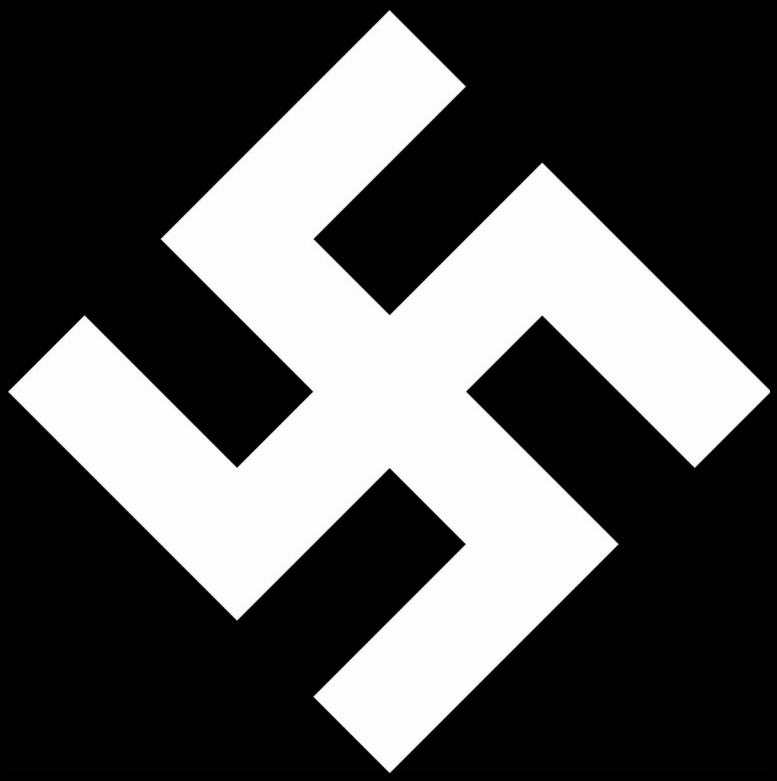
Kundalini-Project's Book On Cybersecurity



"Without Knowledge, Power Is Lost, As Power Is Lost, So Is Understanding Lost And So Is True Knowledge Lost." ~ BrightSpace666

Introduction

This book contains writings of mine that I have also published on forums, and some of them are available on my website. The purpose of the book is to highlight to readers the extent of jewish influence on the internet and to analyze the so-called 'secure' services/software more deeply in order to uncover the truth.

The main essence is to raise awareness among people in the online space; everything we do leaves a trace on the internet. This book will be monumentally helpful to you and will gift you with critical thinking.

This book is the first part of a larger work.

Be safe,

Sieg Heil!

BrightSpace666

https://joyofsatan.org

https://ancient-forums.com

https://kundalini-project.neocities.org

https://brightspace666.neocities.org

Content

Introduction……...2
Anonymity & Security Advice……..4
Secure Extensions In Browsers…….15
Monumental Security Reviews…….20
On Encryption……...66
Let Us Be Clear About A Few Things [Avoiding Misunderstandings]……70
Contact……75

Anonymity & Security Advice

Anonymity

Unfortunately, effective anonymity on the internet is not easy to achieve. Websites are monumentally full of negative js, ads that can all fingerprint you and identify you.

With the **uMatrix** add-on you can control what happens in your browser - putting the power in your hands. However, many people are not familiar with **uMatrix** and add-ons like xiMatrix, **AdNauseam** and so on - this needs to change.

Basically, your anonymity starts with what operating system you use. Jewish windows is a monumentally large "spyware" and collects and sends a lot of data about you to a number of IP addresses. Telemetry is also discouraging and a cause for concern.

Linux distros also have their drawbacks unfortunately, and that is **systemd**. If you want real security, ignore distros with **systemd**. This can be difficult, as **systemd** offers simplicity, but in return it takes away much of your security.

Slackware Linux is the most suitable distro for me, and it was my "Magnum Opus" in the **Linux** world. Before that I used Kali **Linux**, Parrot OS and other distros that included **systemd**. **Devuan** is still a decent distro to this day, and not that complicated.

Slackware, on the other hand, requires knowledge and experience in the Unix world and is not for those who are just getting acquainted with **Linux**. However, everything can be learned and mastered. The purpose of this post is to achieve security and anonymity.

Note, however, that what I say does not necessarily have to be accompanied by a source. Everything I say is true, but if you want to be sure, you have to check it

out. I have no desire to spend time looking for sources. If you want to, find it yourself.

Linux

As I mentioned, a **Slackware Linux** [or **Slackware** based **Linux**] is perfect. However, if you're not familiar with the **Linux** world, I'd wait on **Slackware** if I were you. To start with you can choose a **Devuan**, which is completely **Debian**, just without **systemd**.

Browsers

Well, this is probably one of the most shared topics. Browsers like **Firefox**, Chrome, Edge, Opera all tout "security" - but they all call home, collect and store data, share that data, and are actually spyware of monumental proportions.

LibreWolf or **Tor Browser** are considered mild spyware, but both are based on a version of **Firefox** - we can't be too careful. The **Tor Browser** is a browser that simply connects to the **Tor** network, which you can do in **LibreWolf** by configuring the ports properly.

However, they are still more decent than the first one. **Ungoogled Chromium** and **IceCat** are not spyware, they support add-ons, but **Ungoogled Chromium** depends on the monumentally large, Jewish google, so we can't be too lenient here either.

In any case, **Ungoogled Chromium** is a decent choice for safety. I'd recommend an earlier version of **Ungoogled Chromium** [you don't necessarily need the latest version of everything].

Pale Moon is a browser based on an older version of **Firefox**, and is probably the most unique on the list. While Moonchild has tried to screw up their browser, as if this is some sort of mission, it is not beyond repair.

Pale Moon is initially a "mild spyware" that makes requests to Google, but these can be turned off. In fact, you can choose between **Pale Moon**, **Ungoogled Chromium**, **IceCat** and **Tor Browser** for security. **IceCat** and **Ungoogled Chromium** do not make requests to anyone, so they are not spyware.

The **WebBrowser** by **Nuegia [Tom]** is a **Pale Moon** fork, not spyware, but the guy doesn't seem to keep it fresh - it's a damn good browser anyway.

In my opinion, an **Ungoogled Chromium**/**Pale Moon** is a good choice for everyday browsing, **Tor Browser** is a good choice for the **Deep/Dark Web**, and

LibreWolf is a good choice for **I2P**. Note, however, that you'll have to fight for security - there are a lot of things to change and add to a browser to get it right.

Unfortunately that's just the way it is, you have to do everything. You cannot make something from nothing.

VPN

Many VPNs are under the "secure, encrypted, zero logging policy". Most of these are lies and are after your data. VPNs like **NordVPN** should be avoided by far in terms of security. **ProtonVPN** also collects data and I wouldn't say it's completely secure.

