GrapheneGoat's

Digital Privacy Quick Start Guide

A Tech Normie's first steps towards meaningful digital privacy and security

GrapheneGoat.com

Sections in this Guide

1. Do immediately / Easy button Digital Privacy

This section involves very quick and easy tasks such as signing up for email, Virtual Private Networks (VPN), anonymous virtual payment cards and much more. These are all things that can be deployed immediately, and for free.

2. We need to fix your operating system part 1: GrapheneOS

It's time to address the elephant in the room; your Operating System (Mobile devices). In this section we discuss how to migrate to a secure Android device, arguably one of the most important changes we can make to shut off the tracking and tracing of our digital lives.

3. We need to fix your operating system part 2: Linux

Much like our phones, we need to take control over our computer Operating System using Linux. These days this is a much easier task than you might imagine, and is the only way to break free of big tech's spying and tracking our every behavior.

4. Continue your journey

Learn about where to discover more resources to continue your own privacy journey. While there is not necessarily a destination, the journey itself is the adventure and will reward you with taking back your own digital sovereignty and dignity. Encourage others to join you as you discover a better way to embrace Free and Open Source Software (FOSS) and Technology.

GrapheneGoat.com

*Cover page image: Mt Olympus summit, Washington state, USA

Foreword

Please view this guide for what it is, a simple and easy pointer towards a better way to use technology. (and a better way by *NOT* using certain technology…) Approach this from the point of view that this has all been well researched and tried out by many before you, and while I don't go into very much depth here for the sake of just getting things done, know that more information about each of these topics is well discussed on the website https://graphenegoat.com/ and on the forums listed in the last section of this guide, so don't let perfect be the enemy of good enough (for now).

I can almost promise you that you'll never 'feel ready' to jump into a so called privacy journey. If you're waiting to begin because you want to learn everything first so that you don't make a mistake, I'm living proof of why that is not likely to happen. *You will absolutely make mistakes*, however do not let that thought prevent you from beginning.

We could study books and videos on how to, say, ride a bicycle for years, but without actually ever getting on a bike ourselves, we don't possess the skill to actually ride the bike. Privacy and Security is no different, simply begin by addressing each topic in this guide and don't worry about not doing it perfectly. Often the very best way to learn something is by making mistakes, we tend to learn from mistakes much more strongly than we do our successes. In a short time, your mind will adapt to a new way of thinking about the technology we interact with as you exercise your new skill set. It will pay dividends in the future, I can almost assure you of that.

It should also be mentioned, that whether we are talking about any given software, setting or operating system, there is absolutely no 'point of no return' in any of this. No one can instantly become comfortable with a completely new system overnight, so gradually begin using these tools, and only switch to them once you are reasonably comfortable.

I think you'll find that most of these Free and Open Source Software (FOSS) options will make your life a lot cleaner and leaner, and overall a better experience for several reasons. One, we are removing the growing cancer that is big tech spyware that tracks our every move, but two it is generally a much cleaner user experience; less bloatware, spam, junk, notifications, clutter and useless advertising bothering you as you use the technology. The content of this guide is a result of my life gaining incredible satisfaction by taking control of my data sovereignty. I sincerely hope this helps you as much as it did me, now go forth and begin, and never stop learning if you want to be free.

"Saying that your privacy doesn't matter because you have nothing to hide, is like saying that your freedom of speech doesn't matter because you have nothing to say."

-Snowden quote

Foreword (cont'd)

Some key areas to think about as you begin your transition to better technology are decentralization, open source, zero knowledge encryption, end to end encryption and using proper security when creating and using passwords, and always use Two Factor Authentication (2FA) on your accounts where possible.

Centralized - - - > Decentralized

Closed Source - - - > Open Source

No Encryption - - - > Zero Knowledge Encryption

Phone Contract - - - > Own fully Unlocked Phone

Poor Passwords - - - > Unique, Long, Strong Passwords

No 2FA - - - > 2FA using Software Token app and/or Hardware Tokens

These above concepts apply, but are not limited to hardware devices such as your mobile phones and computers, and software or applications and services that we use.

Centralized control of a system puts one entity in full control (think Google's strangelhold on the internet) vs. Decentralized such as Tor (The Onion Router, or 'dark web') where it would take an immense undertaking to take down all 7000+ Tor nodes. No one central authority truly controls it. Many crypto currencies operate this way as well, no centralized figure can shut down something like Bitcoin.

Zero knowledge encryption means that only we possess the decryption key to our data, such as our email or cloud service. Google Gmail for example, can see all of our data and email traffic, however it is encrypted (they possess the keys.) However with a service such as Proton Mail, it is encrypted but Proton does not possess the keys, only us as the user can view the data. This gives us full control on who gets access to our email data, but apply this to other applications such as note taking apps and cloud storage, etc.

For our devices such as phones and computers, whoever controls the Operating System (OS) controls the device. I also strongly advocate to avoid mobile phone stores and contracts, in favor of buying a fully unlocked phone outright and owning it. This allows us to remain anonymous if we choose, and allows us to use any OS on the phone, and any carrier we wish to use. No contracts or credit pulls just to buy a phone.

The most important topic of this guide is to begin using a Password Manager, and Two Factor Authentication on all of your accounts. Doing so properly will make you as close to 'hackproof' as possible. This is often overlooked these days, I see some pretty horrendous and weak account security 'out in the wild,' ignore this at your own peril.

Overall, as you encounter the next shiny new service, device, whatever- think through the prism of these above concepts before blindly accepting to use it. Enjoy.

Section 1:
Do immediately / Easy button tasks

In this section I demonstrate how to get up and going, no matter what type of phone or computer you have. Do these simple and easy quick tasks in approximate order as you find the time. Many of these only take several minutes to accomplish, yet they gain you quite a bit of both security as well as privacy.

Take decisive action. Today.

Your future self will thank you.

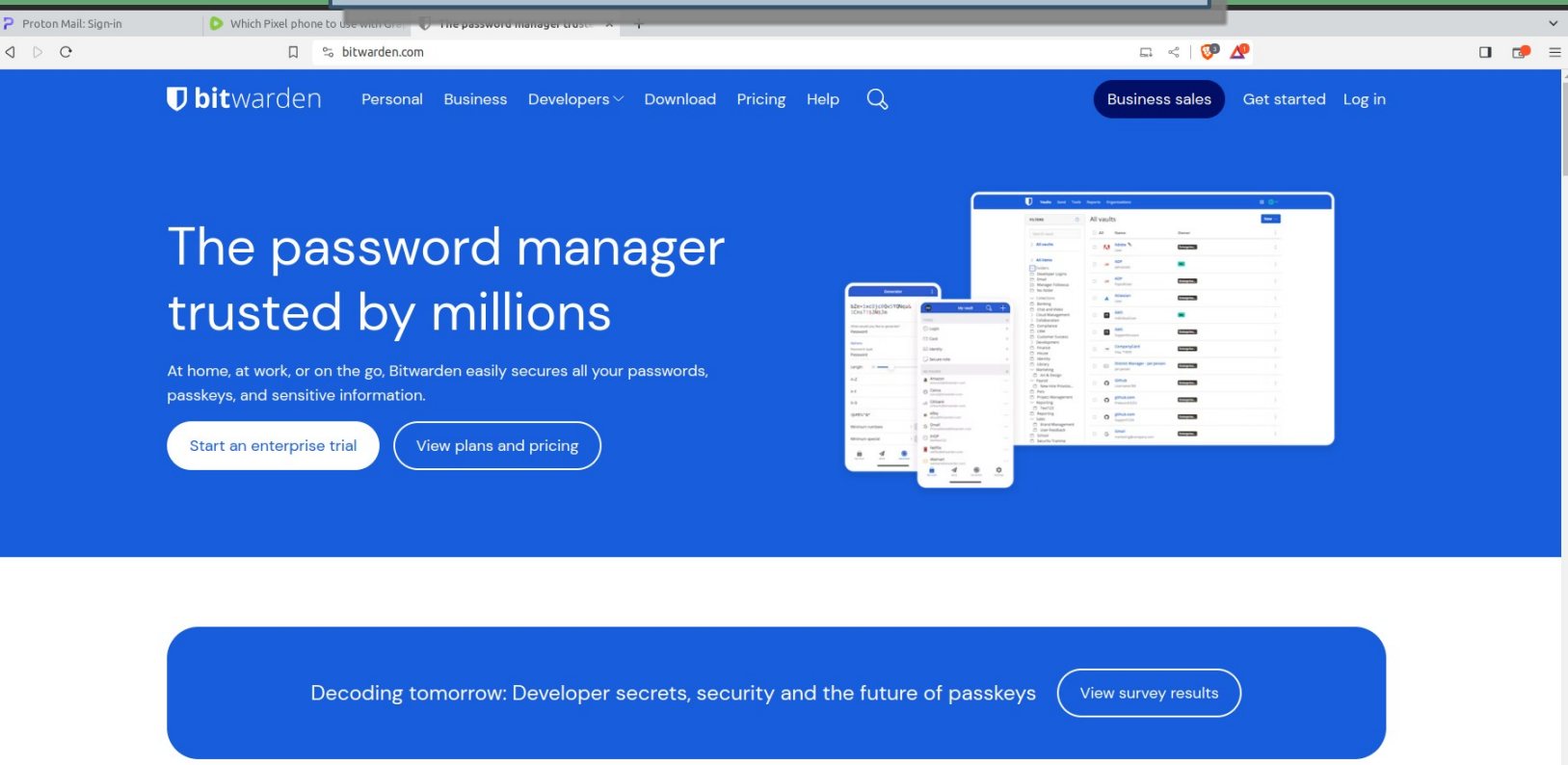
1. Password Managers
2. 2FA (Two Factor Authentication): Aegis, Ente Auth, Standard Notes, Yubikey
3. Proton Mail, VPN, Drive, Pass, Authenticator, Calendar and Lumo AI
4. Alias email: SimpleLogin, 33mail and AnonAddy
5. Privacy.com virtual card account
6. Extra Cloud storage: Proton, Tresorit, Mega, Icedrive, Internxt, Zoho
7. Signal Messenger, Session, Jami, Mirotalk, Telegram
8. Standard Notes
9. SSD External Drive: Local data storage
10. Data Encryption: VeraCrypt, Cryptomator, EDS Lite
11. Export contacts to .vcf, Export email and contacts
12. Credit Freezes

Password Managers

Yes, there is a great reason why I choose this as easily the first thing to do. Using a password manager coupled with good Two Factor Authentication (2FA) will make your online accounts nearly impossible to breach. There are several that I really like, and like to recommend to others.

With a password manager, you only have to remember *ONE* good strong password that unlocks your password manager database, making life much, much easier for us.

Bitwarden



***Important: even though your data is saved on a remote server, you need to periodically download (export) a copy of this database and store it safely.**

Bitwarden is a cloud based password manager that should suit nearly everyone. The benefit to this one over something like KeePassXC is that your database is automatically synched in a secure cloud for you, plus gives us an offsite backup copy.

Bitwarden can be used from a web browser, or you may download the app to any device and begin using immediately to store all of your login information, or credentials.

This manager is also open source software, and is fully encrypted end to end (E2EE) with zero knowledge (meaning even Bitwarden cannot decrypt your information). This means that we must remember our password or you will lose your database, there is no one at Bitwarden that can recover your account.

