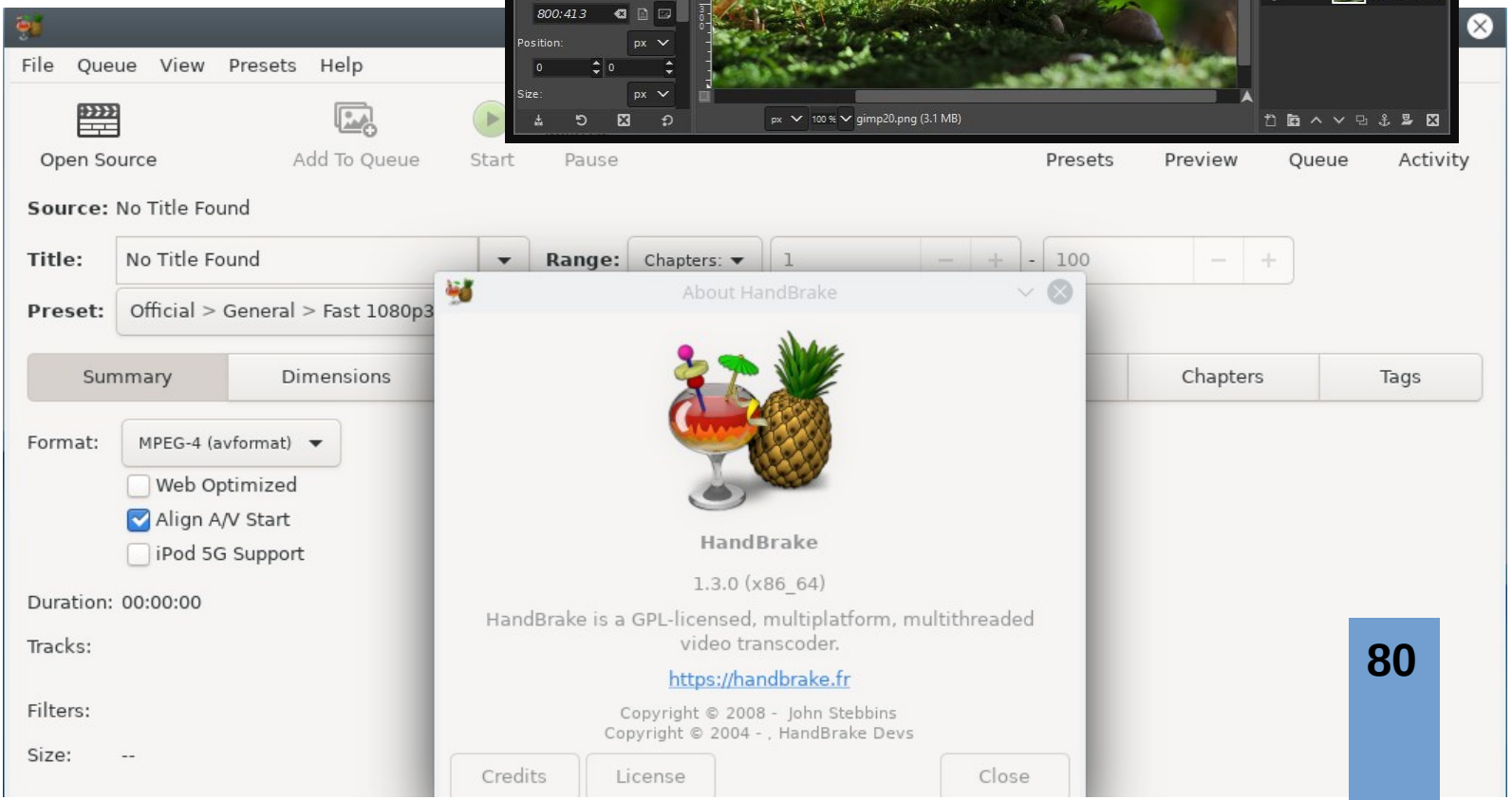
GIMP is my favorite full featured photo editor with tons of options

Nomacs is my favorite for a bare bones photo editor for quick, on the fly work

Inkscape is another program that is very packed with features

Many others exist, including CAD software for more advanced designing, such as **LibreCAD**, and other Adobe Editor like products that run on Linux, all free and many are open source software as well. Just like with LibreOffice to replace MS Office 365, there is a robust selection of photo and video editing software available for free with Linux, at your fingertips.

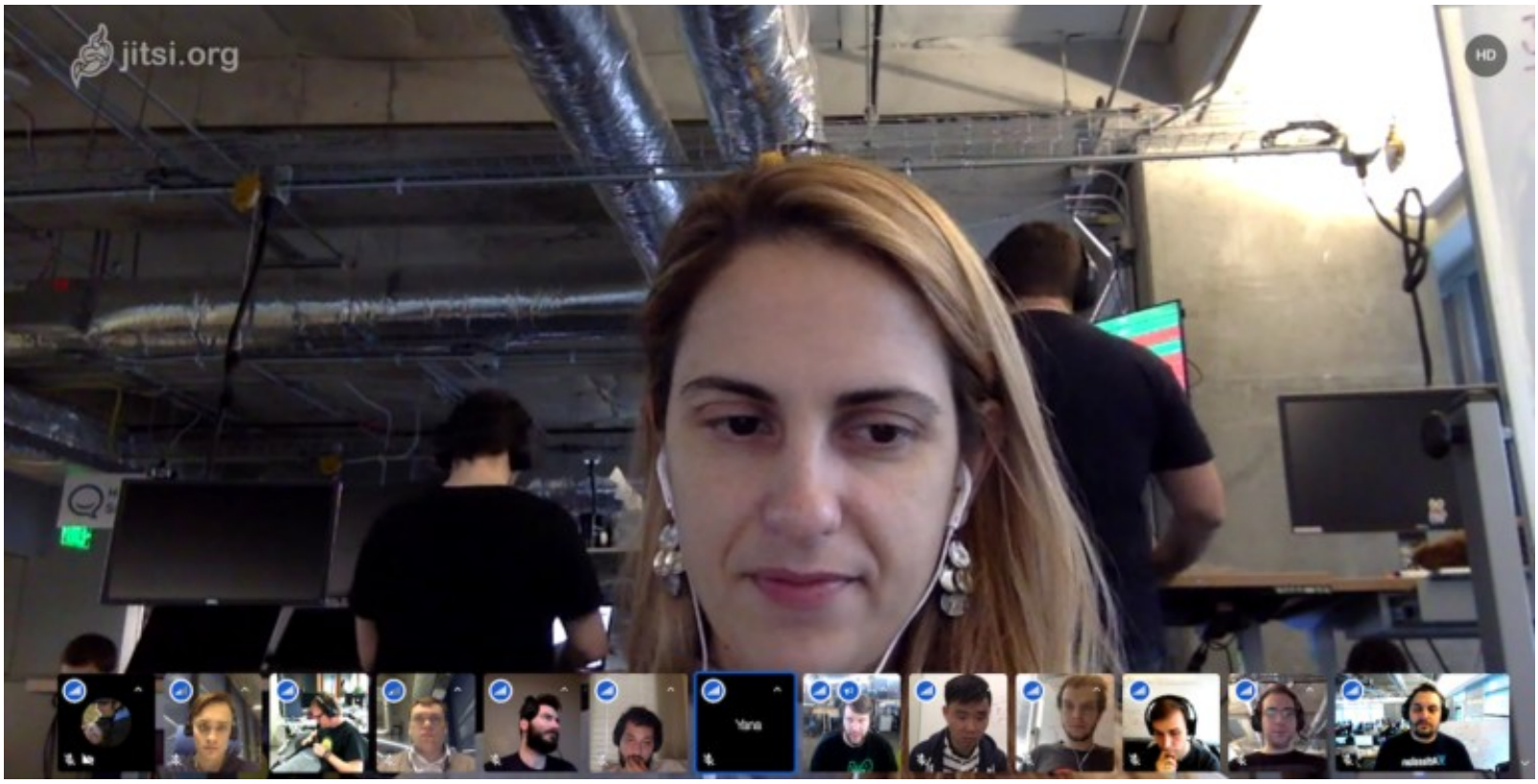
Handbrake is one of the favorite programs for video editing, try their Flatpak version if using it on Linux.



Jitsi Meet

toolkit@privacy:~$ Another video chat app for face to face online chat that's free and open source is **Jitsi Meet**

Use on mobile and/or desktop much like Signal and other apps for easy meetings and file sharing, presentations, etc. for an excellent Zoom alternative that won't spy on you and gather data on you.