RiseupVPN is a decent choice, with encrypted and secure servers, as is **Mullvad**VPN. **Riseup** is ingenious, with **Mullvad** you have to dig into your wallet. There is an OpenVPN genera**tor** script [also used by Kundalini-Router] for **RiseupVPN**, which is an even more decent choice. Check out the Kundalini-Router & **Kundalini-Tool** in the "Programs" section, you're sure to like it.

Add-ons

I won't give a detailed description because the point of my posts of this kind is not to explain but to focus on the point - the explanation, analysis and interpretation has already been done by others [links at the bottom of the post].

Without **uMatrix/xiMatrix**, don't really go online. They show you how many requests one page makes to another, how many items are categorized, and you can decide what you want to allow and what you don't.

uMatrix also blocks malware, third parties and more - perfect for ad blocking. **uMatrix** is perfect as it is. Add-ons like **AdNauseam, Decentraleyes/LocalCDN, ClearURLs** are also relevant.

Make sure **WebRTC** is turned off in your browser. In **Firefox** based browsers, you can change this in the "*about:config*" menu or with add-ons like "Disable **WebRTC**". In Chromium-based browsers, you can rely on the "**WebRTC** Leak Shield" or "**WebRTC** Control" extensions.

Email

ProtonMail, MailFence - they offer security, but if you do a little research you'll find they lie to your face. Gmail is one of those emails you shouldn't use even if it were your last. **RiseupMail** is also the safest choice here, but you need an invitation [if you have one, think of me :D].

Disroot Mail is also a decent choice. **Riseup** collects less data [barely collects anything], **Disroot** collects some data such as IP address, but these are encrypted on **Disroot** servers for 1 day and then deleted - not transmitted to third parties. [If you use it through Tor, you have nothing to worry about].

The Postman service in **I2P** [**Susimail**] is also a decent and good choice, but requires **I2P**. If you want to pay, I recommend **Posteo**.

Cloud Storage

There are many cloud services out there, but none can be fully trusted. **Disroot** Cloud seems to be the most honest, so if you must use a cloud service, go with that. Better still, store everything locally, for example on a USB.

You can encrypt the data stored here with **GPG** [you can also upload **GPG**-encrypted files to the cloud for even greater security] and not worry about the occasional attack that might hit your cloud service.

Video

Jewish YouTube is the worst thing you can do here. Invidious or **IncogTube** are much better choices. For Android you can use **NewPipe**. With **NewPipe** you can get the same experience, plus in **NewPipe** you can download any video in MP3 or MP4 format you want. You can download **NewPipe** from **F-Droid**.

Final thoughts

More than 80% of the internet is under jewish influence, not to mention **Cloudflare**, which is behind a monumental percentage of websites. Many websites block access via Tor, preventing your anonymity. That tells you everything - they want what they can profit from - your data.

You can also use an **I2P** Outproxy to browse the Surface Web if you're advanced and know how to do it. The internet is not what it was years ago. Years ago it was about freedom and information - now it's about money and power.

We live in a money-based society, and this affects everyone. Politics defines the mindset of a country, and money defines who you are. Unfortunately, in an ignorant society, this is the most important thing, but that does not mean you have to adapt.

There will always be alternatives - Tor, **I2P**, **Lokinet**, **Freenet**, **Riseup**, **Leap** - you just have to find them. Social media is a match on gasoline and could explode at any time. Many people will want to join in, but it will be too late - many will be lost in their own ignorance and swallowed up in darkness for good.

Wake up from the dream world while you still can - look around the world. You will see the decline. This is the sad reality. Without National Socialism and **Satan** there is no future and many will see that. **Satan** created us and gave us Knowledge - the answer is within you, you just have to find it.

Secure Extensions In Browsers - Protect Yourself

Secure extensions can provide monumental security on the Internet if configured properly. Of course, there are some that are set up by default (like **Privacy Badger** or **ADBlocker Ultimate**), but there are also some that you have to configure yourself.

This is a shorter (a bit longer in hindsight) post, and explains briefly (rather longer) what add-ons you can use to keep yourself safe. These apply to all sites, including Forums.

It is also worth disabling cookies and scripts on the Forums. You don't need to worry because the Forum is secure. The Forum is in good hands, but your safety is important.

I write extensions for several Browsers, there are plugins for both. I wrote a post earlier about setting up browsers, if you haven't already done so, read it.

About Firefox configuration settings;

https://ancient-forums.com/viewtopic.php?f=3&t=80307&sid=148b28e20bad57a64e602e9dda116a56

Add-ons For Firefox; uMatrix, xiMatrix, uBlock Origin, HTML Content Blocker, NoScript, Decentraleyes, LocalCDN, Cookie-AutoDelete, I don’t care about cookies, Cookie Quick Manager, ClearURLs, UserAgent Switcher, Disable WebRTC, WebRTC Leak Shield, FoxyProxy Standard or Basic and HTTPS Add-ons.

uMatrix - An add-on that allows you to block many things on a website (cookie, CSS, frame, script, image, other). You can do these by clicking on **uMatrix** in the add-ons, then clicking on what you don't want to appear and setting it to red (block). Red is block, green is allow.

It takes a little learning and getting used to **uMatrix**, but you will get used to it.

uBlock Origin - A great add-on. You can block many things in the settings, such as scripts.

NoScript - Script blocker. In the settings you will find "Site Permissions" and here you can change all of them to "Default". This way scripts will be blocked on all sites.

/*When adding plugins, make the changes immediately, not just on the specific pages.*/

Cookie Auto-Delete - Once you've added it, click on the plugin and then turn it on. "Autoclean Enabled".

FoxyProxy - If you want to configure it for **I2P**, for the HTTP part, enter "127.0.0.1, localhost", Port: 4444. If you want to configure it for Tor, enter "127.0.0.1", Port: 8118 or 9050. But you'll need Privoxy, which can be used for **I2P** as well.

Cookie Quick Manager - This will tell you how many cookies a page has. You can delete them by clicking "Clean".

User Agent Switcher - You can set up multiple browsers for yourself that sites will see. The key is to choose a browser/system version that you don't use. For example, you use **Firefox** on Ubuntu - in User Agent Switcher you change the browser to "**IceCat**" and the system to, for example, Fedora **Linux**.

/*The ones I described are the extensions where you have to configure things a bit. That's what I'm doing with **Pale Moon**.*/

Add-ons Pale Moon; ADBlock Latitude, Block Content, Cookies Control Panel, Decentraleyes, Eclipsed Moon, FoxyProxy Standard or Basic, HTTPS

Always, HTTPS Enforcer, HTTPS Inquirer, I don't care about Cookies, ScriptBlock, Toggle JavaScript, uBlock Origin, eMatrix.

eMatrix - Similar to **Firefox**.

uBlock Origin - Same settings as **Firefox**. However, here you need to add the extension via Github. What you click on **uBlock** in **Pale Moon** will redirect you to Github. In the "Latest Release" section, you will see a "**uBlock**0_1.16.4.30.**firefox**-legacy.xpi" file.

https://github.com/gorhill/**uBlock**-for-**firefox**-legacy/releases

It will redirect you to this page, and underneath it you will see the **uBlock** file. Click on it and the program will add it.