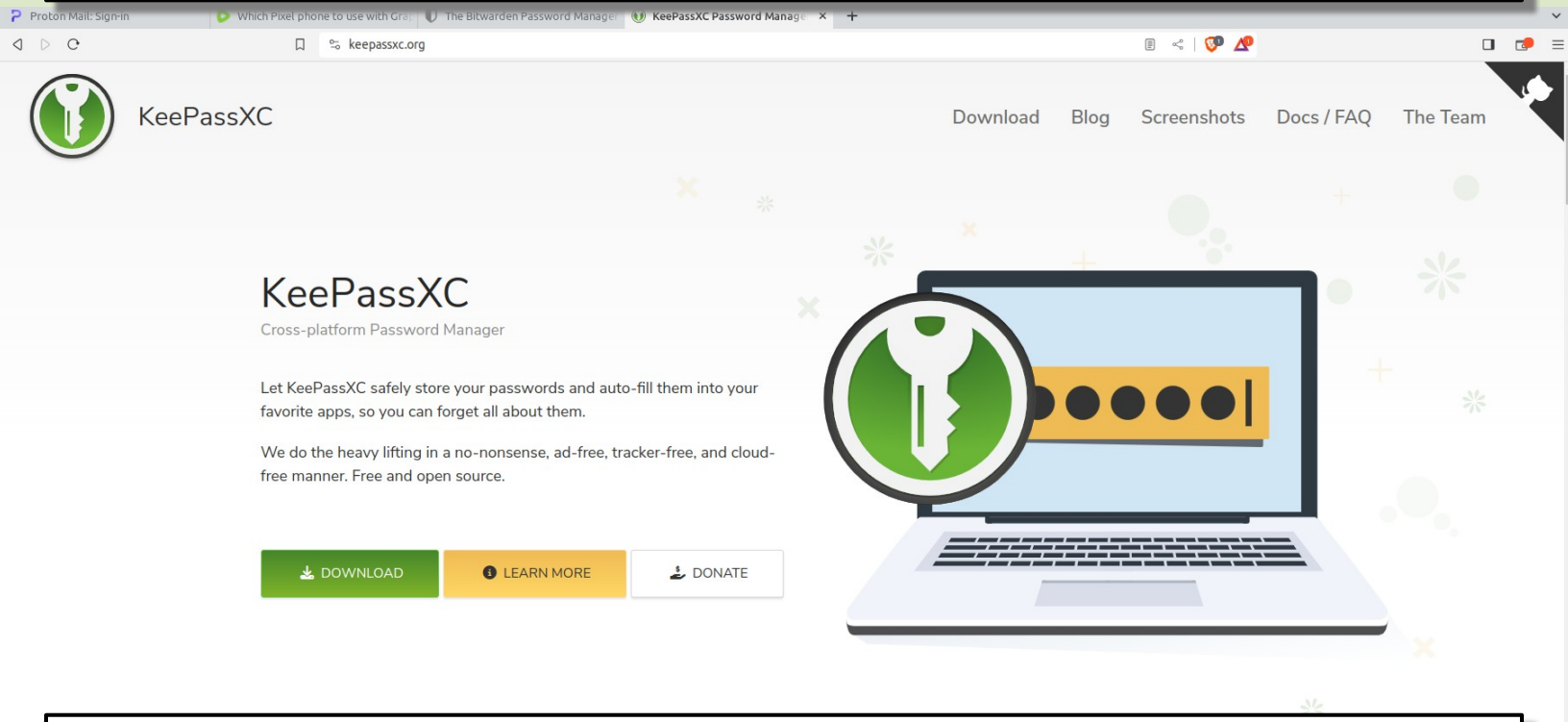
Password Managers

KeePassXC

KeePassXC is arguably the more secure of all of these since the database file is stored locally and not on a remote server. However this is also a disadvantage *IF* you don't have good data management habits, so this may not be the best for everyone. If you don't have solid data management discipline, then this may not be the most appropriate option.

You are responsible for managing copies of this, it will not sync automatically, you have to update each instance manually. Many will not want to do this, but it is what I prefer for the most extreme cases of privacy and security. Remember, this is an extremely damaging thing to have compromised as it's quite literally the keys to our entire life.

While you certainly can back this up in a cloud of your choice for online access, it is not as convenient to use as such, compared to something like Bitwarden.



My own use case for KeePassXC looks something like this:

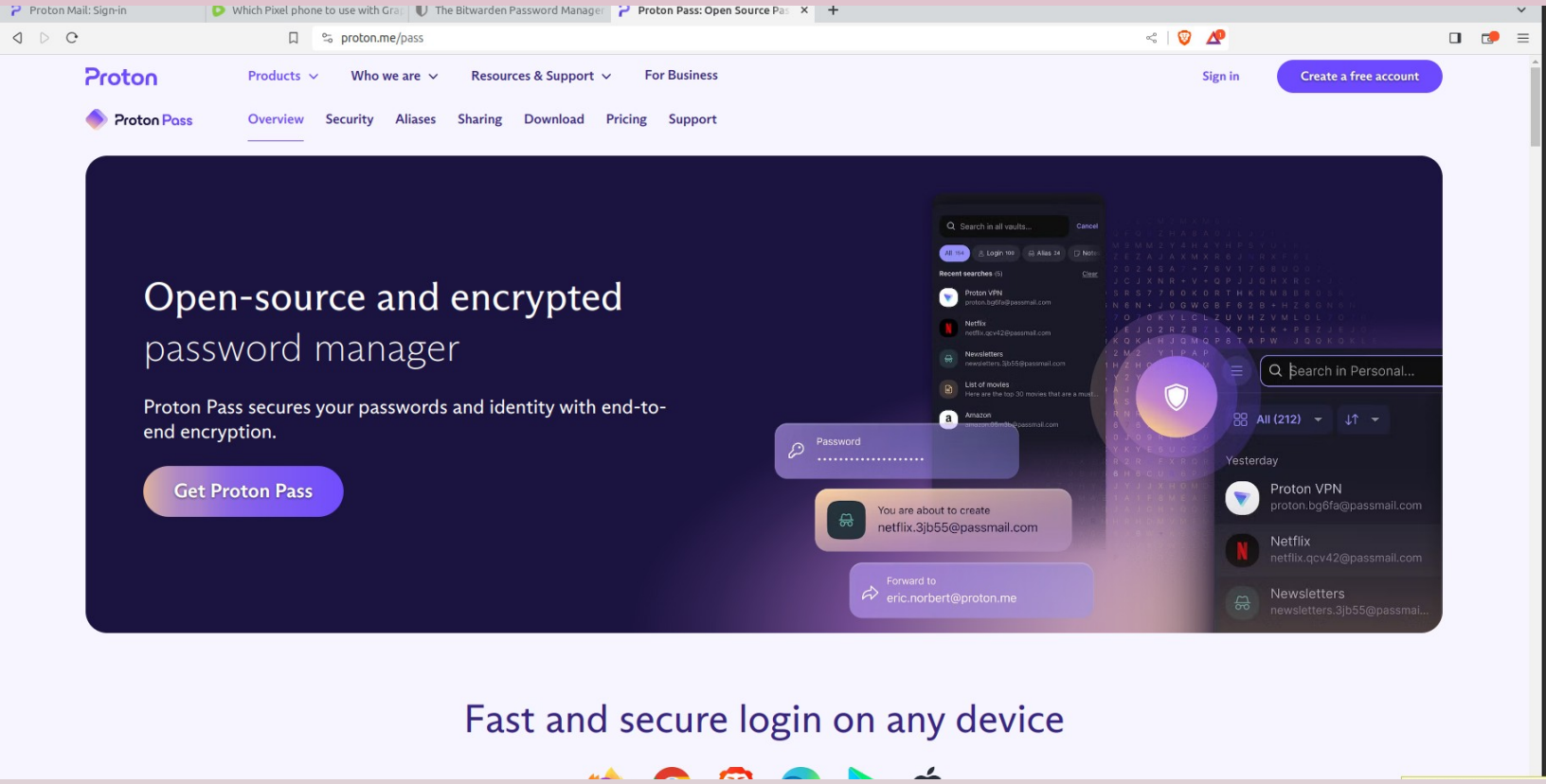
Download KeePassXC software and create a new database, save onto a USB

About once a week I copy the database file to several other backup USB sticks as well as a copy in a secure, encrypted cloud

This USB stays with me at all times, so I have constant access to my database, even with no internet connection

Password Managers

Proton Pass



This is an excellent option by Proton, this provides the user with a password vault on a remote cloud server. Your data is end to end encrypted and even Proton does not possess the ability to view your passwords and data.

This means that much like the others, we have to maintain control of our database by remembering one unique, strong password to get us into the database, as well as any 2FA that is enabled on the account (highly recommended to enable 2FA, or Two Factor Authentication as discussed shortly).

Proton now also has their own Authenticator app as well, so you can choose to use Proton for both your passwords as well as your 2FA.

** Also, since we now have a Proton account up and running, go ahead and download their VPN on each of your devices and begin using this tool to hide your true IP address when signing up for the remaining services in this guide.

While using a VPN is very helpful, it is not magic, there are many other ways in which the devices we use are being ‘fingerprinted’ but that should not deter us from using the VPN. A VPN encrypts our traffic as well as hides our traffic from the internet service provider, or ISP. Other VPN options include **Mullvad VPN** and **IVPN** **

Password Managers

Now let’s talk about passwords themselves

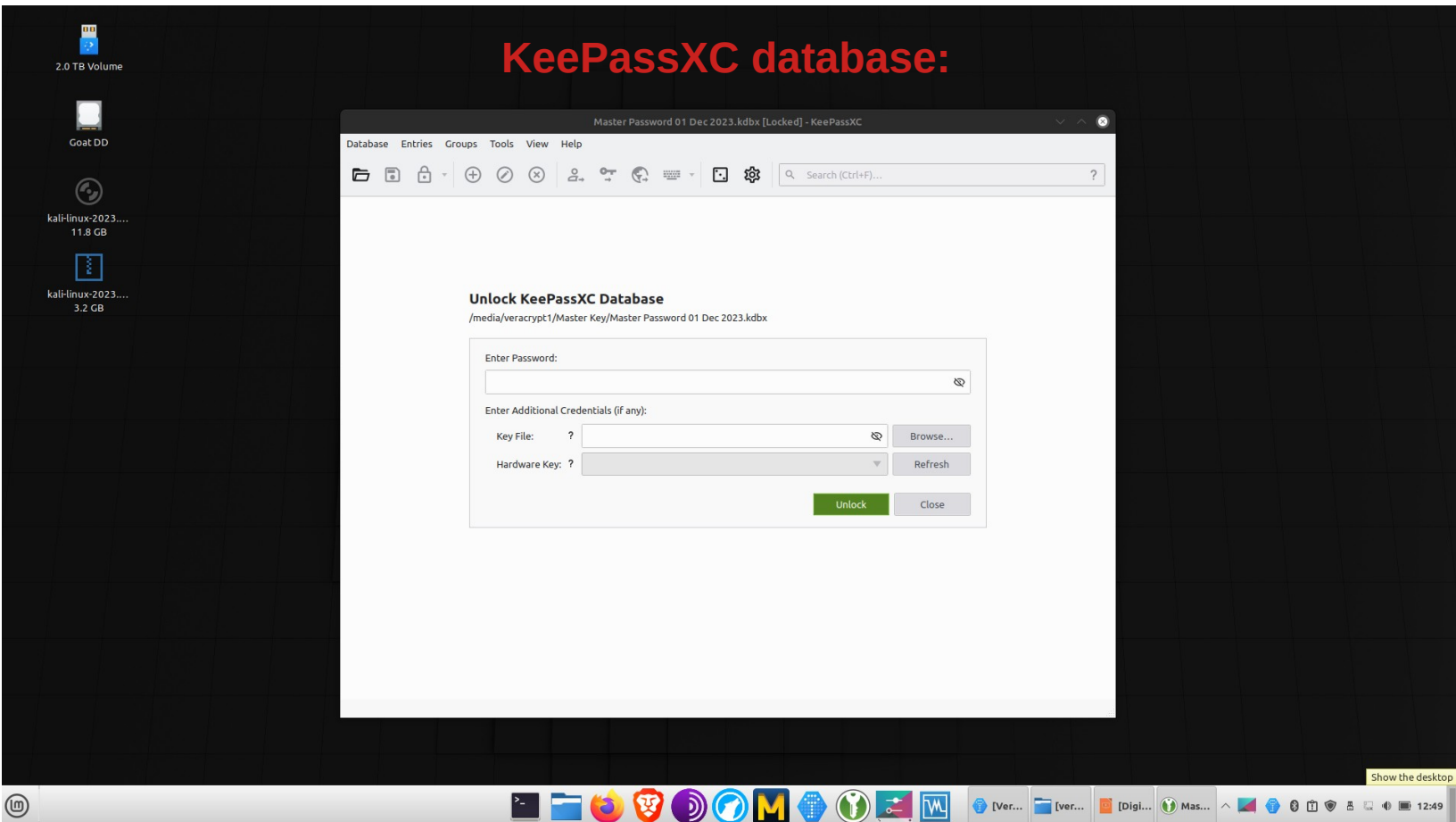
Do:

Use your password manager for all accounts
Use the manager to generate a random, unique password for each account
Choose a minimum of 12 characters, go higher to increase strength
Use all 4 types of characters in your password
Change your password periodically
Lock your database when not in use
Store a copy of your database safely in at least three places

Don’t:

Make up your own passwords (unless you adhere to 4 types of 12+ characters)
Use your pet’s name or birthday in any part of your password
Ever use the same password on ANY two accounts
Ever use an old password you’ve used before (recycled passwords)
Use a ‘racetrack’ or any keyboard layout pattern, these are easily cracked
Use a weak password to access your password manager database

KeePassXC database:



Two Factor Authentication (2FA)

While using a proper long, unique strong password on our account is a great way to help secure things, we can make it exponentially harder for an attacker to gain access by enabling 2FA. This is done in several ways as shown below, try and use either a software or hardware token, or email TOTP, rather than SMS text.