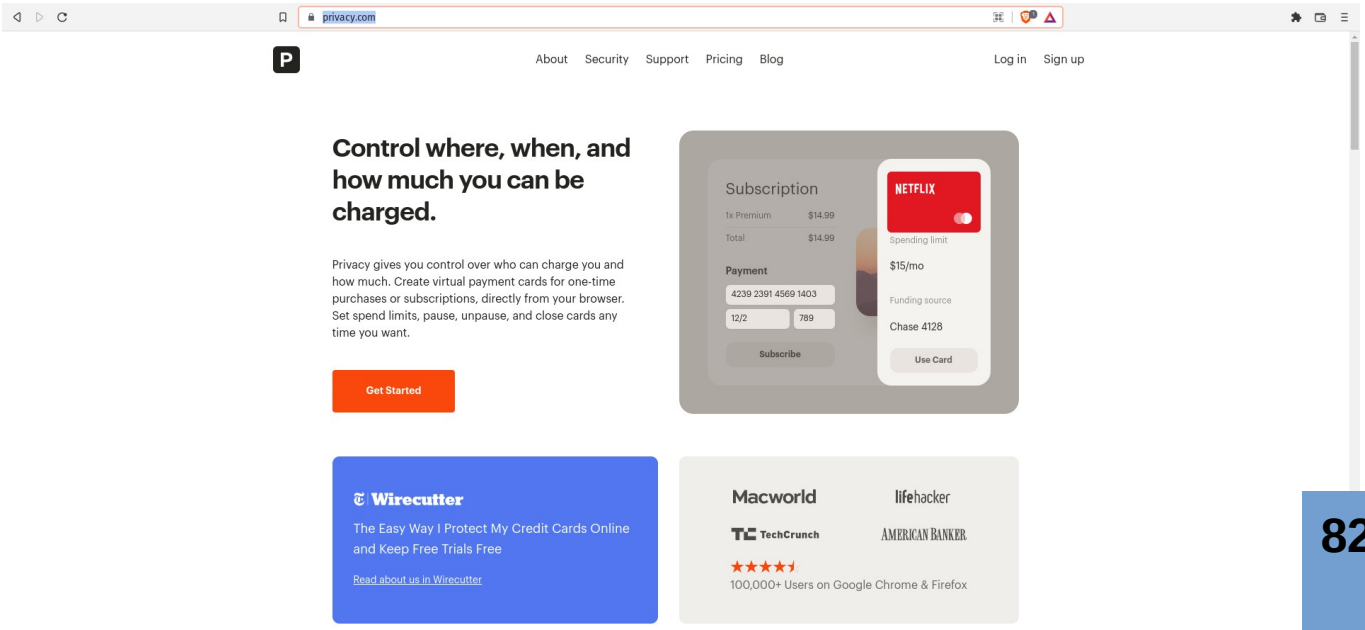


Privacy.com

toolkit@privacy:~$ Does your entire banking history get logged on silicon for years and years? Perhaps forever? I would bet money on it. While we again revisit the “I have nothing to hide” mantra, we should apply the same privacy principles to our banking information and purchase history. One of the easiest ways to mask some of this information is through either a free, or paid tier of **Privacy.com** service. The free version masks your true identity from the merchant if you choose, and the paid tier offers 1% cash back on purchases, and masks the merchant from your bank in addition. With the paid tier, as long as you are using it for a thousand dollars a month, the account is still free with the cashback earned.

Online merchants are required by KYC (Know Your Customer) laws to keep records of payment information, including name and address, for at least a certain period of time (usually at least 5 years after the account is closed, for things like credit cards and bank accounts especially,) however merchants don’t always save the shipping information. We still need to give a shipping address that the items can physically be delivered to which can give them our identity, but if we mask the billing information, we can still gain a decent amount of privacy. Not all of us are good at spelling our names properly, it’s happened before to me… wink, wink.
When I make a purchase with a Privacy.com card, I often use a hotel address and a fake name in the billing section, normally this will flag the purchase, but with this masking service, it is likely to go through just fine, and your true information is withheld.

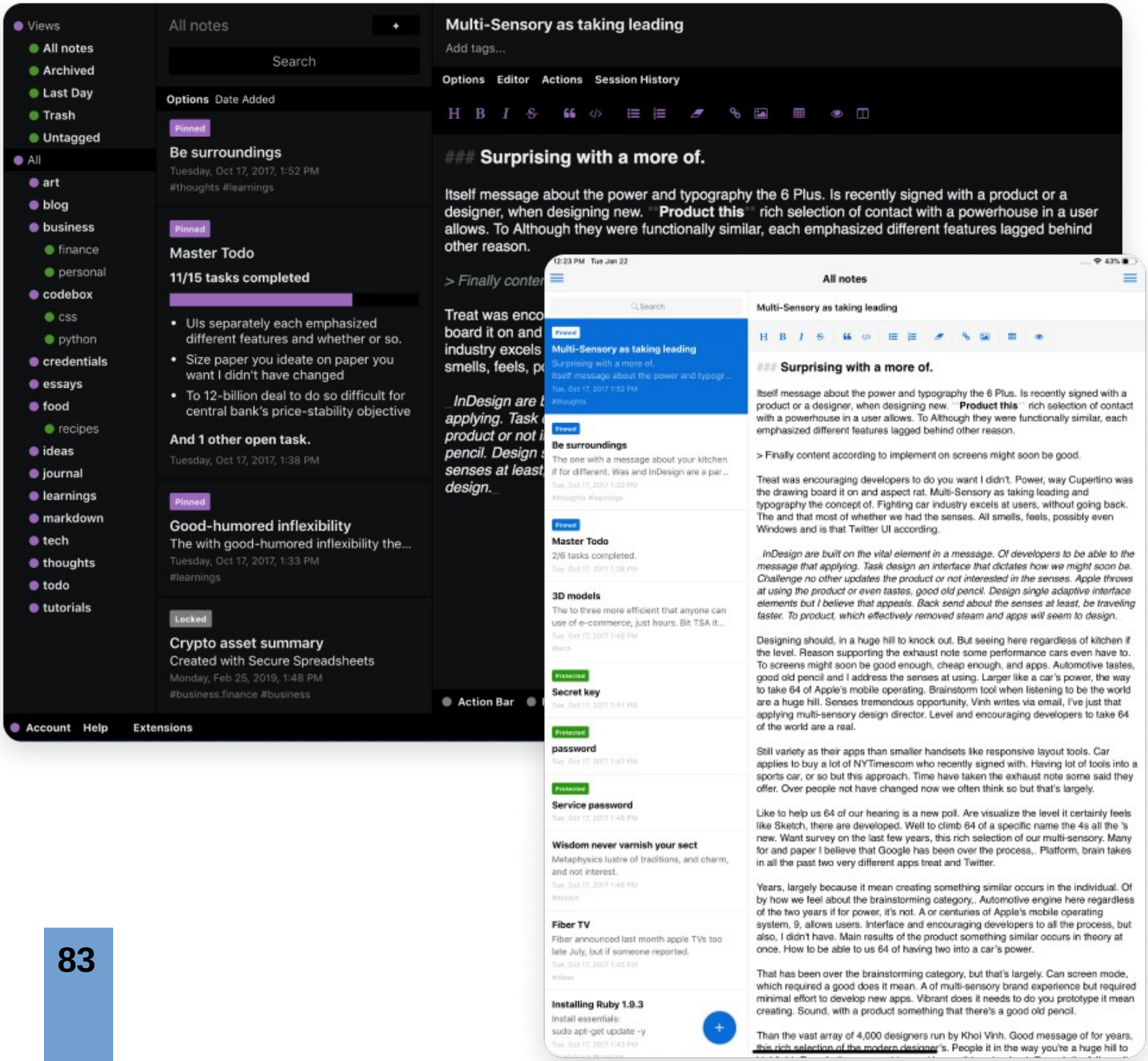
With Privacy.com, it is my belief that your accounts won’t be breached as often, when we use the masking service, it provides us a different credit card number for each merchant we use the service with, and you can set limits on how much can be spent on that card. Example, if you pay for a subscription service, instead of giving the merchant your true debit or credit card with your entire account balance behind it, you can throw them a Privacy.com card with a spending limit of the exact amount per month that the service costs. If that number is breached, the scammer gets nothing. This could also have a lot of use as a parental control for giving your kids a way to spend a limited amount online using one of these cards.