/*Just click on it and it will add it automatically. The page requires a Script, and since Scripts is automatically blocked in **Pale Moon**'s "*about:config*", you may need to change this. Or open the link in another browser, then right click on the file, "Copy Link", then paste it into **Pale Moon**.*/

Note: **Pale Moon**'s "*about:config*" settings are set by default, it's not advisable to configure things. You may want to set "SendRefererHeader" to 0 and "geo.enabled" to "false".

Block Content - One of my favourite extensions wiht **uMatrix**. In the plugins, you can click on Block Content next to "Preferences" to block a number of things. (All extensions have "Preferences" where you can set things.)

“Block Download Of” - Font, Image, Media, Object, Script, Stylesheet (This is not worth blocking as it will disable CSS on pages so pages will look "weird"), SubDocuments and XHR (XMLHTTPRequest).

“Permissions" Image - Block all images, Object - Block all objects, Script - Block all scripts, Subdocument - Block all subdocuments.

"Other" - Cookies - Not Accepted, Send Referrer - Never, Local Storage - Disabled.

LibreWolf - This browser has been said good and bad about, but it is in fact safer than **Firefox**. **LibreWolf**'s "*about:config*" settings have almost everything set by default that I mentioned in my "Browser privacy" post. There were some that weren't, but most of them were.

Think of this browser as **Ungoogled Chromium**. **Ungoogled Chromium** is a secure version of "Jewgle Chrome", **LibreWolf** is a secure version of **Firefox**. Of course **Firefox** is also safe if you do all the setup and configuration.

The only thing I didn't like about it is that **WebRTC**, sending referrer and geo is not turned off by default. You can disable it with all false of "*media.peerconnection.enable* / *media.peerconnection.turn.disable* / *media.peerconnection.video.enabled*". You may also want to use a **WebRTC** blocking extension - **WebRTC** Leak Shield, Disable **WebRTC**.

The **LibreWolf** extensions are almost the same as for **Firefox**. GNU **Icecat** is good and secure browser too.

Secure Browsers:

GNU Icecat

https://www.gnu.org/software/gnuzilla/

Tor Browser

https://www.torproject.org/download/

Pale Moon

https://www.palemoon.org/

Ungoogled Chromium

https://github.com/ungoogled-software/ungoogled-chromium

LibreWolf

https://**librewolf**.net/

Secure search engines:

Mojeek

https://www.**mojeek**.com/

MetaGer

https://**metager**.org

Monumental Security Reviews

Content

Introduction
1. [Browsers]
Google Chrome
Brave
Ungoogled Chromium
Mozilla Firefox
GNU IceCat
LibreWolf
Tor Browser
Pale Moon
WebBrowser
Joke Browsers
2. [Add-ons]
The Most Useful Add-on - uMatrix
3. [Linux Distros]
Linux Security
4. [Anon Networks]
I2P
Lokinet
5. [Emails]
Gmail
ProtonMail
MailFence
Postman (**I2P**)
RiseupMail
6. Encryption
VeraCrypt [Files]
KeePassXC [Passwords]
GPG Symmetric File Encryption
Closing Words

Summary

Introduction

In everyday life, it is important that you use the internet in ways that are crucial to your safety. There are a number of browsers, perhaps the best known of which are here. I will analyse some of the most popular ones so that many people can understand them better.

I won't go into too much detail here, just by way of introduction - most of the 'famous' browsers do almost nothing to ensure security. "Security by design", "Privacy Focused" - advertising slogan. Nothing more, they are just given a role to enhance appearances.

Worth putting this post in your bookmarks if you don't have much time to read. I have checked some information from other sites to make sure it is correct and really conveys the truth.

I hope this information will provide you with enough knowledge and understanding for your future activities on the internet. Well, let's get started.

Browsers

Google Chrome - Level of Spyware: MONUMENTALLY HIGH

Probably the most famous browser worldwide. Well, when you connect to the browser, it sends all sorts of data about you to various Google addresses, purely for "statistical" and other "security" reasons, and of course, just because. This includes your system type, your IP address, your browser settings, your passwords, your data etc about you.

In short, anything that contains information about you.

Since Google doesn't have an "*about:config*" like competi**tor Firefox**, you can't customize these functions. Since Google's search engine is the default, it sends the same amount of data to the same number of addresses, including your content.

If you have the "Show search suggestions" feature enabled, it will automatically send you a prompt with your details, your search and what you want to search for. This is by no means good, in fact it's worse. Let's also take an example of "security" settings.

You can set up "secure" DNS providers. Nothing could be further from that, because what's there is anything but secure. Starting with the evil **Cloudflare**, which acts as Mitm, that's where the data goes first.

I'll give you an example - on any page, next to the certificate, you see "**Cloudflare**", the following happens. Your request to the site is first sent to **Cloudflare**, along with all your data, and then **Cloudflare** stores that data and then decides whether or not to pass it on.

So initially all your data ends up with Cloudlflare and then with the site. Two arithmetic operations in just seconds.

Tor is blocked. Since you can hardly know anything about the people using **Tor** [this includes location, IP address and traffic], Cloudlfare doesn't like this, as it can barely get any information. Any site that uses **Cloudflare** is doing the worst possible thing to both itself and its visitors.

In short, Google Chrome should be the last browser you think of. Not to mention Microsoft Edge, which is probably even worse than Chrome.

Brave Browser - Level of Spyware: High

By default it includes an ad/sniffing/script blocker, but that alone isn't worth much. Script blocking does not protect against tracking, only against certain negative scripts and XHR [XmlHttpRequest]. Of course Script Blocking has several advantages, but by itself it is just a Script Blocker that you can block in your browser settings.

Brave sends data to several places, including itself, and does what it wants with that data. Since it is a Jewgle based browser, it depends on it. It has many google components, so google knows you well.

By default it connects more Brave addresses, static addresses that suck your data sufficiently. Not to mention Brave's abuse of privacy rights, which is nothing new with them.

The data they collect - your name, address, phone number and other "minor information" - obscures the collection and storage of your IP address. But in the background, this information includes your operating system, IP, location, etc.

Also just a crappy browser with false promises that should be avoided. But then what can be done? Use a fork such as [i.e. the only decent one] **Ungoogled Chromium**. Brave Search doesn't seem to be bad - good search results, doesn't collect IP addresses, doesn't require scripting, although if I remember correctly it's closed source so these are not certain. Basically this browser is like Google Chrome with a few additions.