Using a Password Manager correctly, along with 2FA, will almost guarantee that your account will be safe, don't be the low hanging fruit waiting to get breached, use 2FA.

In any of these cases, you will first enter your account username and password, you will then be challenged for a second authentication using one of the following:

SMS Text message

Poor choice due to SIM swap attacks and cross device tracking, but this is usually better than nothing. Use any of the others below instead, to maximize your security.

TOTP – Temporary One Time Passcode

This is similar to SMS Text, usually done through email. This is an acceptable, strong way of providing 2FA on any account provided you use email account that is secured well.

Software Token

Excellent choice of 2FA, this is an application that you will download/install on your device, this will store any account 2FA codes you have. The code is based on the current time, passed against a hash value. If the software token app code matches that of the service you are using, access will be granted.

Hardware Token

Excellent choice, this is a physical device that you buy, usually a small device the size of a USB stick, that is required to be present in order to gain access to your accounts. Yubikey is my preferred hardware token, make sure to always buy at least two of them so that you hae a backup. Often, services will allow for a recovery seed phrase to be used in the event you lose your hardware token, but not always.

Two Factor Authentication (2FA)

Software Token apps:

Aegis (Android only)

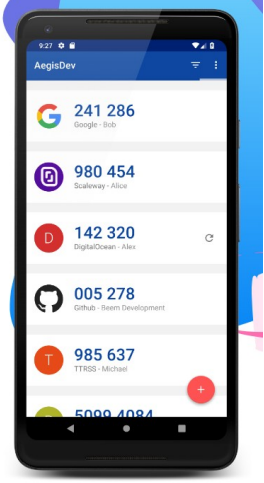
Ente Auth

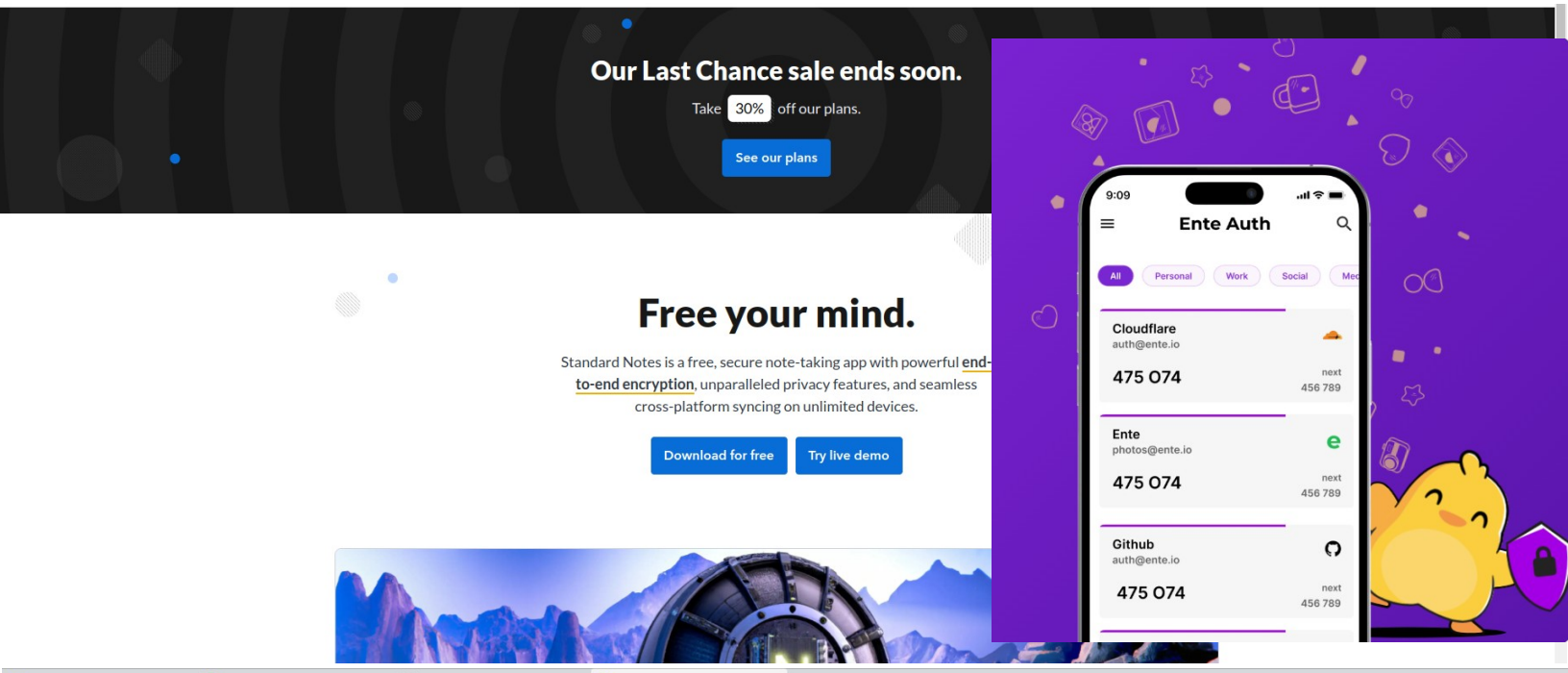
Standard Notes app (paid feature)

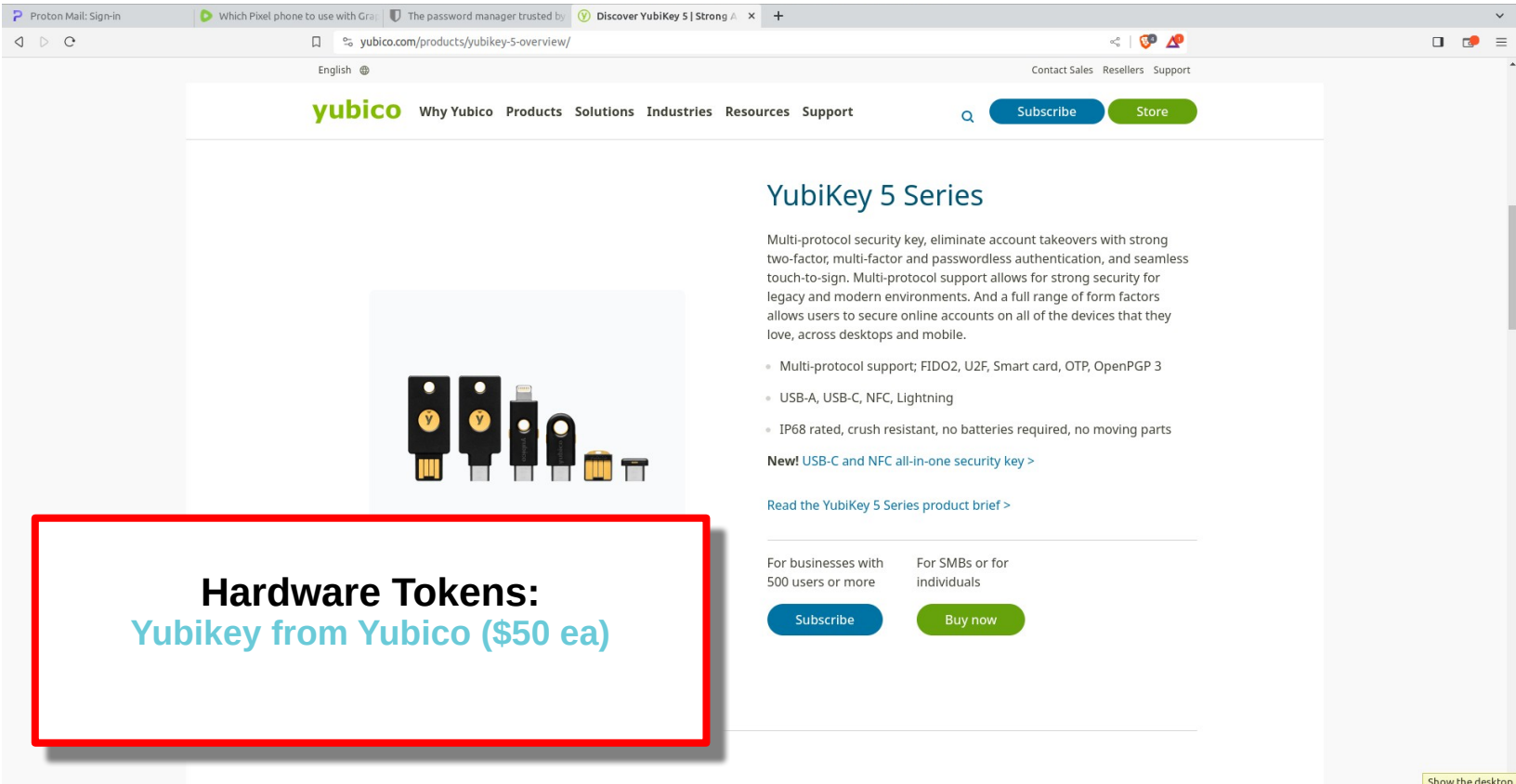
Aegis Authenticator

Aegis Authenticator is a free, secure and open source app for Android to manage your 2-step verification tokens for your online services.

GET IT ON Google Play | GET IT ON F-Droid







Hardware Tokens:

Yubikey from Yubico ($50 ea)

Password Manager &
Two Factor Authentication (2FA)

To Do List:

1. Create a Password Manager database using one of the following:

- ☐ Bitwarden
- ☐ KeePassXC
- ☐ Proton Pass

2. Use 2FA, any number of these applications:

- ☐ Standard Notes (only on paid tiers)
- ☐ Aegis
- ☐ Ente Auth

- ☐ Purchase at least two Yubikey hardware tokens

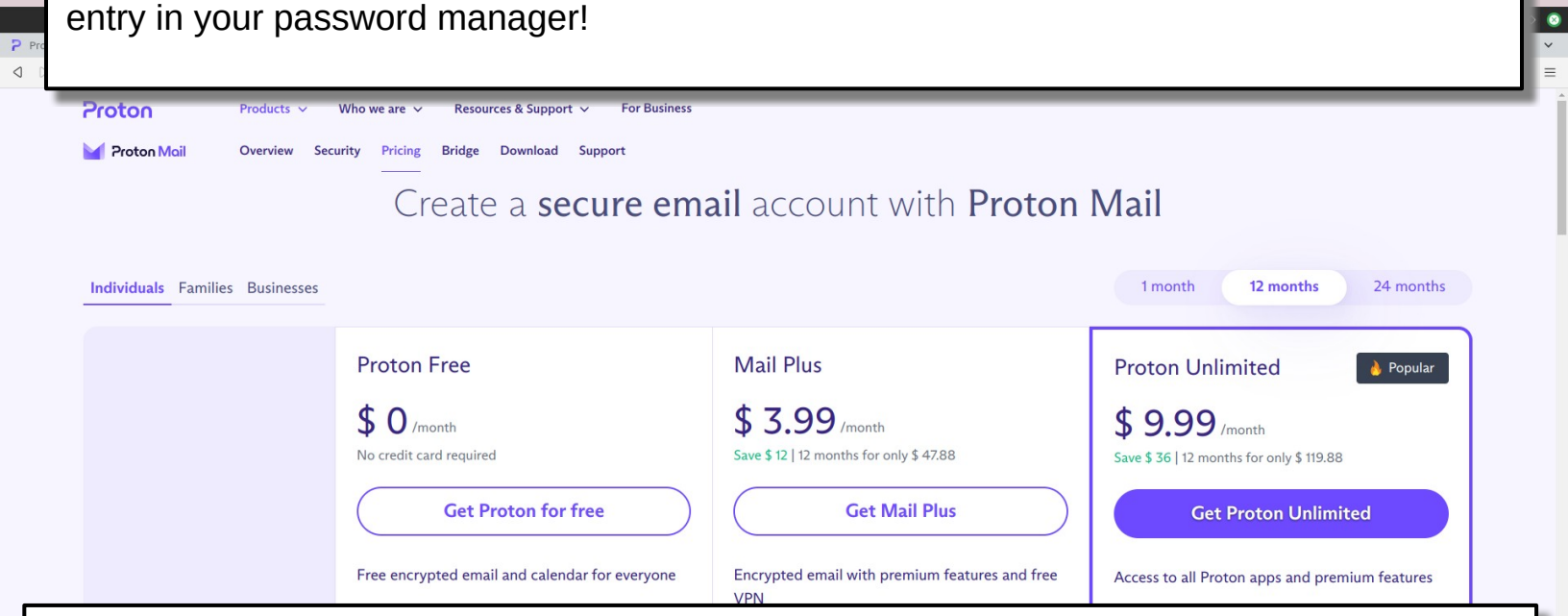
Get a Proton Mail account

If you're using a big tech email such as Google Gmail, Yahoo Mail, Outlook, etc then several things are happening. One, all of your incoming and outgoing emails, even your draft folder messages, are being recorded, along with any attachments, and the sender/recipients email address. Second, those companies are recording the metadata as well, your IP address, operating system, browser type/version, date/time stamp, physical location and much more.

We've been effectively trained to not think or care about this extremely invasive privacy obliteration, let's undo that and start migrating towards a better option. Even if you plan to keep your current email service, it's good to have an option in your back pocket.

Email is a service we really should be paying for, after all, it costs a lot of money to run email servers. The hardware, the data, brick and mortar location, staff, security teams, etc. Why are Gmail and Yahoo free? Because they are making a ton of money off of your 'boring' data. If your data was truly boring and useless, how is it that these companies are making a ton of money from it? Data has value, and is the new coin of the realm.

Navigate in your browser to https://proton.me/mail and click Create free account in upper right corner. Pick a plan that suits you, I recommend just starting with a free account, and then wait for a sale, they happen fairly often. Now add your login information in a new entry in your password manager!



In addition to an email account, Proton also gives you these other services:

VPN (Virtual Private Network)
Calendar (up to 3 on the free tier)
Drive (cloud storage space up to 1GB)
Proton Pass password manager

3. To Do List:
   ☐ Proton Mail account

Proton Mail is completely end to end encrypted (E2EE) with zero knowledge, meaning your email body and attachments are all completley encrypted, and even Proton cannot decrypt them, only sender/recipient. This only applies to emails sent between Proton accounts.

Get an alias email service

Now that we have a Proton Mail account up and running, let's take email a step further, by using an alias email service. While Proton provides you with up to 10 alias emails on the free tier, go ahead and set up an account with one or more of the following services:

SimpleLogin (owned by Proton, paid Proton accounts get a premium SimpleLogin account)

33mail

AnonAddy

All three of the above alias email services provide tons of free alias email addresses, we want to be using these instead of our true email whenever possible. This affords us a big layer of protection, by letting these alias addresses serve as a proxy to our true identity.

Each of these services, you point it at an inbox that you choose, such as your new Proton Email account, that way anytime someone sends you an email to the alias email address, it lands in your Proton Mail inbox (or wherever you set it to go). When you hit Reply, these services mask your true email and replies as the alias instead, so your identity can remain anonymous if you wish.

To use 33mail for example, once set up, you can simply create unlimited alias email addresses on the fly. All you have to do is remember one string of syntax, simply add anything you want in front of the @ symbol, and it will arrive in your Proton Email.

anything@yourcustomalias.33mail.com

Where 'anything' can literally be anything you choose, and 'yourcustomalias' is the unique, first come first serve address/domain you choose when you sign up. Example, you get your vehicle serviced at Honda, instead of giving your real email, try using your alias email:

honda3dec2023@yourcustomalias.anonaddy.com

Pretty easy, right? And it's completely free to do. If Honda decides to sell your email address to marketers, you'll know exactly who dunnit. If you wish to stop receiving email to that address, simply login to the service and disable it, poof. Be sure to document logins using your password manager.

4. To Do List (pick one or more):

☐ SimpleLogin (Proton)

☐ 33mail

☐ AnonAddy

Get Privacy.com Virtual Cards

Get Privacy.com

Privacy.com is an anonymous payment option that is free to use, or enjoy more features and higher limits by doing a paid tier at $10/mo. The paid tier can easily be free also since you receive 1% cash back on all of your spending.

This service allows us to spin up a new, virtual credit card in just a few clicks. This eliminates the possibility of someone intercepting your true debit or credit card information. Privacy.com allows you to place a limit per card on how many times it can be charged per month, per year, as well as dollar limits, or simply make it a one time use.

Note that each card can only be used with a single merchant.

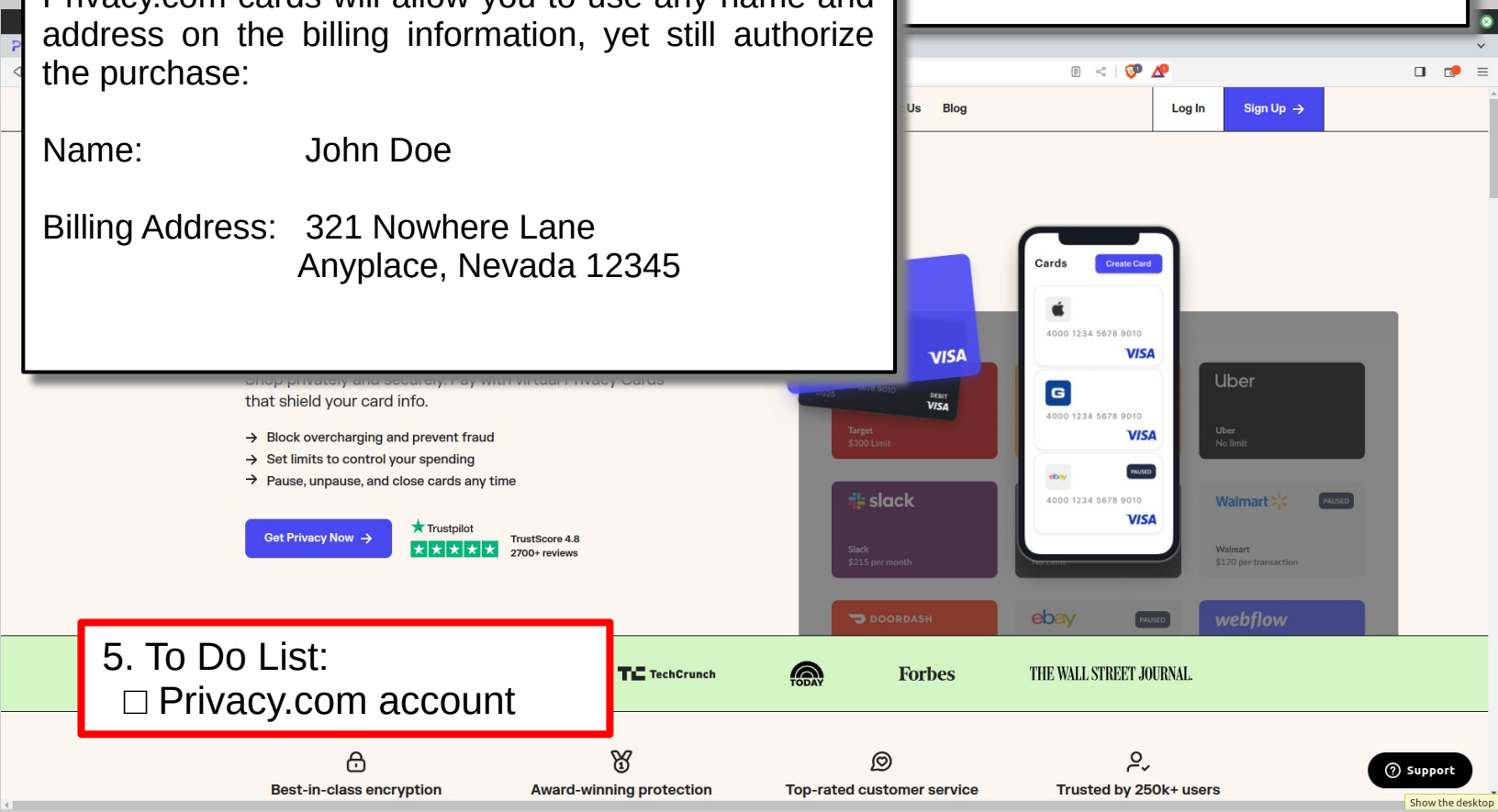
The merchant cannot see your true name, billing address or card information, allowing for anonymous purchases. Know that in the US with the Know Your Customer laws, you are not anonymous to court orders, just the merchant you shop with. On paid accounts, not only is the merchant unable to see your true identity, the bank cannot see the merchant. Privacy.com acts as a proxy, or middle man using the Plaid service.

To get your free account, simply go to Privacy.com and sign up. You will need your banking information, but once you link it to your bank, you are all set from then forward, super easy to use and maintain. Make sure to document login information in your password vault and add 2FA.

When checking out during an online purchase, Privacy.com cards will allow you to use any name and address on the billing information, yet still authorize the purchase:

Name: John Doe

Billing Address: 321 Nowhere Lane
Anyplace, Nevada 12345



5. To Do List:
☐ Privacy.com account

Extra Cloud Storage

We already have our Proton account up and running with 1GB of free storage, but we want more than that. We have several options, we could pay for a premium account to get up to 3TB of storage with Proton, or we could add on another service. Or you could eventually do both of course, but let's stick with the theme of 'free.'

One advantage we gain when adding extra cloud services is that we can compartmentalize our online accounts, which could be useful to us to gain a little privacy or security.

Mega offers a whopping 20GB for free and is completely encrypted. Be sure to document your credentials in your password manager and enable 2FA on the cloud account.