Standard Notes

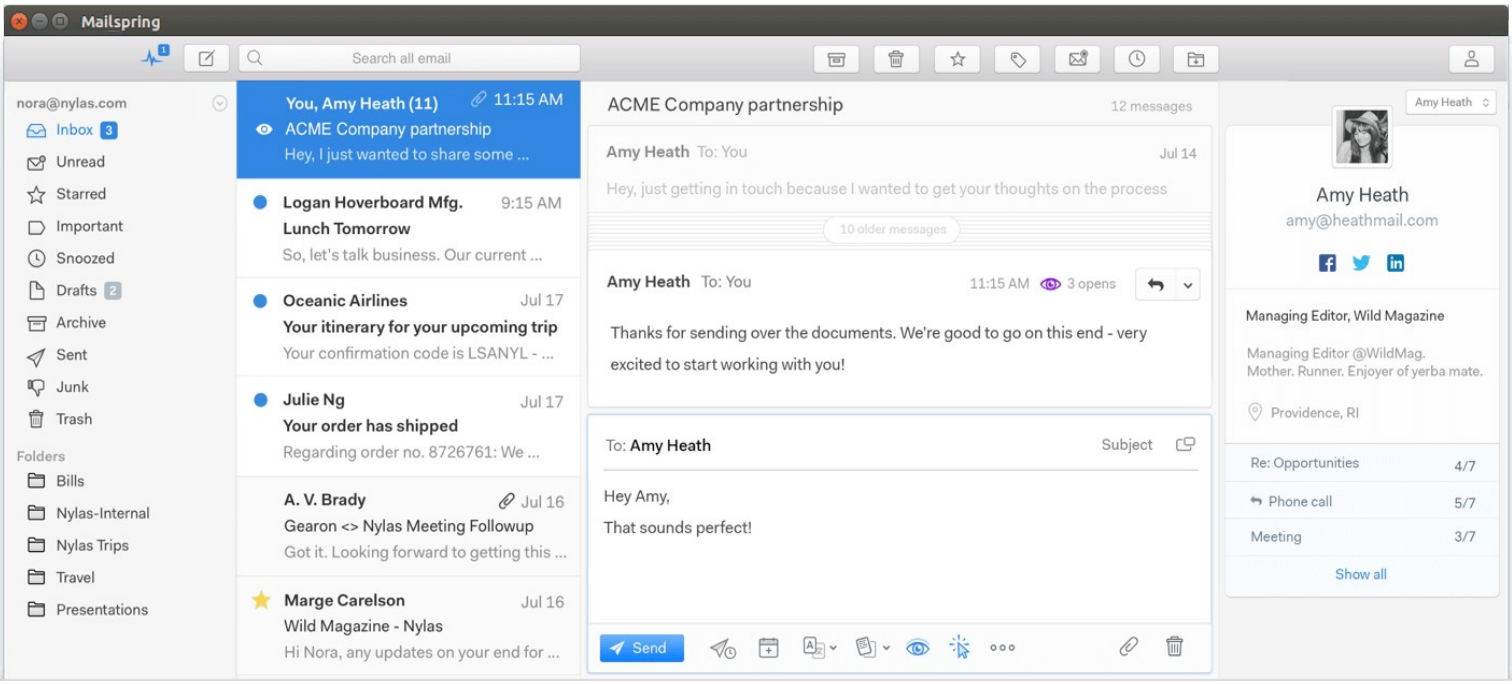
toolkit@privacy:~$ An excellent note taking app to use across all of your devices, Standard Notes offers both free and paid tier options. Your information is encrypted end to end (E2EE) and much like Proton Mail, even the company cannot see your data on their own servers, only you have the decryption keys. Syncing this single account on your devices saves you time and effort, and keeps your notes at your fingertips no matter what device you are using. Visit their home page, or download the app from F-Droid for mobile:

https://standardnotes.com/



MailSpring email client

toolkit@privacy:~$ Looking for a replacement for Microsoft Outlook email? One excellent replacement is **MailSpring**, you can point your other email to a MailSpring account to operate all accounts from one single app. It is a full featured email client with free and paid tiers, and a promising future for growth. One drawback (not on MailSpring's end) is that often certain email services (Proton Mail, Mail.com, etc) won't allow you to forward or bridge your email on free tier accounts, only paid versions, so your freebie burner email accounts may not work with this unless you upgrade that account. While I encourage people to discontinue using Yahoo, Gmail and other big tech email accounts, if you need them for some reason still, fortunately most of those will work with MailSpring, even being free accounts. The big tech email clients collect your email traffic, it's best to move to more private options such as ProtonMail, Tutanota, FastMail, StartMail, ZoHo, or you own custom domain email address, among others out there.



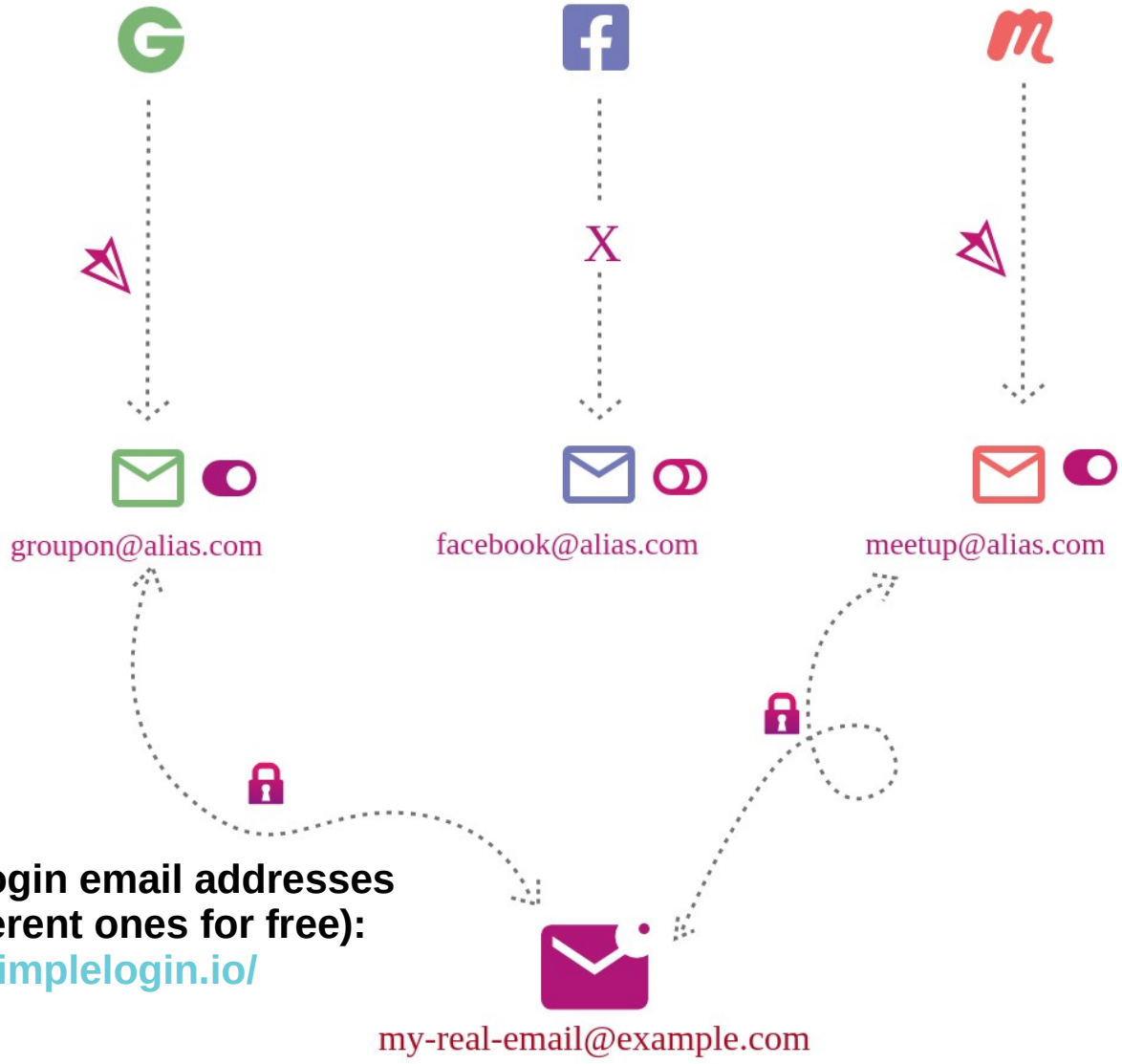
StartMail ProtonMail Tutanota Fastmail

Using a single inbox for all of your email accounts helps you get more done in less time. Mailspring supports every major mail provider—Gmail, iCloud, Office 365, Outlook.com, Yahoo!, and IMAP/SMTP—so you have a single, streamlined command center for all your messages.