This browser isn't a big gimmick, its default "security" features don't work as powerfully as they claim. Like if you buy a Google, put in an AdBlocker and set ScriptBlock in the settings. This is not talent.

Tor's functionality might be suitable for someone who just wants to remain anonymous, but on a smaller scale. Because Brave sends you a number of requests before you do anything, using the **Tor** functionality does not affect their ability to

collect data about you. They know everything except your web traffic, which is probably the only thing they don't know about you. For Tor, use the **Tor Browser** itself, or a browser configured for Tor, such as **IceCat**. The key is to avoid the Brave browser by far.

Ungoogled Chromium - Level of Spyware: No Spyware

Sends no unsolicited requests anywhere, gets rid of Google completely. It's a "de-googled" browser, without any google bindings, and gets rid of them for you. Available for jewdos, **Linux**, but there is also an AppImage which I think is more worth using.

It also doesn't add extensions exactly through the Chrome Webstore, but with a secure alternative. Probably the best Google fork ever. It has removed all the Google bindings and the developer is a very smart person and takes care of a lot of things.

However, as far as I know, this browser has one developer and they are trying to develop it with the community [I haven't confirmed this, but that's how I remember it], which is a big disadvantage against Google's monumental development team, and it's not clear how long they can keep up.

There are of course other Google forks, but this is by far the cleanest of them all.

Mozilla Firefox - Level of Spyware: MONUMENTALLY HIGH

Also a poser, touting "Security". Well, **Firefox** has some useful features, but it is far from secure. To be so, telemetry must be disabled completely, all connections with **Mozilla** must be severed.

Even when you open the browser itself, it makes unsolicited requests to a number of addresses, and this does not change while you are browsing. Its default search engine is Google, which it prompts every time you hit a key, thus connecting to it and removing a big layer of security.

Turning off all telemetry in **Firefox** is justified and, not incidentally, it uses Google Safe Browsing, which again connects to the evil Google.
Of course, this requires a lot of "*about:config*" fiddling and skill, because it's easy to mess up. My **Kundalini-Tool** helps the **Firefox** situation, but that's only because many people don't even care what browser they use, they just "have to have something".

The plugin support is great, uses Webxt, as does Google, and GTK3 library. The source code is open, so security risks could easily be fixed with outside help. **Firefox**'s developer base is large, but security is still lacking.

If you want some security in it, use the "Secure-Browser" feature of **Kundalini-Tool**. This does not exclude some of the telemetry and requests that are still in progress, or even what is happening in the background, but it is more than nothing.

GNU IceCat - Level of Spyware: No Spyware

It uses an earlier version of **Firefox**. It happens to be a browser based on **Firefox**. Also does not send unsolicited requests anywhere, takes care of your security. It also has "*about:config*" preconfigured [missing one or two things], but it's a good browser by default.

Completely open source, getting rid of **Firefox** as much as possible. It comes with several pre-installed plugins [if you download from their site, but if you download from e.g. slackbuilds, this is not true there], but it lacks **uMatrix** here too.

It doesn't send unsolicited requests anywhere, which makes this browser No Spyware. On this list, **IceCat** and **Ungoogled Chromium** are the ones that are spyware-free by default.

LibreWolf - Level of Spyware: Low

Also a **Firefox**-based browser, getting rid of **Firefox** in most cases [IN MOST CASES]. Still handles **Firefox**-bound requests. You can add extensions through **Mozilla**'s site, which will make requests to it, thus hindering its security.

The development team is not very big, much smaller than **Firefox**. In fact, it is dependent on **Firefox** to some extent, and as soon as **Firefox** dies [because you can see the smoke of that already], it will take all **Firefox**-based browsers with it.

Google wants to take over the whole Internet, and as soon as that happens, the Surface Web will die [It is died, btw]. Unfortunately, there is currently no browser that is completely secure by default [Maybe WebBrowser, which is a **Pale Moon**-based browser, or **Pale Moon** with minor modifications].

Both **LibreWolf**, **IceCat**, and **Tor Browser** are under the influence of the evil **Mozilla**, and all are tied to it to some degree.

LibreWolf is a **Firefox** browser with some "*about:config*" modifications, which **Kundalini-Tool** also provides, so we're pretty much in the same place. Although it doesn't send as many unsolicited requests as **Firefox** itself, it is dependent on it, and it's not known how long its team can keep up with **Mozilla**.

In any case, it is a much safer choice than **Firefox** itself.

Tor Browser - Level of Spyware: Low

Well, it is probably considered the "most secure" browser ever. Well, the reality is far from it. **Tor Browser** is nothing more than a **Firefox**-based browser that runs over the **Tor** network. You can do this yourself if you configure **Firefox** Ports properly.

It still makes a certain amount of requests to **Mozilla**, its default search engine is DuckDuckGo [it has jewgle in it - joke], but DuckDuckGo is not known for its security. DuckDuckGo also contains spyware, although it is a better choice than the Google search engine. It stores your data and who knows what it uses it for.

It uses Telemetry and sends requests to **Mozilla**, of course it does this anonymously, but this can get worse with later updates [and of course "Auto Update"]. Look in "*about:config*" for "*app.update.auto*" and set it to "False".

Automatic updates are enabled by default, which only makes things more difficult. You have no way of knowing what goes into these updates. Also, in the security settings, "Safest" just blocks JS, media and a bit more at some level, with the default **NoScript** addition on the side.

Now, **NoScript** could be useful, in addition to blocking several things with it - script, frame, ping, fetch, etc - but those are just individual things that **uMatrix** does better.

Tor does not recommend adding browser extensions [this has been strongly denied by other browser developer], but feel free to add extensions. Adding extensions is done through **Mozilla**, even if you are using Tor, and this means requests to **Mozilla**. It's worth adding **Adnauseam** and **uMatrix** extensions for better security.

Tor Browser does not provide security. You may even encounter malicious software or sites. **Tor** gives you anonymity, but it does it very well. In fact, a properly configured **IceCat** or PaleMoon with **Tor** implementation is worth more

than the **Tor Browser** itself.

Or if you're very paranoid about cyber security [Which as an SS can be a normal phenomenon, at a healthy level of course], run the entire **Linux** Distro over the **Tor** network. You can do this by configuring **Tor** files and using Iptables.

The **Kundalini-Tool**'s "Torify" feature provides system-wide **Tor** enforcement. Although I write this post before the **Kundalini-Tool** update, when **Tor** enforcement was still browser-based, I don't know if the update was available at the time of publishing this post or not. Who knows.

In any case, I don't want to destroy your idea of Tor. The **Tor browser** is still more optional than most browsers in terms of anonymity, but if you want to be safe while using the **Tor browser** in addition to anonymity, use extensions like **uMatrix**.