6. To Do List: (pick one or more)

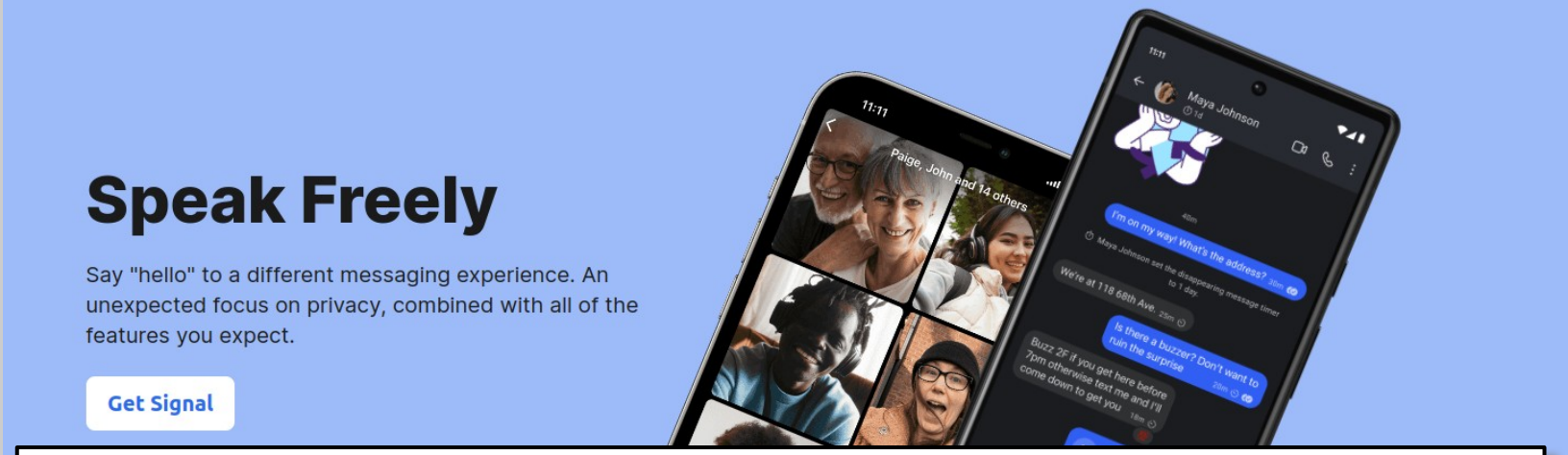
- ☐ Tresorit: (5GB free trial) https://tresorit.com/
- ☐ Proton Drive: (10GB free) https://proton.me/drive
- ☐ Mega.io: (20GB free) https://mega.io/
- ☐ Icedrive: (10GB free) https://icedrive.net/
- ☐ Internxt: (10GB free) https://internxt.com/
- ☐ Zoho: (10GB free) https://www.zoho.com/

My top choices are Proton Drive and Tresorit, but those plus Mega, Icedrive and Internxt are far from the only options, I just select these based on their encryption and ease of use, as well as a generous amount of storage on their free tiers. Zoho is not as handy on the free tier, and they are much, much more than just a cloud service, they offer one of the most robust alternatives to many of the business CRM products out there. All of these have free tiers available, but you may need paid tiers to meet your needs.

Other options you'll want to explore are self hosted clouds like Nextcloud, Etesync, TrueNAS, Owncloud, FileBrowser, Personal Drive are all great options as well if you have a little skill setting up your own hardware. Docker installs are generally easiest.

Still, there are many other cloud services that don't require us to tangle with Microsoft, Amazon, Apple or Google. Kick them to the curb and explore one of these better ways. Ensure the cloud you pick offers true 'zero knowledge encryption'.

Signal messenger and Video chat apps



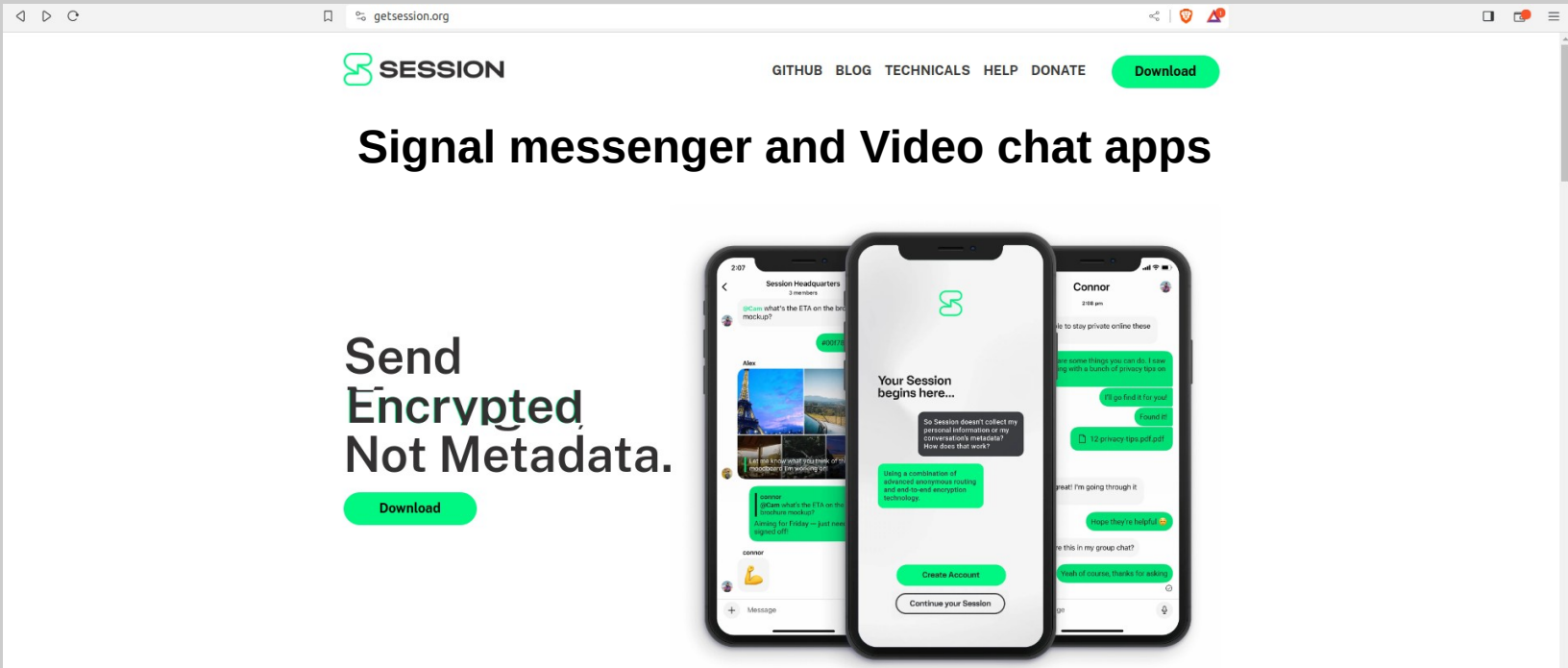
Did you know that every single text message and voice call you make or receive is intercepted and recorded forever by both the telecoms company as well as the US Government?

While you may not feel you have anything to hide, you have everything to protect. Why allow yourself to be completely monitored when we have options for encrypted messengers. Imagine what can be inferred about you after decades of data collection, not only the message contents, but the even more valuable metadata (date/time stamp, location, etc.)

For text, voice and video chat, Signal is by far the easiest go to for most of us. It's had very wide adoption over the last five years, and allows for up to 40 people on voice and video calls, and up to 1000 people on group text chats. Signal is fully encrypted and it's also an open source app. Be sure to check out the others as well on the next page.

7. To Do List: (pick one or more)

☐ Signal	https://signal.org/
☐ Session	https://getsession.org/
☐ Jami (video chat)	https://jami.net/
☐ Mirotalk (video chat)	https://sfu.mirotalk.com/
☐ Telegram (not encrypted by default)	https://telegram.org/



While Signal is an excellent first choice to handle our message, voice and video chat needs, it's good to have backups.

Session is an excellent messenger backup, no information needed to sign up, completely anonymous, free, open source and encrypted

Jami is a video call app that can replace Zoom. Zoom collects horrendous amounts of data about us in addition to recording every session we participate in.

Mirotalk is another video messaging platform that can be used without giving any information about ourselves, without downloading any app, use in browser

Telegram is a hybrid of messenger and social media, not a great replacement for normal messaging. However it's great to quickly share large files for free, and one on one conversations can be encrypted if that setting is toggled on.

7. To Do List: (pick one or more)

- ☐ Signal https://signal.org/
- ☐ Session https://getsession.org/
- ☐ Jami (video chat) https://jami.net/
- ☐ Mirotalk (video chat) https://sfu.mirotalk.com/
- ☐ Telegram (not encrypted by default) https://telegram.org/

jami
a GNU package

Telegram
a new era of messaging

Standard Notes app

There are plenty of note taking apps out there, however I really enjoy Standard Notes for several reasons. (I get it, a note taking app is not all that exciting… but it's very powerful)

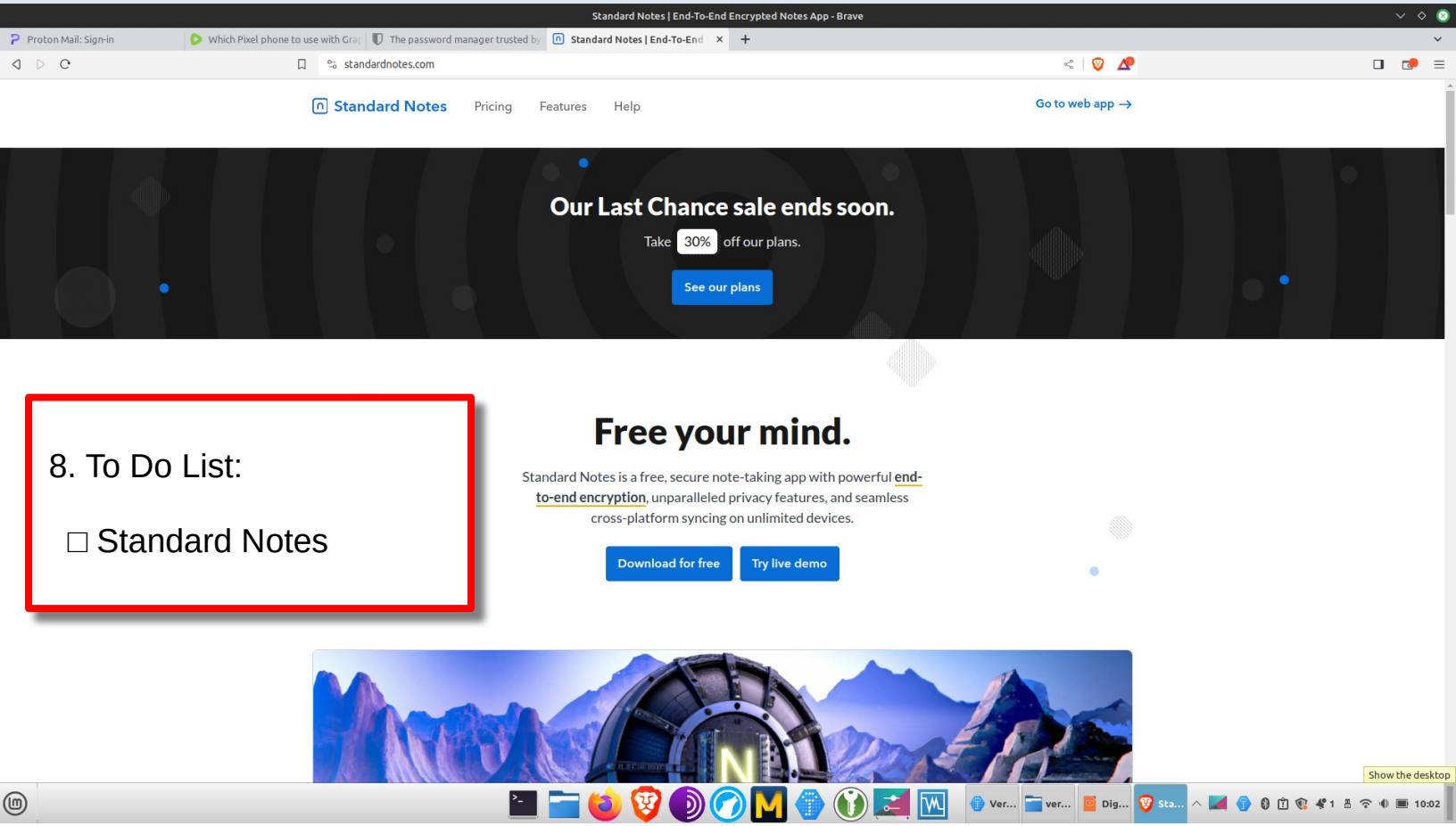
For one, it's fully end to end encrypted, and zero knowledge so only you can see your content. This is quite valuable for our privacy, but Standard Notes offers another feature in the paid tiers, it can handle our 2FA software tokens. Meaning we can use Standard Notes as our 2FA on any of our other accounts. They typically do half priced plans on Black Fridays, but even standard price is very fair for what you get.

Visit https://standardnotes.com/ and click download, then sign up using an alias email address. No need to give them any real identity, making this a very private and secure way to keep notes. This app works offline also, and syncs when connected again.

In the settings, even on the free tier, set the intervals (such as weekly or daily) for backups, Standard Notes will email an encrypted backup copy of your account for offline use if needed.