Alias and Masked Email

toolkit@privacy:~$ Help keep your main email protected by using an alias, or masked email service such as **33mail or SimpleLogin**, my two favorites, although there are others as well. Many paid email accounts also offer alias email options, such as FastMail for example. This allows you to use the alias email to protect your true email address, which is a gateway to your identity. Using an alias email allows you to email back and forth anonymously to anyone or any service from your existing email inbox. This will not only add protection for you, but also can aid in figuring out which service has compromised your data if you use a unique alias for each service. Proton recently acquired SimpleLogin which can unlock more features if you have a paid Proton Mail account.

See how it works in depth here: **https://simplelogin.io/blog/what-is-an-email-alias/**



Get a SimpleLogin email addresses (up to 15 different ones for free):
https://simplelogin.io/

Get your own free 33Mail email addresses:
https://www.33mail.com/

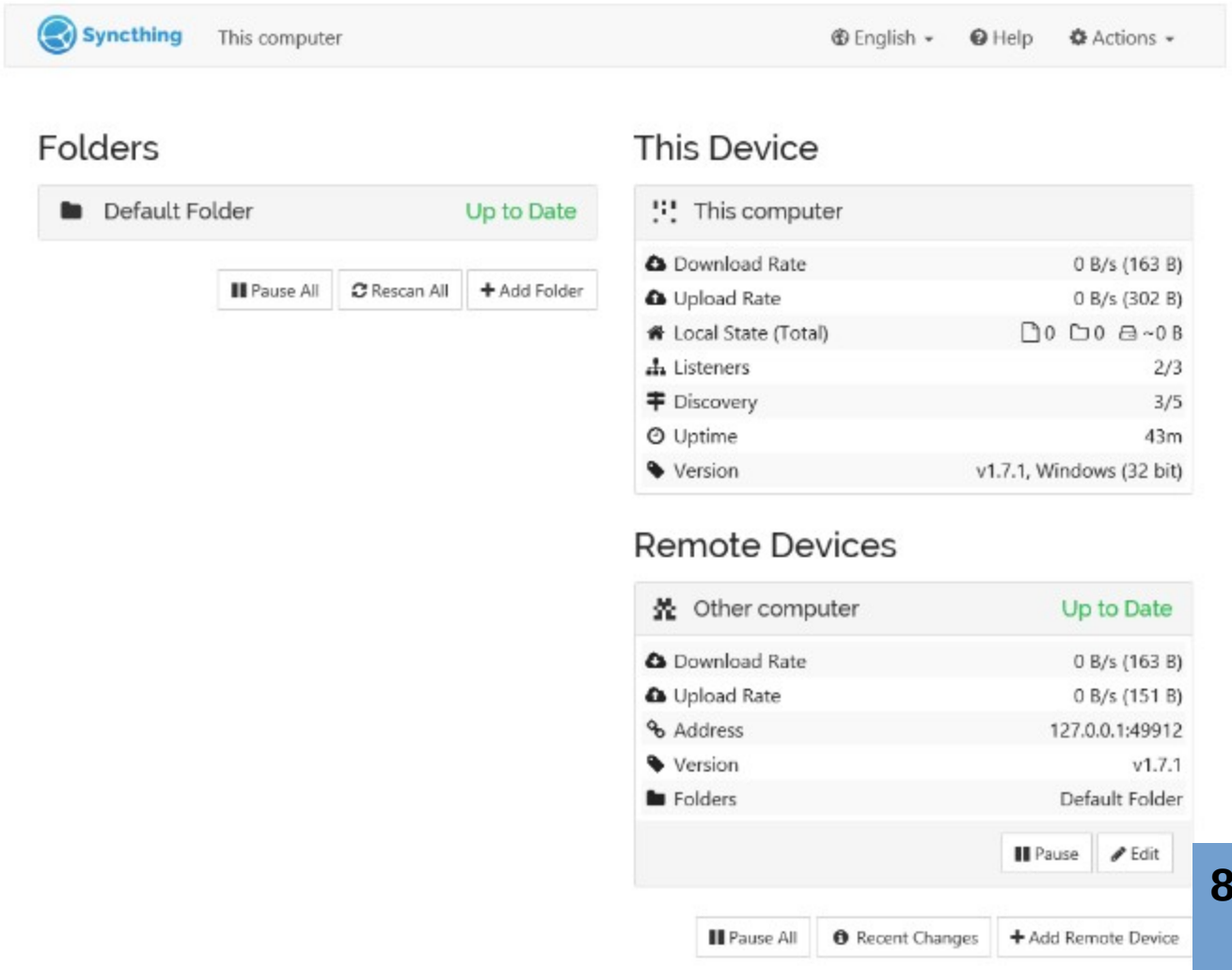
If you have your own email domain, try out their sister service:
https://www.emailengine.io/

Syncthing

toolkit@privacy:~$ Automatically sync your phone and computer for photos and other files, using this free and open source software, download here: **https://syncthing.net/**

Download onto any devices you want to link/sync such as your computer and cell phone. Use F-Droid store to download for Android phones.

Once linked, whatever folders you point it to, will be synchronized on all devices to save time and effort of copying pictures and other files back and forth. See more details on their Get Started page: **https://docs.syncthing.net/intro/getting-started.html#getting-started**