Pale Moon - Level of Spyware: Low

Probably the only browser on the list that I would say would be the most optional choice. Perhaps because **Pale Moon** has fallen into the trap of contradicting the statement "Your Browser, Your Way".

It used to, but the backlash has started. The **NoScript** and **Adnauseam** plugins have been disabled because they "cause page breaks". Are you serious? If you set up **Pale Moon**'s "Block Content" plugin, it breaks pages the same way and provides security, just on a larger scale.

The problem is what gives you security on the web and the good is what spies on you, right? Extensions like **Adnauseam** or **NoScript** strive to provide security, yet they are blocked. Where did the point of the above statement go?

Adnauseam is a good blocking extension, but it was blocked by jewgle, and **Pale Moon**. You can re-enable them in **Pale Moon**, but that requires "*about:config*" knowledge, and for a beginner it's not easy. In **Firefox** you can find it in the plugins, but it requires a **Mozilla** bind.

Pale Moon offers add-ons on its own site, not **Mozilla** add-ons. There are fewer add-ons, but they are more useful and important. Only those that are monumentally needed are included. In any case, adding add-ons in **Pale Moon** is different than in **Firefox**, for example.

Although the most important extension, **uMatrix**, is available for **Pale Moon**. Unfortunately, **Pale Moon** is starting to sell itself, it is starting to prioritize its partners as its own users, and has become something of a "weaker" **Firefox** clone. Apart from that, it still stands up to some of its claims and cannot be said to be unsafe.

Someone called PM a "sinking ship", and in this he may be right.

The **Tor** network is blocked. I cannot view the **Pale Moon** site through **Tor**

because it is blocked by Moonchild. It is also backed by the evil, phishing giant **Cloudflare**, and they are all and all systematically sinking this lovely little browser.

Here are some "*about:config*" options that if you change, the Spyware level will be reduced to zero:

extensions.blocklist.enabled -> False

services.sync.prefs.sync.security.OCSP.enabled -> False

security.OCSP.GET.enabled -> False

security.OCSP.require -> False

security.OCSP.enabled -> 0

geo.enabled -> False

After the changes, Pale Moon looks like this - Pale Moon - Spyware Level - No Spyware [Secure]

I recommend this browser for any use. Every secure browsers have minor issues, as does PM, but it's still the cleanest of the browsers currently available for everyday use and for your safety. **Pale Moon** is good for everything if you take a minute or two to set it up first.

Available for jewdos, Mac, **Linux**, **FreeBSD** [Beta]. Remember to add the **uMatrix** extension to all your browsers if you want to stay safe.

In fact, if you configure **Pale Moon** properly and enforce Tor, or better yet, if you run your entire **Linux** system over the **Tor** network, you will be much more secure and anonymous than if you use a **Tor** browser.

WebBrowser - Level of Spyware: No Spyware

Well, perhaps this is the browser, along with **Pale Moon**, that I can confidently recommend for the modern internet. It doesn't send unsolicited requests anywhere, and is itself built on **Pale Moon**. Definitely worth a try, you can check out the Project below.

https://git.nuegia.net/webbrowser.git/

Opera, Internet Explorer, Safari, Opera Gaming, Microsoft Edge - Level of Spyware: MONUMENTALLY HIGH

Avoid them, they fall into the pity and joke category.

The Most Useful Add-on - uMatrix

This is an all-in-one add-on that allows you to block almost everything on any page, or even globally at once.

uMatrix automatically blocks malware, trackers, third party domains, protects against fingerprinting, blocks ads and much more. You can block P**ages**, **JavaScript, Cookies, CSS, Frames, Media, Images**, **XHRs** [HTTP requests made by scripts - **XmlHttpRequests**], and much more to keep you safe.

Of course the benefits of using **uMatrix** cannot be condensed into a small post, it all depends on understanding.

If you use **uMatrix**, your security will increase monumentally. The downside is that it takes time to learn how to use it, but it is worth it for your security. It is available for almost all browsers. Some browsers [**IceCat** for example] require a bit of tinkering to add, but it's not complicated.

The "Advanced" option in **uBlock Origin** is pretty good, but not nearly as useful as **uMatrix**. With **uMatrix**, you can literally block everything, plus it protects you from many things in the background.

For a properly configured browser, you only need 3 add-ons - **uMatrix**, **Adnauseam** and **NoScript**. **uMatrix** blocks what you don't need in the background and on certain pages and protects your activity, **uBlock** blocks a number of things and **NoScript** ensures that suspicious scripts are blocked.

But if you set up **uMatrix** to globally block Scripts and only allow them on pages where you want them [for example, **JoS**], you can leave **NoScript** turned off. You can add Disconnect or Disable **WebRTC** instead, although you don't need the latter if you've changed the values manually in "*about:config*".

For **Firefox**-based browsers, you need to change "*media.peerconnection.enabled*" in "*about:config*" to "false". On Chrome-based browsers, you need to use an

extension such as **WebRTC** Leak Shield. **Pale Moon** disable **WebRTC** by default.

I would never go online without **uMatrix**, and I wouldn't use any browser without it. **Decentraleyes** may conflict with **uMatrix**. **Adnauseam** may also conflict with other ADBlockers.

About Linux Security - Life Without Systemd

I explain it in more detail in the **Kundalini-Tool** "README666" file, but here is a smaller list and some useful instructions you can do to ensure your security.

There are many **Linux** Distro, and most of them follow the **Linux** Philosophy principle - "Your system, your way, your business". Jewdos is the monumental opposite.

Well, if you are serious about your security [which as a SS is HIGHLY RECOMMENDED], then choose a **Linux** Distro that is free of **Systemd**, such as **Slackware**, or for **Debian** fans, **Devuan**, or an Arch Fork, like Artix. Although, you can squeeze out some security on systems that contain **Systemd**.

Some of the famous **Linux** distros that have fallen into the **Systemd** trap - Ubuntu, **Linux** Mint, Kali **Linux** [the Kali's site is behind fucking **Cloudflare** - pathetic], Parrot OS, etc. **Systemd** is a hindrance to your security, but you can do something about it. For example, keep all your files and folders in **VeraCrypt**, and all your passwords in KeePass.

To access the internet, use multiple VPNs [WireGuard or OpenVPN, combined with iptables], or even Tor, and properly configured browsers. Using google on Windows systems is like physically walking alone with all your data out in the open on a several-mile stretch of road to your destination. So the jews know more about you than you know about yourself.

Systemd has its flaws, not that I give it a positive, one or two of its features are tolerable. **Slackware Linux** is the best in terms of security, but it has several drawbacks - you have to install many programs from source and build them manually from Terminal.