Standard Notes also syncs across all of your devices, making this an extremely handy app for getting work done, saving interesting links or any other note taking needs. Paid tiers allow for rich text and file storage up to 100GB, as well as other great features, but at least grab a free account for now, upgrade later if desired. (Standard Notes is now owned by Proton)

Get Standard Notes



8. To Do List:

☐ Standard Notes

Data Storage

Many of us have grown accustomed to having all of our data in the cloud. While this is generally fine, remember several things. A cloud is simply someone else's computer, we do not control it.
We also cannot see our stuff without internet, this is a major problem. Even large companies with good security such as Google and Apple still suffer data loss at times, don't trust a lifetime of family photos or anything else precious to a cloud. Download and manage local copies of your data.
Most of us put this off until it's too late and we suffer a major loss. Grab yourself some SSD drives and some extra USB drives to keep your data on, and have room to grow and add more as time goes on. You'll also want enough physical storage to create at a minimum one backup on site.

While any brand will do in a pinch, I prefer to stick with **SanDisk, Kingston** and **Samsung** for SSD drives, these have proven themselves reliable and worth the cost. Avoid the cheaper off brand stuff for best results. Before you begin backing up your data, read the section on Encryption next to see if you should encrypt your drives first before adding data.

MicroSD cards are yet another great thing to have extra of, these can be tucked away nearly anywhere to keep copies of important data at your fingertips.

See more about data storage options here: **https://grapheneGOAT.com/resources-and-links/data-storage/**

3-2-1 Data Backup Rule:

At least **THREE** copies of your data,
on **TWO** types of storage,
and **ONE** copy offsite

9. To Do List:

☐ Data Storage drives

Data Encryption

VeraCrypt

Data is critical in our lives these days, and just as important as the data itself, is who can access it. With encryption, we can tightly control who gets to see what data that we control.

The only real disadvantage to encryption is convenience. It takes an extra step to view our data when it's encrypted, let's discuss several tools I use and recommend.

If you've never used Linux before for your computer operating system, you'll want to read the third section in this guide. On Linux we can encrypt our entire hard drive of our computer using **LUKS**, all that's required to unlock it is to enter a passphrase upon boot up.

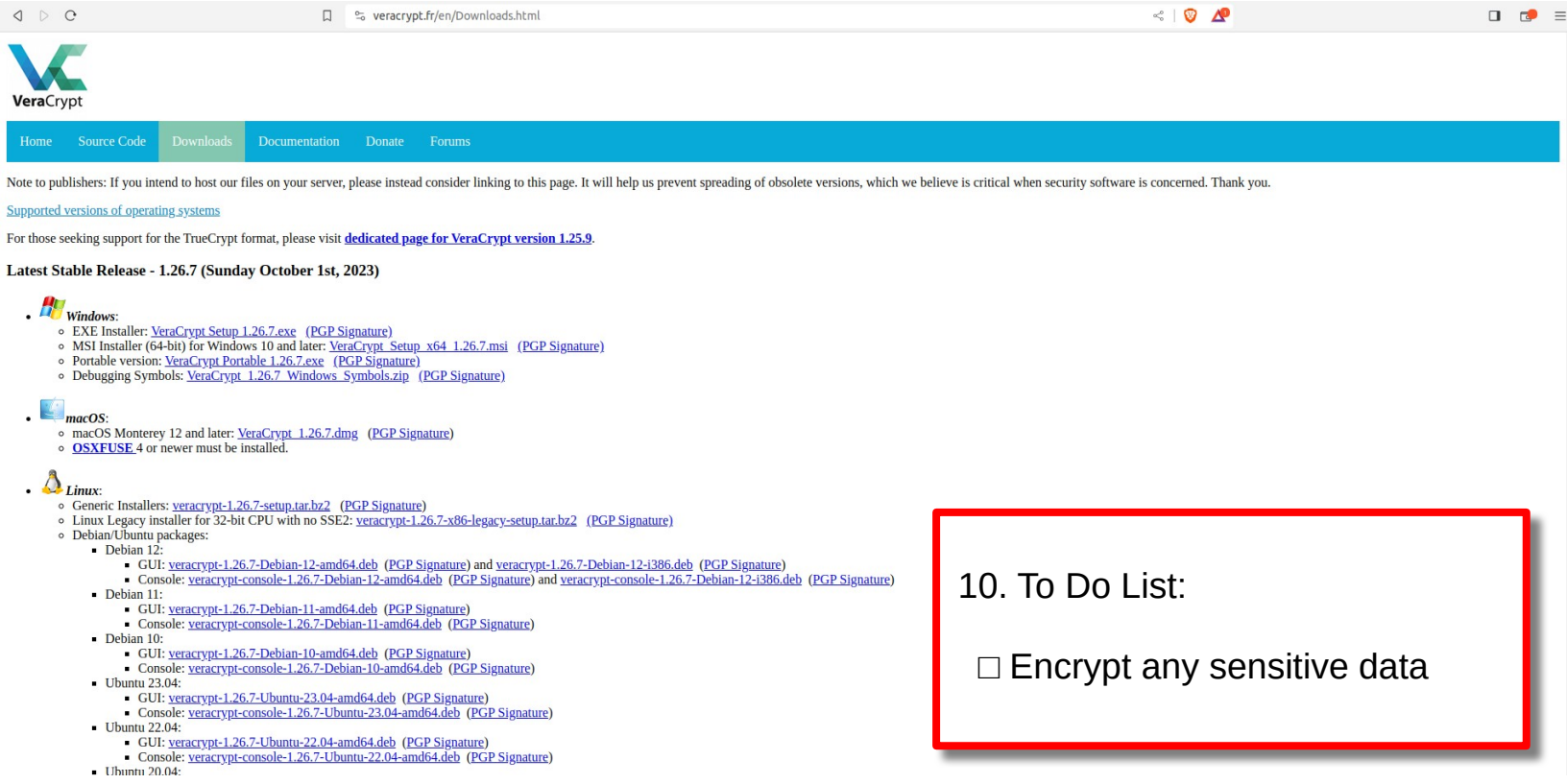
Read more about LUKS (Linux Unified Key Setup) here: **https://itsfoss.com/luks/**

For encrypting USB, SSD or microSD drives, or creating encrypted containers on any computer system, I highly recommend an application called VeraCrypt. This is free and open source software used to create encrypted containers, as well as for viewing encrypted containers. This works cross platform on Windows, macOS and Linux.

Download VeraCrypt here: https://www.veracrypt.fr/en/Downloads.html

For Android, you will require an app called EDS NG, from Aurora Store, this is software for viewing the encrypted containers on Android. This replaces EDS Lite.

Alternative: Cryptomator works on all platforms, and functions similar to VeraCrypt.

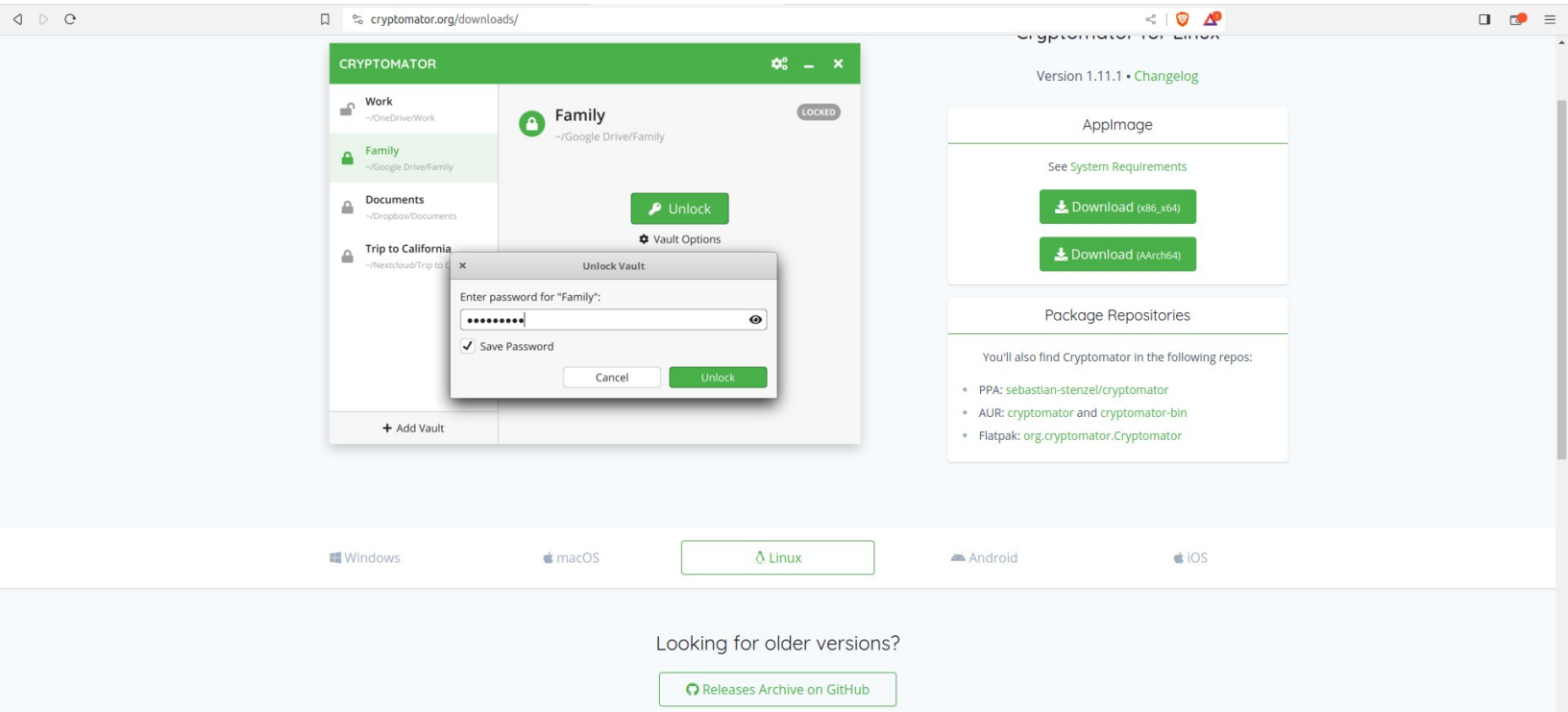


10. To Do List:

☐ Encrypt any sensitive data

Data Encryption

Cryptomator



If you do rely on a big tech cloud product such as Google Drive or similar, we can defeat their prying eyes by using an application called Cryptomator. (Yes, Google, Apple, Microsoft and others see every single item you transmit or store on their platforms)

Of course if you don't trust Proton or Mega or any other cloud service either, you can store an encrypted Cryptomator container on their cloud, even though it's already encrypted using their cloud platform. This just adds peace of mind for really sensitive items.

Some cloud storage solutions won't accept the VeraCrypt file format, but thankfully nearly all will accept encrypted containers from Cryptomator. It functions nearly identical to VeraCrypt, very easy to use and is also cross platform, including all desktops and mobile devices.

Download Cryptomator here: https://cryptomator.org/downloads/

Important!

VeraCrypt or Cryptomator do not encrypt existing files. You first create a blank container using the software, then mount the container much like you would a USB drive, and drag and drop files into the container, it appears and functions like any other folder. Once you close (unmount) this container, it is then encrypted at rest until you unlock it again using the respective VeraCrypt or Cryptomator software.

Backup your Contacts

Do you possess a copy of all of your email and cell contacts, say, on your hard drive or a USB stick? If not, you very well should. Don't trust your cell or email service to do so, exporting and keeping a copy for yourself is very easy.

While we're on the subject, now is a good time to remind you to also backup a copy of your email so that you have them even offline. Most of us rely on the IMAP protocol to check our email, which means there's no local copy, you have to connect to your email server in order to see any of your information.

Email and Email Contacts

In your email, you should see a feature in your Settings menu called Backup or Export. Use this feature to download a local copy of all of your contacts as well as your emails. This may take an hour or more depending on how many emails you have, and can take up several gigabytes or more of space.

Doing this ensures you'll have access to every single email, even with no internet connection. This could prove useful for many things, including legal action.

Cell Phone Contacts

Apple makes this slightly difficult, to save a backup of your contacts, you have to login to your iCloud account and export them from there to a local file.
On Google Android, open the Contacts app, open Settings and Export as local .vcf file.