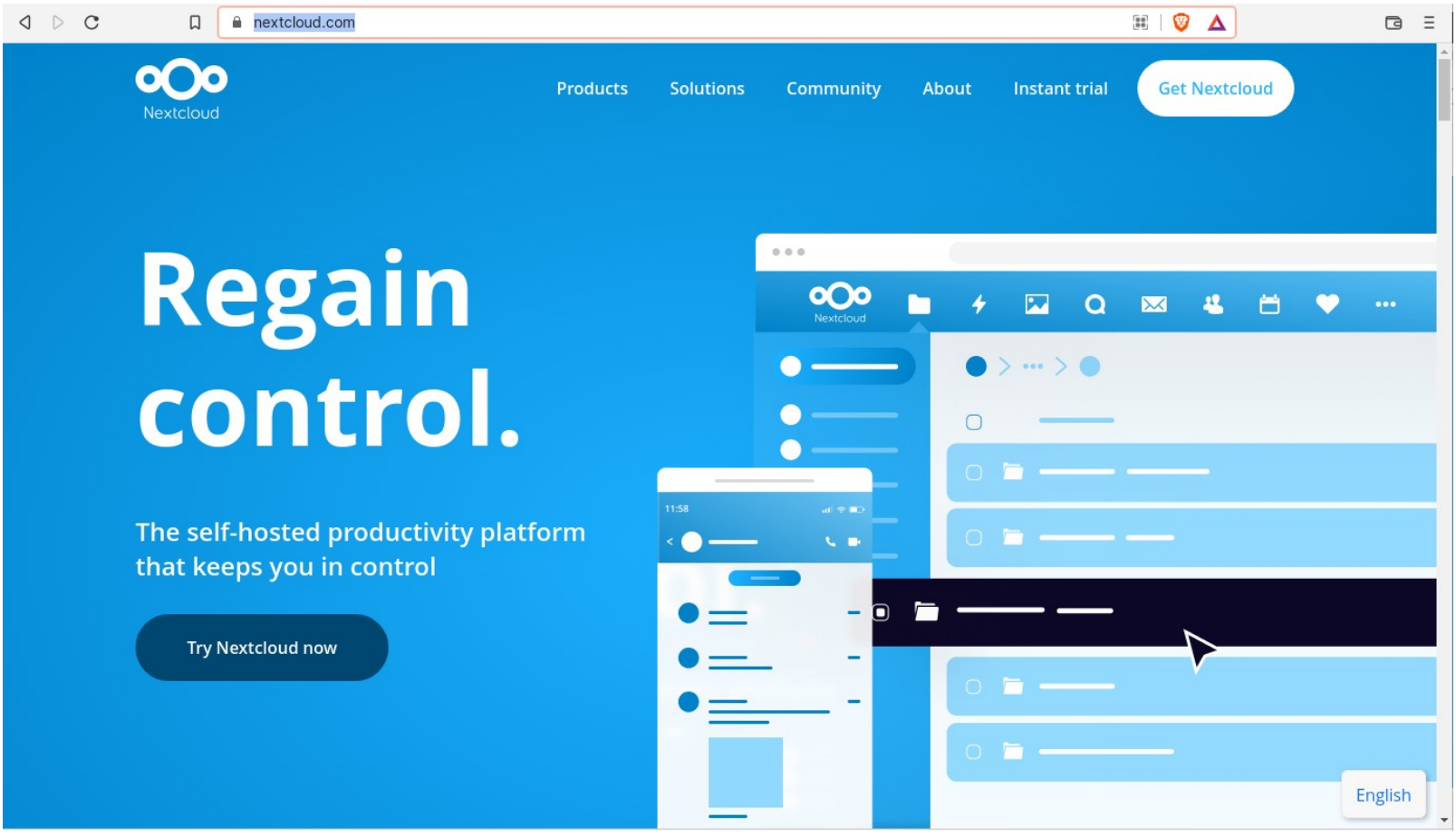


Nextcloud

toolkit@privacy:~$ NextCloud is a very popular tool to host your own servers and take full control of data storage and access. Free and open source, this is a very robust option for those with the desire to self host files. While this is not an easy button type thing to set up, and not ideal for beginners, this is an excellent example of how to shift the tech paradigm. Rather than allow Google and others to host and control all of your files, using options like this puts the control back into your hands, and is completely private, suitable for personal on up to large business level. Did I mention that it's free?

Start learning about file hosting with Nextcloud:

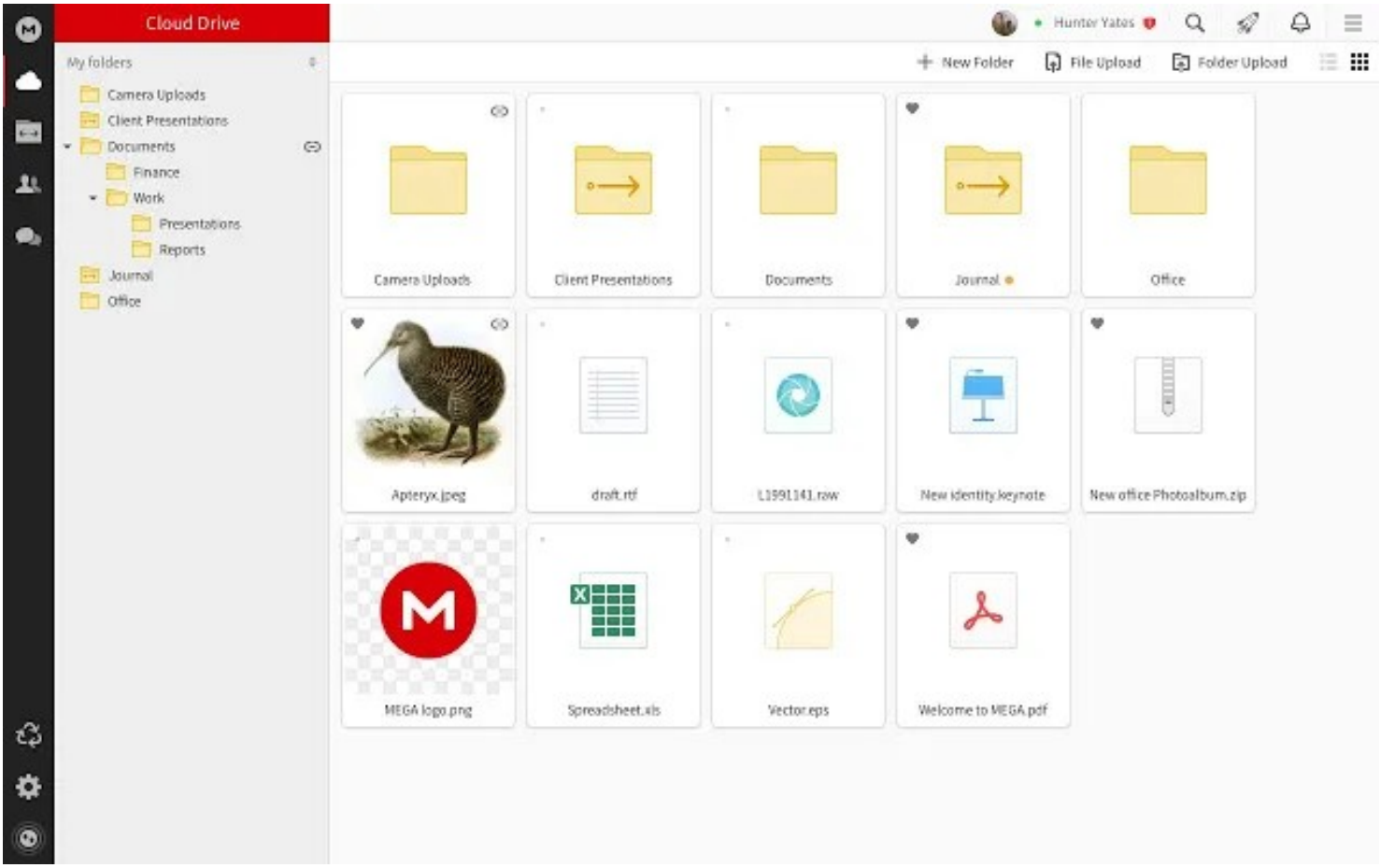
https://nextcloud.com/



Mega.nz Cloud Storage

toolkit@privacy:~$ Mega.nz is an excellent free private cloud for anyone to use by signing up with just an email address. You do get good basic features for the free tier, and of course they dangle the paid tier upgrades in front of you, but many just stick with the free option, which allows a nice 20GB of free storage. Share files back and forth with just a link, the other person does not need an account to view your Mega file/cloud to view and download. You can also give them permission to upload to your folder by whitelisting their email address to do so, and other improved storage and features with a paid account.

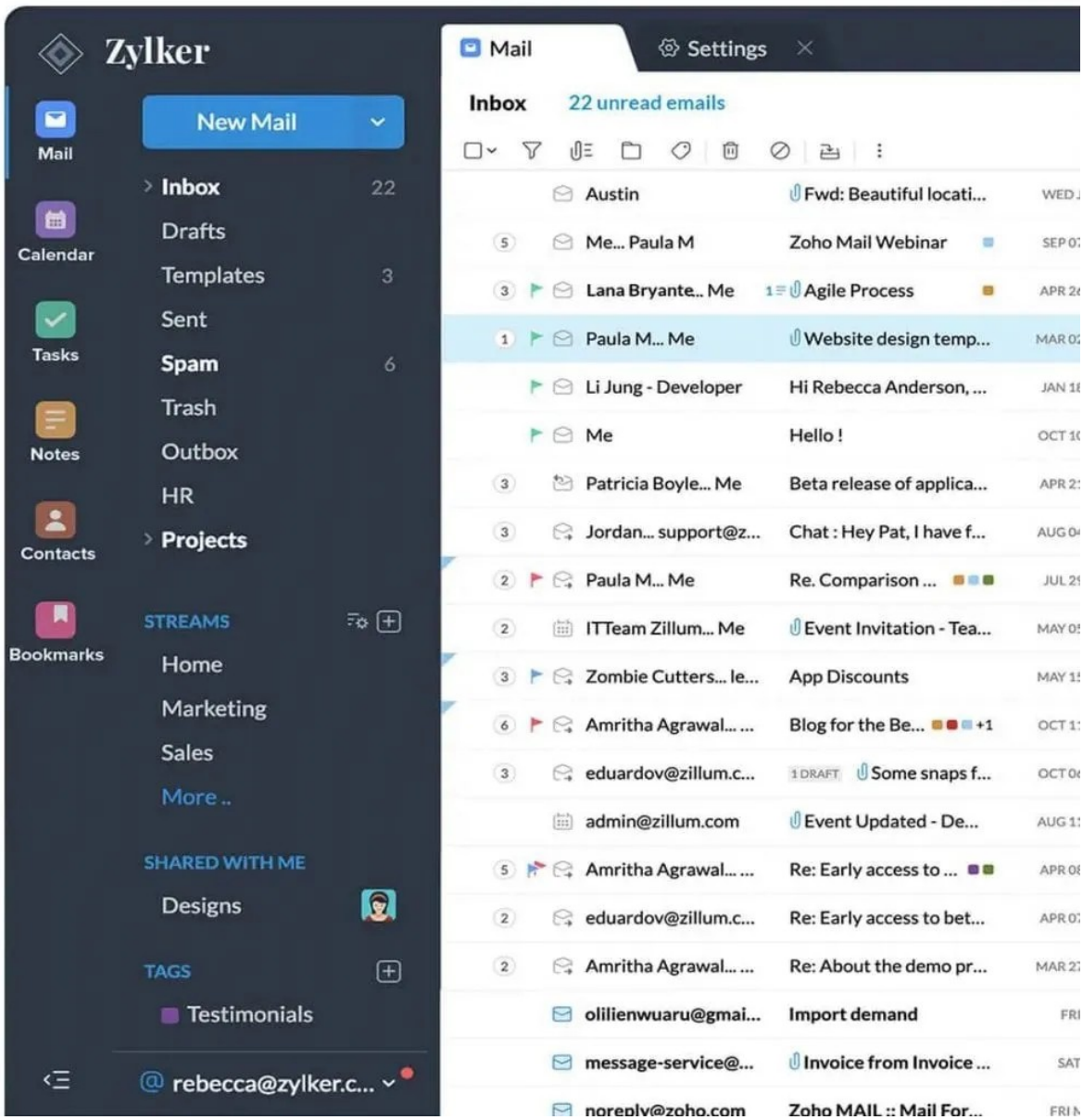
I'm very happy with how simple and easy this service is, and looking forward to seeing this one continue to develop, it's treated me well so far as a user.