You need to know and understand **Linux** architecture and architecture, otherwise you will get lost during installation. For **Slackware**, you can manually configure several encryption settings from Terminal during installation [e.g. encrypted

/home, encrypted /root, encrypted /swap, encrypted partitions, overwrite partition with metadata to increase security] using **Cryptsetup**.

But this requires a higher level of knowledge, not to mention time. **Slackware** is more complicated than an Arch in my opinion, but it's also more secure. If you don't have time to learn **Slackware**, or other serious Distro, you can choose from the list below.

Although the distributions listed above include systemd, they provide a beginner-friendly alternative;

Linux Mint [systemd] - Offers more encryption options and is beginner friendly. You can access many packages and programs from the Software Center, and **Kundalini-Tool** works perfectly on it.

Parrot OS [systemd] - Although this is a system for IT professionals, there is a "Home" edition that is secure and offers many pre-installed useful programs and packages. [**Tor**, **Onionshare**, **AnonSurf**]

Devuan [sysvinit, openrc]- **Debian**-based, without **Systemd**. If you know **Debian**, you should have no problem with it.

Kali Linux [systemd] - While not for beginners, you can test the security of your machine, network and devices.

PureOS [systemd] - A security-oriented, **Linux** Distro with Gnome.

EndeavourOS [systemd] - Arch **Linux** based, uses Arch repositories with minimal pre-installed programs and graphical interface. Preferably the choice of Arch fans.

Slackware [sysvinit] - **Systemd**-free, secure **Linux** Distro. It follows the "One Application" philosophy. Nothing runs in the background, only the things needed

for the system. My personal choice.

Whonix [systemd] - Worth running under a secure **Linux** Distro with VPNs pre-configured for monumental security.

Tails [systemd] - Excellent for laptop users, or those who just want to browse the Dark/Deep Web. However, not entirely suitable for everyday use.

Prestium [Linux Distro Through I2P] - Runs entirely under **I2P**, and is a great choice for **I2P** enthusiasts like me.

VPN

There are a lot of VPNs available, and most of them are terrible. The "Gaming VPNs" don't deserve a mention. The likes of **NordVPN** should be avoided by far. The **Mullvad VPN** has pretty good security and doesn't require any personal data, but it's paid, just like **IVPN**.

From the ProtonVPN site:

"Data we collect and why we collect it. Personal data (related to your account): Account creation: To create an account, in order to use our Service, we do not ask your name or surname. All you need to do is select your username, then provide the email address and choose your password. You can also register with your existing Proton account."

They don't ask for your personal details because you're using ProtonMail to access it, and they've already done it there, assuming you've had luck using VPN or Tor, and they don't ask for your email address or CAPTCHA, which isn't much more efficient but a notch better.

Anyway, I don’t recommend to use **ProtonVPN** or any **Proton** services.

Another free VPN is **RiseupVPN**, which uses secure, highly encrypted networks. You can use it with "Bridge", Tor, use it with "Snowflake", even **UDP**; **UDP** is faster regarding the packets, but not safer than **TCP**.

Their email provider is also by far the safest and most secure, plus it's free - but unfortunately it requires an invitation. Another decent email provider nowadays is Postman [**I2P**]. The likes of MailFence, ProtonMail - not known for total security, a lot of their talk is just hype.

The point of **UDP** is to get packets to their destination as quickly as possible, and in the process there is no guarantee that all packets will arrive. **TCP** is the opposite

- it is more secure because it organises the packets and ensures that they all arrive.

RiseupVPN is available for most **Linux** distros [If you are using **Slackware**, you will probably need to look for a **RiseupVPN OpenVPN** genera**tor** script to run over OpenVPN].

If you configure the entire **Linux** system for **Tor** [As Torify does with **Kundalini-Tool**].

If you're a big **Tor** fanatic, you can use **Torify** in **Kundalini-Tool** around the clock, set all your browsers to Tor, and use ".onion" alternatives. If you are an **I2P** fan, use the same method but configured for **I2P**. Or use **Kundalini-Torify**.

Anon Networks

I2P

The **I2P** Network [somewhat similar to **Tor**] is an encrypted, peer-to-peer anonymized network designed for internal use, unlike **Tor**. **I2P** uses the Jetty web server, and through it you can chat, surf and do everything else anonymously.

I2P differs from **Tor** in that, unlike Tor, it is not designed for external use, but for internal use. Within **I2P** you can create pages and forums in the same way, all anonymously and encrypted. Available for jewdos, **Linux** systems.

In my opinion it is better than **Tor** in terms of security and encryption. Outsourcing can be done with "Outproxy", but **I2P** works more inward than outward. **I2P** works with different ports, each serving a different purpose.

HTTP - 4444, HTTPS - 4445, for example. It favours internal use and everyone connects to everyone, that's how this network works. **Tor** is easy to spot as it has a unique fingerprint, but **I2P** has a different way of doing it and unlike **Tor** it is good against DDOS attacks.

Although Outproxy can be used for surfing the surface web, **I2P** is more used for Darknet, Eepsite [**I2P** Sites], or anonymous surfing. **I2P** doesn't have as many sites as Tor, but there are plenty of them, so there's something for everyone.

Torrent also works on **I2P**, in an anonymous version. This site [http://tracker2.postman.i2p/] has a monumental torrent galaxy and you can find almost anything. It is one of the safest ways to torrent at the moment.

I2P has many advantages, basically an encrypted and anonymous internet within the internet.

Lokinet

A pretty cool network, although not nearly as famous as its peers.

https://**lokinet**.org/

Search Engines

Google Search - Spying Level: MONUMENTALLY HIGH

This search engine exists because Chrome, Microsoft Edge - collects information about you. It does nothing useful, it automatically connects to many Google addresses, it collects monumental statistics, it does many queries.

This search engine should be avoided at all costs. Its only advantage is that it indexes most pages, and you can find many pages with it, almost all of them on the Surface Web. But you pay for it with your data, which is concentrated in the hands of the Jews.

It disables **Tor** as much as it can, and uses reCAPTCHA to make tracking even more feasible, as does ProtonMail. Google services should be avoided far, far away, especially as SS.

Mojeek - Spying Level: None

Quite a good little search engine, does not collect IP addresses, only CSS need [Tested this in **uMatrix**]. It has its own index and provides security. The only downside is that the search results are not very rich, but it is by far the cleanest search engine available.

MetaGer - Spying Level: None

Same as above. It has an Onion domain, so can be used in conjunction with Tor. But its search results are much better than **Mojeek**'s.

Tor -
http://***metager****v65pwclop2rsfzg4jwowpavpwd6grhhlvdgsswvo6ii4akgyd.onion/en-US*

I2P -
http://4zdcetlcp3tdg5h23gd3aeyzbvodepid7a6mb3w4qvxkdnm2by6q.b32.*i2p/*

Ecosia - Spying Level: Medium/High

I used this search engine a lot in the past. It is not considered secure, it stores IP addresses and other data, and it plants trees, which is quite nice. However, I would never use it again as it's behind the evil **Cloudflare**, so its essence is gone.