Each should result in a .vcf file, usually just called 'contacts.vcf'
Save a local copy of this file, it contains every one of your contacts saved in the phone.

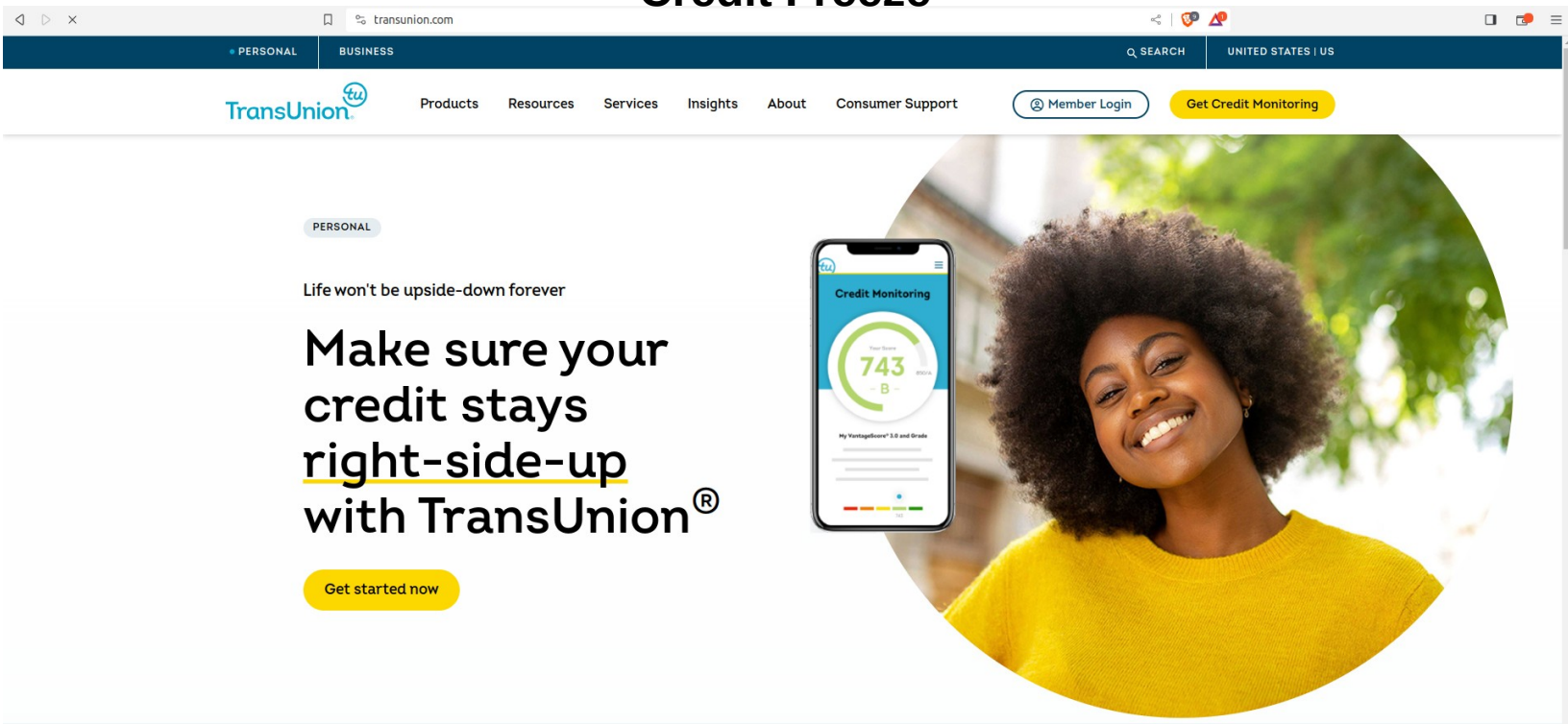
When you get a new device, simply put a copy onto the phone and the Contacts app will quickly install them all to your new device, good to go. Very easy, and something many of us don't do, until it bites us in the rear and we lose some or all of our contacts.

Just like with any other of our data, we should take full control of a copy, never assume that any other service, no matter how reliable, will manage that data for us properly.

11. To Do List:

- ☐ Backup your email
- ☐ Backup your cell contacts

Credit Freeze



Watch a short video on how to quickly freeze your credit and emplace a security freeze or fraud alert on all three major credit union sites:

https://rumble.com/v3q0bj3-freeze-your-credit-in-under-10-minutes.html

If you don't have an account with all three credit bureaus, do so before someone else does! This can be easily done in less than 10 minutes of your time, be sure to document your username and password, and PIN if issued, in your password manager.

Visit here to find links to all three major credit bureaus:

https://graphenegoat.com/resources-and-links/credit-freeze/

12. To Do List:

☐ TransUnion account, Freeze, and set Fraud Alert

☐ Equifax account, Freeze, and set Fraud Alert

☐ Experian account, Freeze, and set Fraud Alert

Section 1 is done!

If you've managed to do most if not all of this section's tasks, congratulations, you have come a long way already on a much safer and more secure digital life. You've gained quite a bit of privacy, and have learned to think like a privacy minded individual going forward.

Don't hoard your knowledge, be sure to share this with others. If you come up with better solutions, or find any errors in these strategies, please let us know in an email to:

privacyguide@graphenegoat.com

Your journey is far from over though, many more steps await you. The next page has a full checklist of all items discussed in this section.

Enjoy, stay safe out there, and stay free.

Section 1 CHECKLIST

1. Create a Password Manager database:

☐ Bitwarden
☐ KeePassXC
☐ Proton Pass

2. Use 2FA, any number of these applications:

☐ Standard Notes (only on paid tiers)
☐ Aegis
☐ Ente Auth

☐ Purchase at least two Yubikey hardware tokens

3. Get Proton Mail:

☐ Proton Mail account

4. Alias Email Service (pick one or more):

☐ SimpleLogin

☐ 33mail

☐ AnonAddy

5. Virtual Credit Cards
:

☐ Privacy.com account

6. Cloud Storage: (pick one or more)

☐ Tresorit: (5GB free trial) https://tresorit.com/

☐ Proton Drive: (10GB free) https://proton.me/drive

☐ Mega.io: (20GB free) https://mega.io/

☐ Icedrive: (10GB free) https://icedrive.net/

☐ Internxt: (10GB free) https://internxt.com/

☐ Zoho: (10GB free) https://www.zoho.com/

7. Video Chat: (pick one or more)

☐ Signal https://signal.org/

☐ Session https://getsession.org/

☐ Jami (video chat) https://jami.net/

☐ Mirotalk (video chat) https://sfu.mirotalk.com/

☐ Telegram (not encrypted by default)
https://telegram.org/

8. Note Taking app / 2FA:

☐ Standard Notes

9. Purchase Drive Storage:

☐ Data Storage drives

10. Download and use Encrypted Containers:

☐ Encrypt any sensitive data

11. To Do List:

☐ Backup your email

☐ Backup your cell contacts

12. Credit Freeze / Fraud Alerts:

☐ TransUnion account, Freeze, and set Fraud Alert

☐ Equifax account, Freeze, and set Fraud Alert

☐ Experian account, Freeze, and set Fraud Alert

Check out the Rumble channel for some additional learning and guides:

https://rumble.com/user/GrapheneGoat

Section 2:
We need to fix your operating system part 1: GrapheneOS

You need a better mobile device

Before you groan when you hear it's time for a new type of phone, know that this process is not near as difficult as you might imagine. Call it fear of the unknown perhaps, but after interacting with a GrapheneOS Android phone, you'll get comfortable with it in short order. I think most of you will wonder why all phones don't behave and operate the way GrapheneOS does, it's simply an Android phone.

This phone is developed with privacy and security in mind as the top priority, but when we look at how it works, it's my firm belief that all phones should function this way. A phone where the user actually controls the operating system, rather than Apple or Google.

Android is free and open source software (FOSS) built around the Linux kernel. Anyone can use and modify this code to create their own unique operating system, or ROM (read only memory), GrapheneOS keeps the source code completely open. Compare this to a Google Android, or an iOS Apple phone where the source code is completely locked, so we have no idea what it is doing, or programmed to do. Google and Apple retain full control of the device.

This allows them to turn on any of your sensors such as camera, mic, WiFi, bluetooth, and can even install software on the device, or toggle on or off any setting that they wish without your knowledge. That is a pretty abusive and garbage way of doing things.

Remember, whoever controls the operating system, controls the device. With iOS or Google Android, the one in control isn't you. With GrapheneOS, you are in full control of the device, as the operating system is completely transparent, and only does what you tell it to do.

When you shut off the WiFi, microphone or location, they are actually off off. On regular 'normie' phones, turning off these sensors does nothing to Google or Apple's ability to turn them on any time they wish behind our backs.

While I could go on for quite a while with phone selection, install instructions and initial setup, in the spirit of this being a 'quick start guide' I'll simply cover the very top level steps. To learn more, I highly encourage you to attend one of our DHAC courses (Digital Hygiene and Awareness Course) in person. This training walks you through the entire process as well as a plethora of additional information, and you receive ongoing access to other content in the future. We travel as well, if you have the space to host, we can come to you. We also have an online Video on Demand version available for instant purchase.

Visit the DHAC course page to purchase your own copy or to sign up for a course:

https://graphenegoat.com/courses/

You need a better mobile device

GrapheneOS can only be installed (ironically) on a Google Pixel phone, and not just any Pixel. You must have a fully unlocked OEM edition with the OEM unlock setting enabled. Even if you wish to flash a device yourself, we can help you source the correct model Pixel.

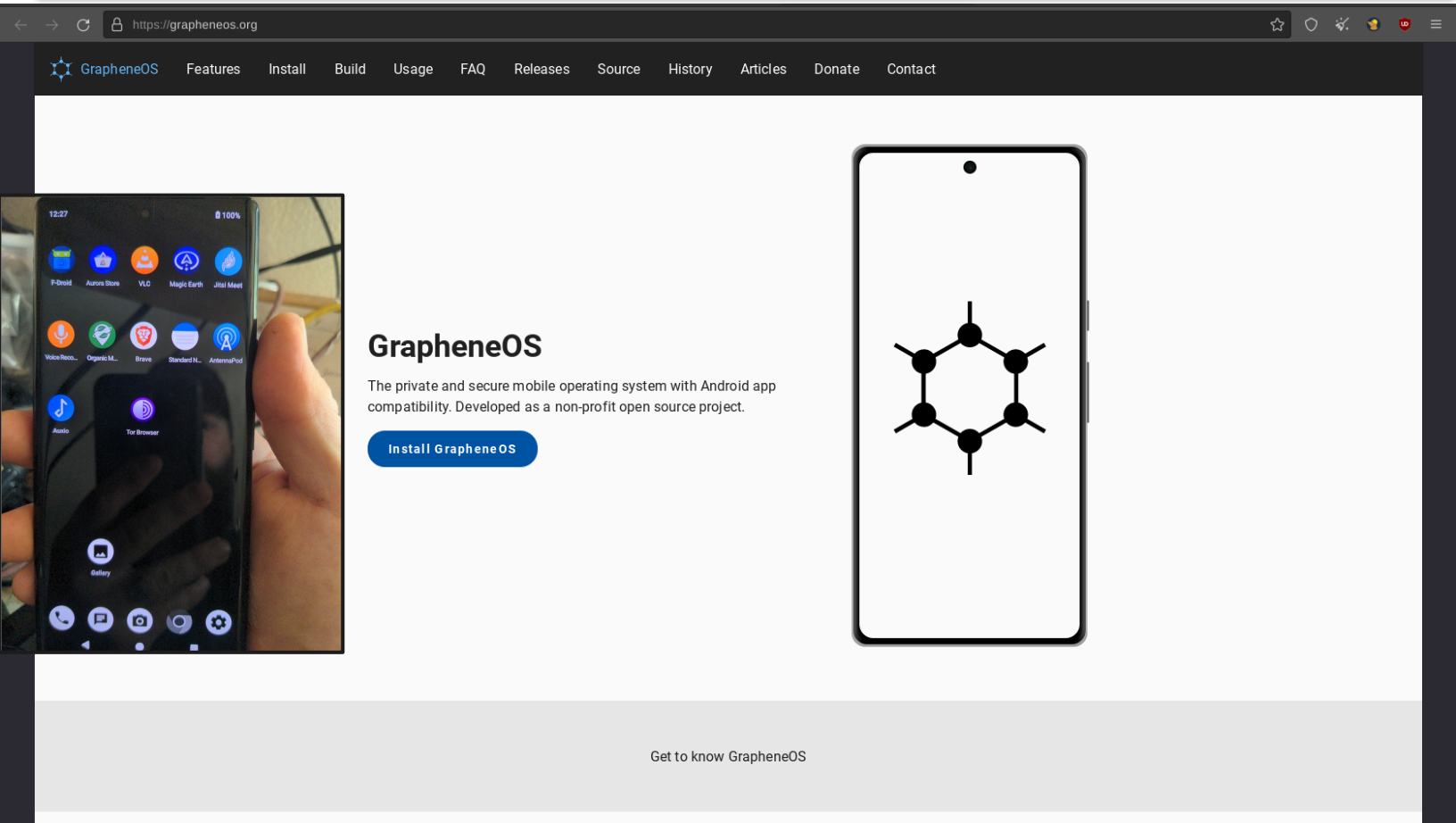
You can also purchase a device from us, we simply charge $50 over the device cost to cover the installation process and system checks, as well as installing some basic apps.