Create a free account here:
https://mega.nz/

Zoho

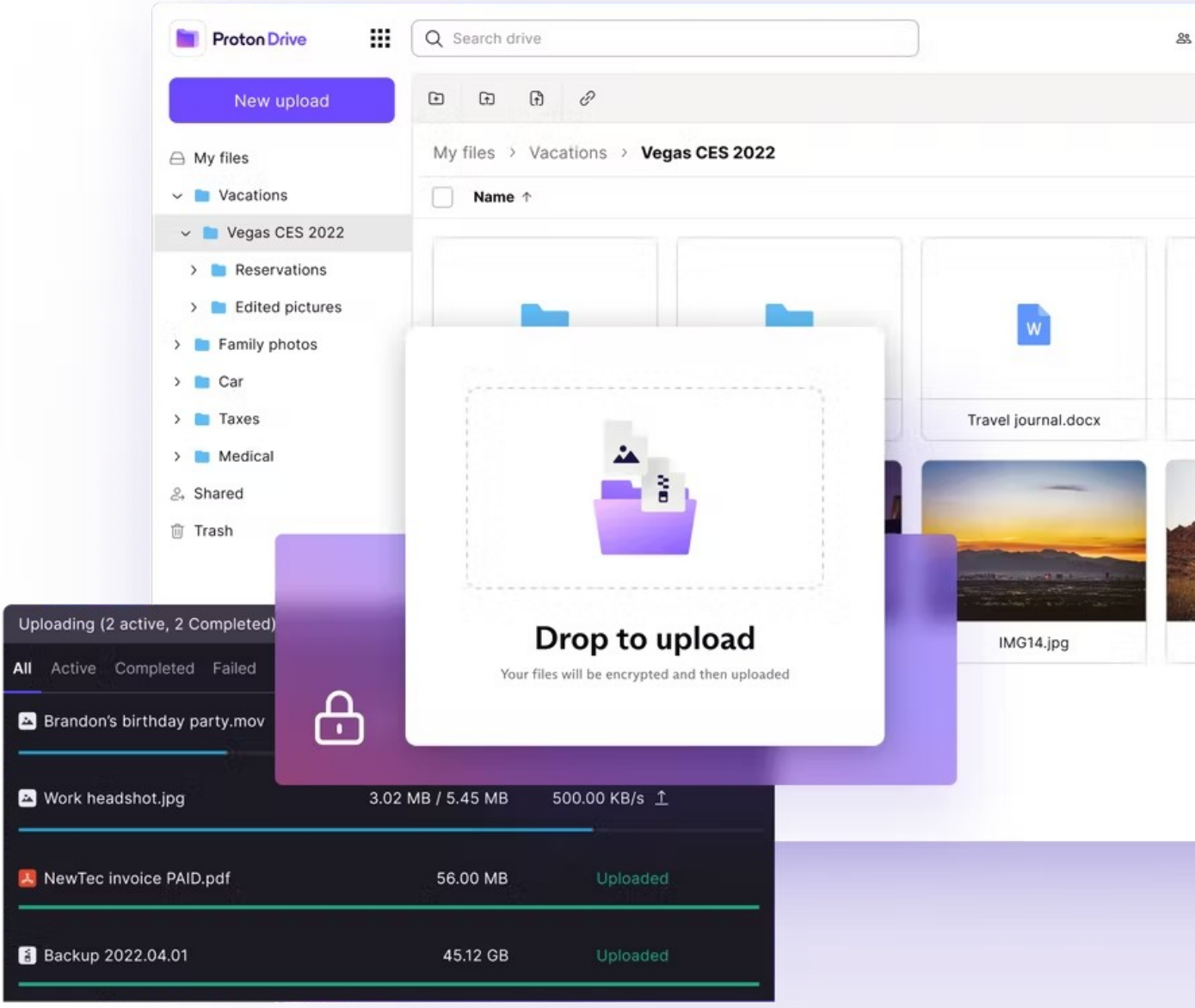
toolkit@privacy:~$ Zoho is an extremely robust option for just about anything for personal use, up to the large enterprise level. Email, cloud storage, AI analytics, invoicing, and endless other products any business large or small could possibly need or want. Zoho has been a slow and steady up and comer, creating direct competition to the established big tech platforms, creating a more privacy respecting service to fulfill any digital task you can imagine, and all ad free. For free cloud storage, you get 5GB to start with which is pretty decent, but explore their site for the massive collection of software products available for you or your business on paid tiers.



Sign up for a free account here:
https://www.zoho.com/

Proton Drive

toolkit@privacy:~$ Proton is one of my top choices for email, file storage and VPN service. Proton Drive gives you secure online storage linked with your account, with different tiers of paid options to increase storage limit and unlock other features. They also increase your email and other storage the longer you stay with them as a reward. Their products are similar to Gmail and Google Drive but are encrypted even so that Proton cannot view the files. In contrast, Google scans your documents, images and other content for various controls and analytics. The free tier of Proton Drive offers 1GB of storage to get you started.



Create a free Proton account here:

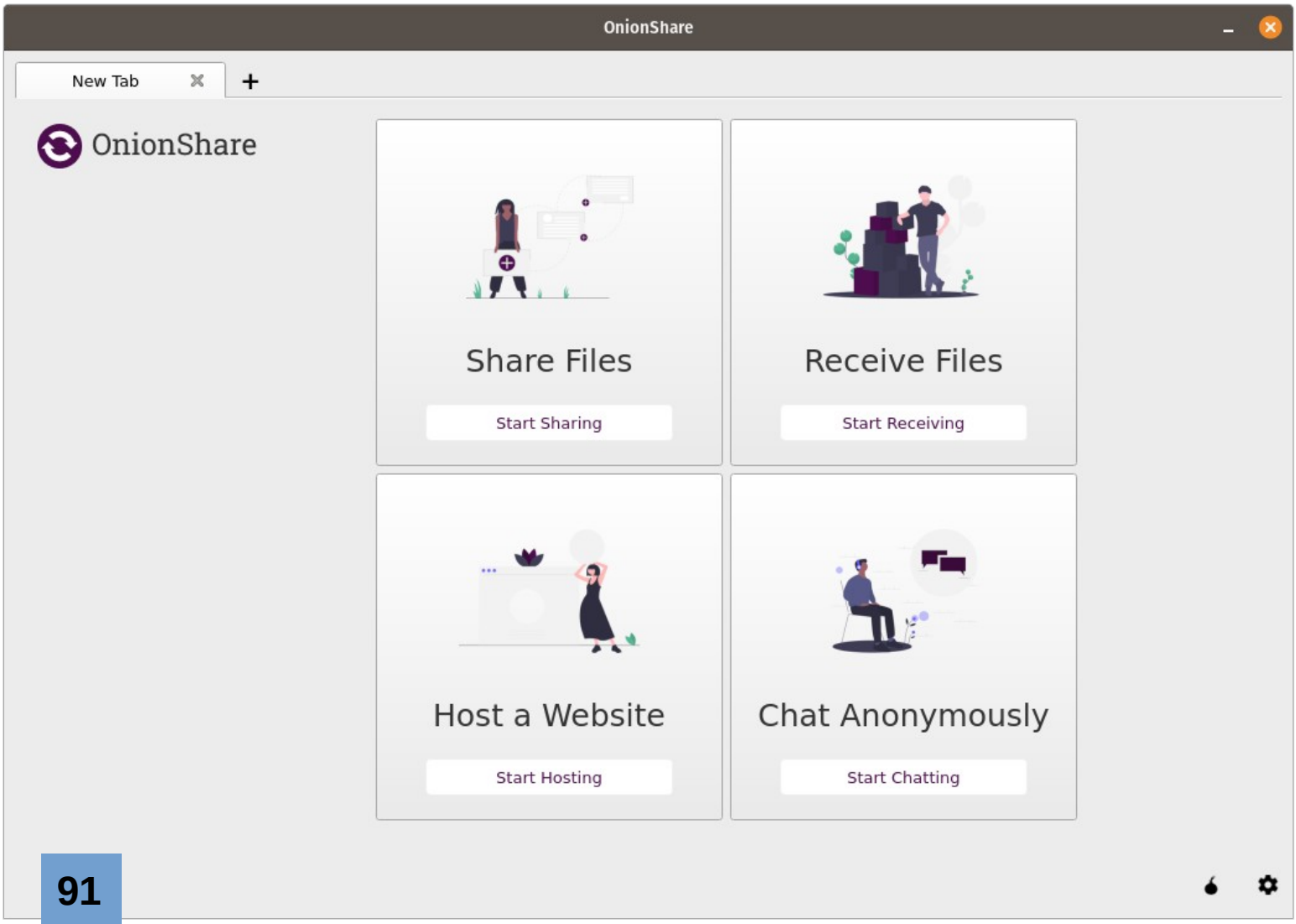
https://proton.me/drive

OnionShare

toolkit@privacy:~$ A less used option for file sharing, is actually quite a good one, at least for folks that don't mind the so called 'mysterious dark web' connotation of using Tor and Onion routing type connections. This provides an excellent way to share content confidentially, a valuable feature beyond just file sharing with Google with our identities attached to our accounts, and our content scanned for 'wrongthink.' OnionShare is free and open source, and can even be used to host a basic website if you wish, on the fly. Overall this provides us an option for a backup if nothing else; I truly enjoy having redundancy for communication. If using Linux, I recommend using the Flatpak download for this program.

Download OnionShare here:

https://onionshare.org/

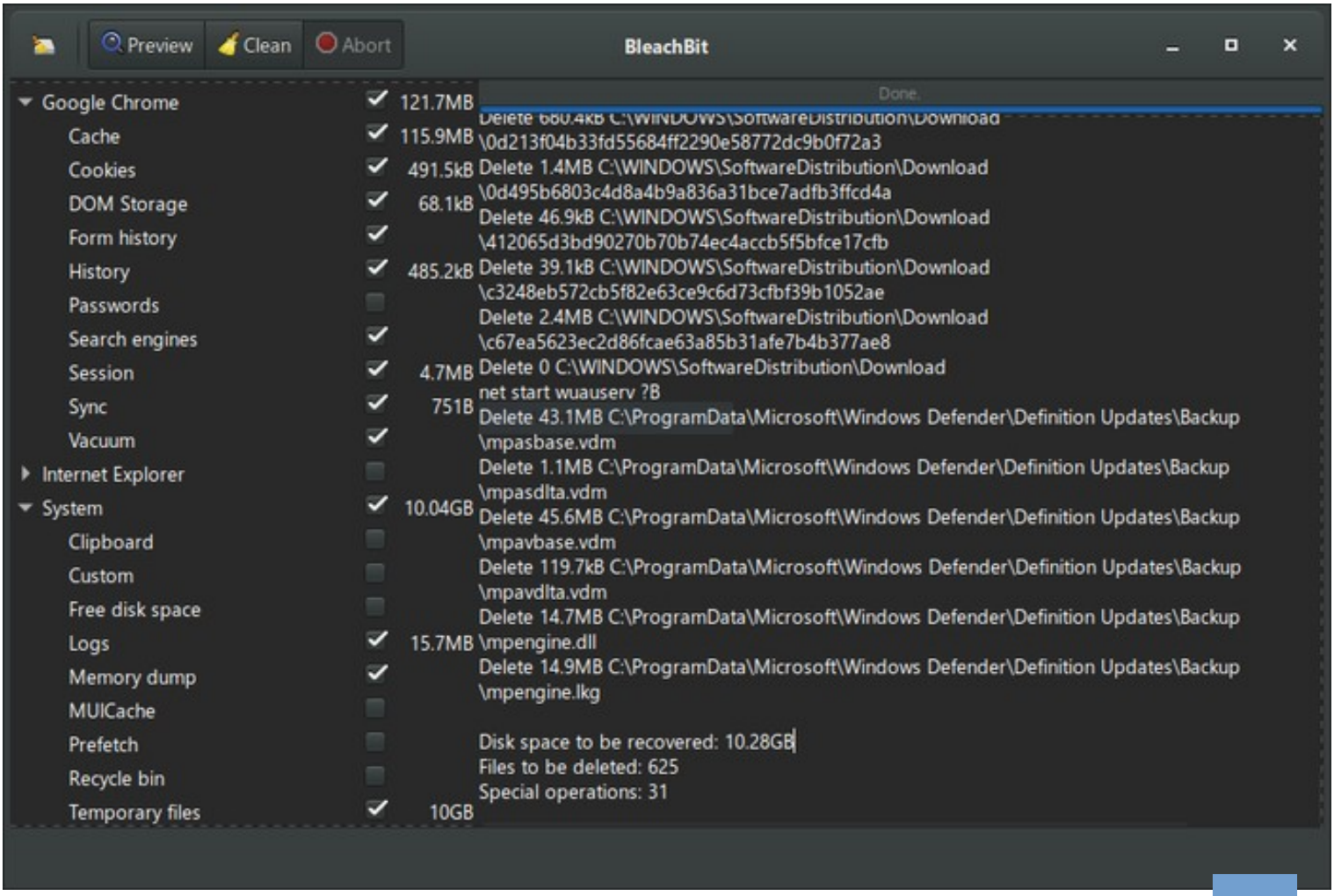


BleachBit

toolkit@privacy:~$ This is a free and open source app for your desktop to clean the digital junk off of your system and create free disk space, and can be used to securely wipe or erase drives to prevent data recovery from them. This is a must have to keep your system tidy, and unlike other apps, it preserves your privacy.

Use BleachBit to:

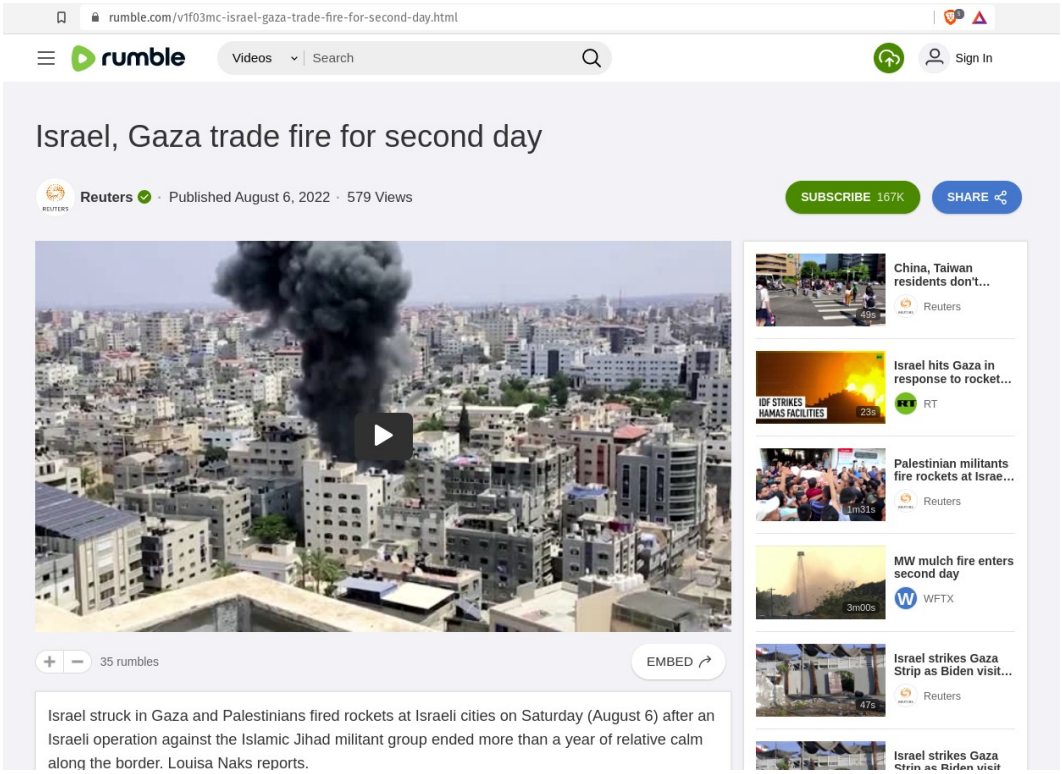
-Free disk space
-Reduce the size of backups and the time to create them by removing unnecessary files
-Maintain privacy
-Improve system performance (by vacuuming the Firefox database, for example)
-Prepare whole disk images for compression (common for "ghost" backups and virtual machines) by wiping free disk space