It's a shame, and it was a good search engine.

Brave Search - Spying Level: Medium

Well, given Brave's data collection, it's not out of the question that it does the same thing. It's backed by Amazon, which is not a **Cloudflare**, but these are things to watch out for. CSS alone is enough to use, but I can't trust this search engine. Avoid it, use **MetaGer** instead.

If you want to browse **JoS**, the safe **Mojeek** is also suitable. But if you want everything else, then switch to **MetaGer** instead.

DuckDuckGo - Spying Level: Medium/High

A notch better than Google, but no more, but if you're torn between the two, go with DDG, or at least use it on **Tor** or **I2P**.

Tor - *https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/*

I2P - http://gqt2klvr6r2hpdfxzt4bn2awwehsnc7l5w22fj3enbauxkhnzcoq.b32.*i2p*

Emails

Gmail - Spying Level: MONUMENTALLY HIGH

Well, not worth mentioning. It's really designed to get Jews to collect data on you, just like Chrome, Jewcrosoft Edge and others. The only advantage is that it supports mail clients, but nothing else.

I won't even go into the "Privacy Policy", we all know that Gmail is Jewish owned. Avoid it by far.

ProtonMail - Spying Level: High

Well, this is probably considered the most famous "secure" Email provider, but that's not quite the case. ProtonMail [Like Mailfence] has a minor form of encryption that researchers say is quite flawed, not to mention that it doesn't encrypt everything. Doesn't works without JS. [Sadly]

The names, addresses, senders and subjects of messages are all visible, and Proton can unencrypt encrypted data at any time. The PGP keys are generated in advance when the account is registered, and are probably full of unsolicited requests.

From the Proton site:

"IP logging: By default, we do not keep permanent IP logs in relation with your Account. However, IP logs may be kept temporarily to combat abuse and fraud, and your IP address may be retained permanently if you are engaged in activities that breach our terms and conditions (e.g. spamming, DDoS attacks against our infrastructure, brute force attacks).

The legal basis of this processing is our legitimate interest to protect our service against nefarious activities."

Of course, that's how everyone delivers - IP address storage and tracking, offered in a nice package. You don't know how long these are stored, because you can't trust Proton.

Another:

"If you enable authentication logging for your Account, the record of your login IP addresses is kept for as long as the feature is enabled. This feature is off by default, and all the records are deleted upon deactivation of the feature. The legal basis of this processing is consent, and you are free to opt in or opt out of that processing at any time in the security panel of your Account."

Seriously, who wants to allow information to be stored about them? Okay, I don't mean the people who irresponsibly accept all the cookies and tracking "protections" [which is also a marketing term, in the background the opposite is happening] on every site.

Seriously, think about what you do on the internet. You accept terms and conditions, cookies that are tied to you. If the phishing happens, it's not the company's fault, it's your fault because you didn't read the terms. Think about it, you can easily get in trouble.

They also have .onion domains that were so, so anonymous that if you weren't paying attention, the **Tor** domain would redirect you to their Clearnet address. How anonymous is that?

Let's look at the facts - "No personal data required", and later "We use SMS for this feature". Even if you just don't use a VPN or Tor, you may not need to provide personal details. If you use VPN or Tor, you'll suddenly have to enter some details.

Not to mention that Proton heavily discloses "sensitive" accounts to the authorities. If you confirm to them that a Proton user is exchanging "sensitive" messages, they can extradite you immediately. In the background they track your activity, collect your data.

IP addresses are collected by default, and stored for a limited time for "security" reasons [just like phone numbers]. It doesn't work without **JavaScript**, I somehow messed it up in **uMatrix**, it's full of crap and bullshit that is unnecessary for an "encrypted/secure" email.

Proton had a case in the past where they leaked data about users. Well use it at your own risk and don't trust it, but if you can, avoid this email as much as possible, just like MailFence. Alternatively it's good, a notch better than Gmail.

If you have a paid option, use **Posteo**, and avoid Proton by far. I know many people in SS use this for easier access [as I do], just wanted to share. If you're

going to use it anyway, do it over VPN or Tor.

*ProtonMail is available on **Tor** - https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/*

MailFence - Spying Level: High

From the MailFence website:

"We collect IP addresses, message-ID's, sender and recipient addresses, subjects, browser versions, countries and timestamps. When registering, you will be asked to enter an external email address. We send your activation code to this address and use it to communicate with you in case you are unable to access your account.

Incoming and outgoing messages are automatically analysed by our anti-spam, anti-virus and anti-abuse checking routines. When you pay by credit card we store some of its details. Team members have signed a confidentiality agreement to protect collected data."

Off to a good start, IP addresses are collected, stored, and additional data/metadata is collected about you. If you pay for this shit, they collect data on that too. When you register, you have to enter another Email address to which they send the code. Are you serious?

Another one:

"Yes. Our cookies are "authentication cookies" and not "tracking cookies": we don't track you after your session on our servers. You can find more information about the types of cookies here."

You don't know what cookies are, just as I don't understand why you need JS at all. You could easily run into a tracking JS without even knowing it. You are not notified that they are tracking your activity. Use **uMatrix** everywhere.

The "secure" MailFence will ask you for your real email account in advance and send you the code to proceed. I don't know about Mailing Client support, but you can guess.

Just read this:

"Should you close your account, all data will be permanently deleted 30 days after the legal expiration date (i.e. the Belgian law imposes 365 days after account closing). This means that your data will be PERMANENTLY deleted, as opposed to the practice of some major cloud companies which are unable to delete data.

We do not delete your account before the legal expiration date because users often ask to reopen their account after having closed it themselves."

Avoid it for the most part, just like Proton.

Postman (I2P) - Spying Level: None

An encrypted and anonymous email service available via **I2P**, which allows you to send messages to both external addresses [Surface Web client, e.g. Proton, or any other] and internal, i.e. ".i2p" addresses. It is currently the cleanest choice.

There is no need to provide personal information when registering, and the registration itself is simple. The email looks a bit different, with different settings. The only Email that supports **I2P** and is accessible through it. At least that I know of.

Here you can create Postman account [Note: **I2P** needs]:

http://hq.postman.i2p/?page_id=16

RiseupMail - Spying Level: None or Mild

Probably the most selective choice of services currently available, and free to boot. However, it does require an invitation, which unfortunately I don't have [If you're reading this and you have one, think of me :D]. The "privacy policy" is relatively tolerable, and fair.

No IP address storage, no sensitive data collected about you [location, operating system, browser, screen resolution, etc.], and strong encryption. You can create multiple "Aliases" within your Email account, which is very useful.