While GrapheneOS stock environment has only very bare bones applications installed (camera, text, voice call, contacts, etc) it has little else, which is very good. Only install what you need, unlike normie phones that have tons of ‘bloatware’ that cannot be easily removed or disabled. While GrapheneOS comes minimalist out of the box, it is a very fully capable smartphone that rivals anything else out there. You can install or use any app you wish.

Because there is no bloatware or big tech grabbing tons of telemetry, you’ll notice a very big improvement in battery life, as well as data usage. This is a lean, mean mobile machine with very robust security defaults, yet remains just as user friendly as any other Android device.

To DIY flash your own Pixel phone with GrapheneOS, or to learn more about the system, head on over to their site and check out the installation process and FAQ’s:

https://grapheneos.org/



GrapheneOS installation wipes clean all of the Google on the device, these are frequently referred to as ‘de-Googled’ phones. If you purchase a device from us, we buy clean, mint condition phones from a reputable supplier and run it through our checks, and complete installation, along with any apps you need.

Post installation we install several app stores for you along with some other basic applications, most of which are free and open source. If you attend our DHAC course, we cover step by step how to do all of this yourself, and explain much more about the device.

Common Questions

Let’s cover some of the more common things we get asked when discussing GrapheneOS:

Can I use my current SIM or eSIM on these phones?

Yes, all SIM cards will work seamlessly, just drop it in and go

How do I get my contacts copied onto the new device?

Apple requires you to login to your iCloud account for easy export
Google Android- simply open Contacts app, Settings and click Export
Each of these should result in a .vcf file, usually named ‘contacts.vcf’ – copy this file onto the new device and it will auto-detect, click Yes to upload to the Contacts app

Can I install GrapheneOS on a different phone?

No, only certain model Pixels that are fully unlocked are supported (OEM edition phones)

Am I ‘going dark’ or ‘becoming invisible’ with this device?

Not really, especially if using your current SIM, which is linked to your true identity most likely. However this does shut down about 98% of the tracking and telemetry over a normal phone. Note that the carrier can still see your location. While this may sound discouraging in a way, do know that this is no small step in privacy and security. This is an extremely meaningful step to a better way of using a mobile device.

Learn more about GrapheneOS mobile devices on our page here:

https://graphenegoat.com/grapheneos-phones/

Section 3:
We need to fix your operating system part 2: Linux

Most of you reading this are probably using Microsoft Windows if on a desktop. I'd like to encourage you to either switch to Linux, or to at least add it to your life.

Much like the previous section about making the switch to a new mobile device, this section briefly covers a similar way of exploring a better way to handle our computing tasks. Many years ago, Linux could be considered quite difficult to those that are not all that tech savvy, however in today's world, Linux has gotten extremely user friendly. So much so, I'd argue it's no harder than switching from Windows 7 to Windows 10 just to pick a random example.

What is Linux?

Linux is colloquially used to describe the Linux kernel by Linus Torvalds (1991) along with the GNU General Public License libraries by Richard Stallman (1983.) Together these create what we refer to as the operating system Linux. (Unix like system) But, there are many types of Linux to choose from, referred to as 'distros' short for distributions. Let's take a look at some of the more popular choices for beginners to start with:

Ubuntu

Linux Mint

Pop!_OS

Zorin

Manjaro

Those are only several of probably a thousand others, but starting there with any of those will be quite easy for nearly anyone. In addition to these five operating systems listed, we can choose different Desktop Environments as well, to create the exact user experience we want out of our system. In most cases, this is also free, no licensing or fees.
Linux is highly customizable, and extremely stable, not to mention fast and lean. It's also the easiest of the three operating systems (Windows, MacOS and Linux) to try and/or install on nearly any computer. Dust off that old laptop or desktop and give it new life with Linux!

To get an idea of just how many types of Linux Operating Systems there are in use today, check out this site: **https://distrowatch.com/**

Learn more about these beginner distros on our page here:

https://graphenegoat.com/linux-operating-systems/linux-distributions/

If it’s any encouragement, nearly everyone who has taken our DHAC course has commented that installing and using Linux was much easier than they had imagined. In the training we walk you through installation and use from start to finish, and send you off with plenty of resources for support and further learning.

However, with the information we have on the site at GrapheneGoat.com, I think many folks will be able to figure out the installation on their own, which I encourage you to try.

Just like with our mobile devices, whoever controls the operating system controls the device. With Microsoft Windows or Apple products, they control the OS. This means that these companies see every single click, connection and anything else that we do. All of your documents, pictures and other files are captured, as well as all of your unique behavior. This data is packaged and sold many times over to endless numbers of companies. To me, that is a massive invasion of privacy, there is no need to tolerate such behavior when we have free and open source software such as Linux. (Again, did I mention, it’s also free?)

In the final section of this guide, you will see a collection of some of the better resources that I have found to help anyone along on their free and open source software journey. Even if you only use it part time, it’s well worth the time investment to understand exactly what you are missing out on. For those able to take it a step further, you’ll find that there is a nearly endless playground to explore in this hidden in plain site ecosystem. Computers should work for us, not the other way around. Free yourself from abusive big tech platforms.

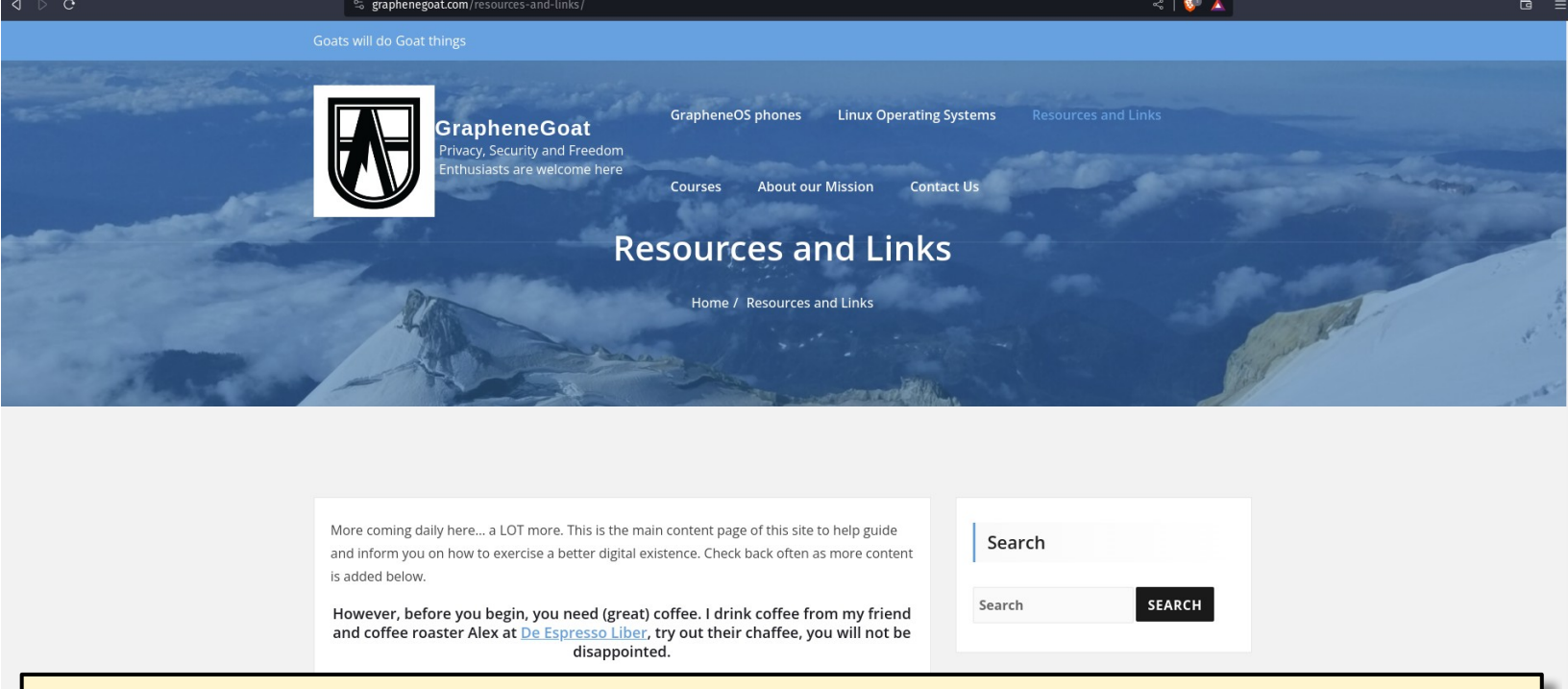
Section 4:
Continue your Journey

To finish out this guide, here I provide some entry points into a new way of using technology. A new way that works for freedom loving people, to shift the tech paradigm from closed source spyware, to open source freedom.

If we had a friend or a spouse that treated us the way that Microsoft, Google, Apple and many others treat us, we would call that an abusive and toxic relationship. They hide, lie and steal behind our backs, while abusing our trust to enrich themselves for further control and leverage over us. These Silicon Valley types have lost our trust forever, let's continue to take meaningful steps towards freedom and transparency. Sunlight is always the best disinfectant, free and open source software achieves this and provides alternative tools.

"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. They may be more likely to go to Heaven yet at the same time likelier to make a Hell of earth. This very kindness stings with intolerable insult. To be "cured" against one's will and cured of states which we may not regard as disease is to be put on a level of those who have not yet reached the age of reason or those who never will; to be classed with infants, imbeciles, and domestic animals."

— C.S. Lewis, God in the Dock: Essays on Theology (Making of Modern Theology)



Visit our main site and explore, be sure to visit the Resources and Links tab:

https://graphenegoat.com/

In the bottom section of the Resources and Links tab on GrapheneGoat.com, you'll see various sections, the top 3-5 links in each section are what I would focus on first to get started, those resources are excellent power hitters in this arena. Folks like Mike Bazzell, LearnLinux.TV, Naomi Brockwell, Rob Braxman and others are excellent entry points.

Some local Telegram channels that help support you day by day are these two here, download Telegram FOSS version from F-Droid here and then use it to join us over at Bones Tech Garage and Jeff.Pro, both very friendly channels where we help you learn Linux and make you aware of any other relevant technology news.

Bones Tech Garage: https://t.me/s/BonesTechGarage

Jeffrey_Peterson: https://t.me/jeffrey_peterson/5651

Mark37.com: https://mark37.com/

Start with the resources on those pages and within Telegram, and you will find a lot of easy and quick tech support to help you make the migration from big tech spyware to free and open source software. It's quite liberating, especially once you begin to understand why we are taking these steps. Learning tech can easily happen by just a little bit of curiosity day by day to learn a little each day. There is no 'plunge' to take, just wade in the waters to start taking back control of your data. Without our data, these large omnipotent companies have less and less power and control over us, and we become truly free.

Stay safe out there, and stay free. -GrapheneGoat