Download BleachBit here:
https://www.bleachbit.org/

YouTube alternatives

toolkit@privacy:~$ Even if not logged in, YouTube (parent company Google) collects a ton of usage data, and perhaps even link that activity to your ‘dossier’ with various tools on their end. YouTube also engages in censorship of certain political topics, medical information and many other areas to limit what we see, and to promote ‘approved’ content. Who gets to approve or disapprove of what we see or don’t see? Increasingly, that answer is not just YouTube or Google, but even government level input, as revealed recently. (Alex Berenson, Justin Hart lawsuits against Twitter.) With these types of abusive propensities, I recommend people use alternative video hosting platforms that don’t censor and manipulate content.



My top alternative is **Rumble.com**, an increasingly robust video platform that functions the same as YouTube, and is actively fighting back against censorship.

Others I frequent that also offer either a separate service, or in some cases simply spoof YouTube to isolate your identity from them, include (click on links to visit sites:)

FreeTube (desktop app, coming to mobile soon) https://freetubeapp.io/

Odysee / LBRY: https://odysee.com/ https://lbry.com/

BitChute: https://www.bitchute.com/search/

NewPipe (for Android): https://newpipe.net/

Brandnewtube: https://brandnewtube.com/

Vimeo: https://vimeo.com/

Invidius: https://invidious.io/

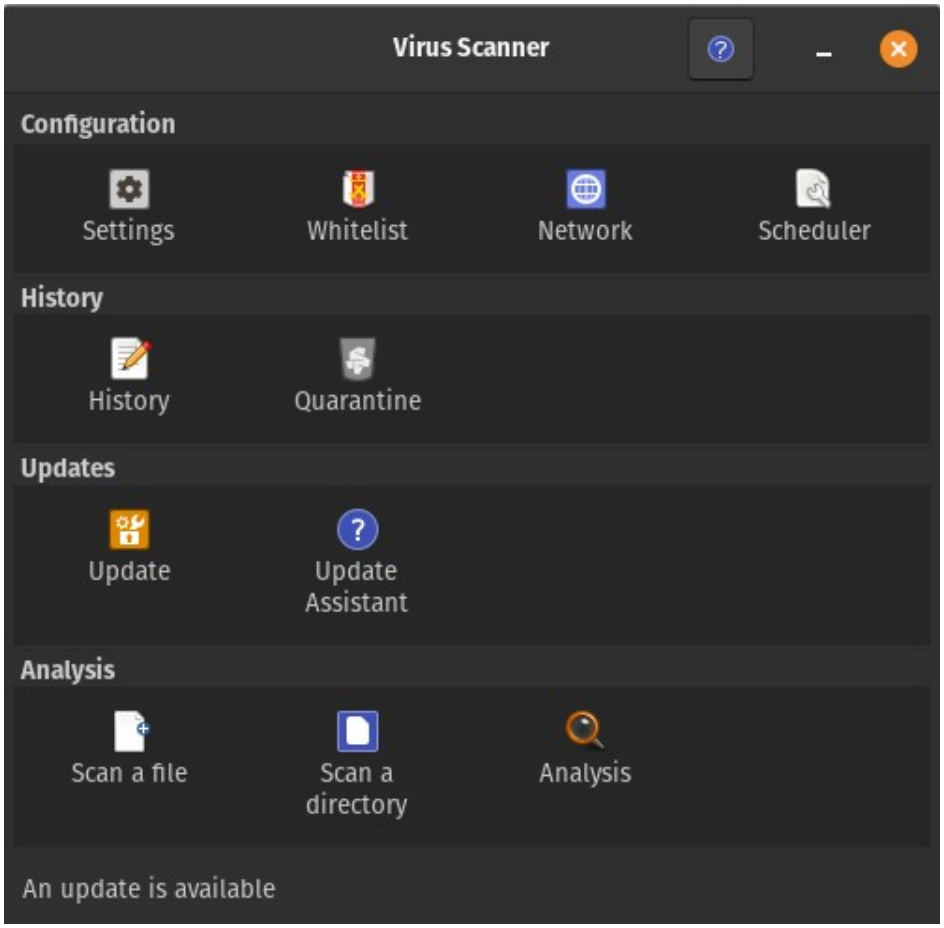
ClamAV (AntiVirus) and UFW

toolkit@privacy:~$ While most malware targets Windows machines, there are still plenty of attacks against Linux systems, so we want an anti-virus program to help sniff out malware while using Linux. ClamAV is free for all to use and is open source software. There are countless other things to do for Linux systems to lock down your machine, but this is an easy one to install and manage, especially with the ClamTK version for newer users.

https://linuxhint.com/install_clamav_ubuntu/

In addition to installation and use in Command Line Interface (CLI, or 'Terminal') ClamTK offers a GUI (Graphical User Interface) version for easier use (image below.) Update either ClamAV or ClamTK frequently, then scan any or all directories for any malware. This can be used to scan unknown USB drives for example, to see if they contain any malware, before trusting them.

In addition to ClamAV, Linux systems come with a built in firewall called **Uncomplicated Firewall (UFW)** which can also be run from either the terminal, or GUI, to setup firewall rules for all incoming and outgoing traffic. The GUI version is referred to as GUFW and may be easier for less tech savvy users, see more details here: **https://itsfoss.com/set-up-firewall-gufw/**



Resources for more Learning

toolkit@privacy:~$ Disclosure, and full transparency, I do not have any benefit or financial gain from any of these resources beyond owning a small amount of CFVI (Rumble) stock, these are resources that I have found to be most helpful on my trek towards better digital privacy and security. I hope you get the same improvements in your life as I did from these, enjoy and good luck on your own journey. Remember there is no destination, just enjoy the ride, and the benefits of better privacy. These are simply entry points to help discover endless others and their content. I highly recommend checking out Jeffrey Peterson and Bones Tech Garage Telegram channels for those interested in a better way forward for technology. You'll find just about everyone including people in their 70's plus switching to Linux, and taking interest in tech. Both are very friendly and informative channels.

Just because there is not an end destination, does not mean we don't know where we are going. The goal is to know more than you did yesterday.

Mike Bazzell hosts a podcast, writes books and maintains a website which has been an absolute goldmine on privacy and tech: https://inteltechniques.com/
His books are worth their weight in gold, try his *4th Edition of 'Extreme Privacy: What it Takes to Disappear'* and *'OSINT: 9th Edtion'*
His excellent podcast is 'Privacy, Secruity and OSINT (Open Source Intelligence)

Rob Braxman (Rob Braxman Tech) for privacy topics on Odysee:
https://odysee.com/@RobBraxmanTech:6

Network Chuck on YouTube for general tech: https://networkchuck.com/

The Watchman Privacy book and podcast (Gabriel Custodiet) on privacy to the extreme, and Bitcoin courses: https://watchmanprivacy.com/

John Hammond, tech deep dives: https://www.youtube.com/c/JohnHammond010

Resources on Telegram to start with:

Jeffrey Peterson – (jeff.pro)	t.me/jeffrey_peterson	<-->	and **jeff.pro forums**
Bone's Tech Garage	t.me/BonesTechGarage		
Linuxgram	t.me/linuxgram		

Other sites:

Linux distribution overview: https://www.javatpoint.com/linux-distributions
https://answers.syr.edu/display/ITHELP/Linux+Distributions
Excellent FOSS news and updates: https://itsfoss.com/

Books: *'Digital Minimalism: Choosing a Focused Life in a Noisy World'*
Mike Bazzell and Gabriel Custodiet books listed above
'How to Be Invisible: The Essential Guide to Protecting Your Personal Privacy, Your Assets, and Your Life' by J.J. Luna
More: https://www.goodreads.com/shelf/show/privacy

Please share this guide, and for any feedback good or bad, or for any questions, you can email me at:

toolkit@graphenegoat.33mail.com