Your data is stored in turn, but with strong encryption, and can only be decrypted by the **Riseup** team, but they don't do this because **Riseup** is a human rights organisation who REALLY have your safety as their number one priority. Good question, then why do they store certain data?

Well, in order to access your account, the data has to be stored somewhere. It's not personal data, it's other data. **Riseup** does not collect personal data about you, or only very minimal data. It is really nothing like what Proton or MailFence does.

From the Riseup site:

*"All of your data is stored in an encrypted format, and only **Riseup** has the keys to decrypt the data. Additionally, as of March 2017, the storage for all new accounts is personally encrypted. **Riseup** is unable to read any of the stored content for these accounts. Any user with an account created prior to March 2017 may opt-in to personally encrypted storage."*

If you delete your account, it won't slide for days or weeks, it will be deleted, instantly. Unlike Proton, who is only willing to delete your account after a period of time, and until then you can imagine what they do with your messages and activity there.

I can actually recommend this Email with confidence, but unfortunately you need an invitation to join. If not, use Postman.

Encryption

KeePassXC

A password store for all your encryption and security needs. You can use Keyfiles with it, just like **VeraCrypt**, and it's a pretty well built secure password store. It is available for many **Linux** Distros and is worth using for secure password storage.

VeraCrypt

A program for high-level encryption of files and folders. It is available almost everywhere and is not difficult to set up. You can choose from several encryption options [up to three for one storage] and set several security levels.

First create a "Standard" container, then a "Hidden" container. In the Standard you keep the not so "sensitive" files, and in the "Hidden" you keep the important stuff, like SS writes. Generate the passwords in KeePass and save them there.

For both, generate a password of at least 30 characters, including all punctuation. Save them in KeePass. For greater security, generate 'key files' [at least four] and then you can even set a PIN for them.

This has several advantages - firstly, your folders/files cannot be accessed on your **Linux** system without you, so an attacker cannot recover or copy the contents of your data, as they cannot be accessed without you.

Secondly, only the people you want to have access to your data. Because you store everything in a highly encrypted storage [two of them], this is the safest way to store data in today's world.

So, if you lose your password, you can no longer access your data. It's worth storing them in a text file other than KeePass, encrypted with "**gpg**". One looks like "**gpg** -c

The program will automatically create a file called ".**gpg**" and delete the other unencrypted file. You can open the ".**gpg**" file by typing "**gpg** -d FILENAME”.

GPG File Encryption

You can use **gpg** to encrypt files locally. Once this is done, the file containing the data can now be accessed with your password. Let's assume that the file containing the super-secret data is called "safe-file". We want to encrypt the data in the "safe-file" file.

Type the following into Terminal: "**gpg** -c safe-file" [Replace "safe-file" with the name of your own file]. The program will prompt you for the password, then type it twice. Be sure to write down this password so you don't forget it. Then type "**gpg** -d safe-file" to remove the Symmetric encryption.

Here it will ask you for the password you entered, and once you have entered it, you will be able to see the contents of the file. This is an easy way to store files locally.

Summary

Briefly about Email - Use Posteo if you want to pay for something, or use Postman if you want something free. Use RiseupMail if you have an invitation [if you do, think of me :)], or use Disroot.

Briefly about Browsers - Use LibreWolf for common browsing, or Ungoogled Chromium. For the Forums, use Tor, or Pale Moon, or IceCat, with Tor or with VPN.

Briefly about VPNs - Use RiseupVPN [or use Kundalini-Router]. Or if you pay for them, use Mullvad VPN. It's worth running multiple VPNs at the same time, at least two. ProtonVPN is not really secure, use at your own risk. Use it if you really need a VPN, but better if you are using Riseup, Kundalini-Router or Mullvad.

Briefly about Search Engines - Use Mojeek, or if you want good search results, use MetaGer, or worst case DuckDuckGo on I2P or Tor. [Not ethical to recommend this, but a notch better than Google Search Engine]

Briefly about Add-ons - don't go online without uMatrix/xiMatrix, uBlock and Decentraleyes. Use Disable WebRTC too.

Briefly about Linux Distributions - If you are a real security fanatic, use Linux distributions without Systemd. If you don't, use Whonix or a security-oriented Distro. The choice is huge. Don't think of Linux Distros with Systemd as "all data is compromised or something", no, just a Systemd-free Distro will provide more security.

Briefly about GPG - Use GPG Encryption for files where you store some of passwords. It is not the best option if you encrypt a monumental large file, for this, use VeraCrypt.

Briefly about KeePassXC and VeraCrypt - Use these if you need a monumental security for your files/passwords.

Closing words

I hope this post has given you a little understanding of the "Projects" currently available that claim to be secure. I have not analysed everything at length, I have tried to be concise in what I wanted to convey.

I have tried to do a lot to encourage many of us to use security alternatives and take care of our online security. Online security is as important as physical security. In fact, we need to be much more careful online about what and where we search.

You don't physically go to people who are helping you with sensitive or even 'harmful' content, so they don't know about it. But you can leave a mark on the internet if you are not careful. It is time for SS to move on and step out of the jewish matrix.

I will not stop. If I can help at least one fellow SS member with these posts, I will have plenty to show for it. I love all my SS Brothers and Sisters equally, I wish you all the **Satan**ic happiness and the Quintessential Side of **Gods**.

Be careful on the Surface Web as it is under monumental jewish influence. Where you see **Cloudflare**, be doubtful and keep your data safe. The Surface Web will soon be under full jewish control and if we don't change this, it will happen. Realize this as soon as possible.

The Surface Web has failed.

On Encryption - Kundalini-Crypt, GPG, VeraCrypt & KeePassXC

It goes without saying how important it is to keep your files safe. In case of an attack or any problem, it is quite constructive to keep your files safe and encrypted from prying eyes.

There are several programs/software that you can use to keep your files encrypted - one of them is **GPG**. In this post we will discuss **VeraCrypt**, **KeePassXC**, **GPG** and Kundalini-Crypt. To get started, you need to get these first:

 # apt install keepassxc

You should get **VeraCrypt** from the **VeraCrypt** site, or from there if it is available in your repository. For **Slackware Linux**, you can install it from source here:

https://slackbuilds.org/repository/15.0/system/veracrypt/

If your distribution's repository does not include **VeraCrypt** and you cannot get it from the **VeraCrypt** website, you must install it from source. Don't worry, it's not complicated, just follow the instructions provided. To get Kundalini-Crypt, see the "Programs" section in the **Kundalini-Project** website.

Once you have it, open it and follow the instructions. Click on the "Create Volume" button, select the "Create Encrypted File Container" interface. You can then choose between "Standard" or "Hidden" volume, this post will now follow the "Standard" section. Same for "Hidden", but here you have to go through the process twice.

Here you need to select a folder for your **VeraCrypt** file, then choose one of the encryptions - I recommend "Aes(Twofish)", but it's up to you. For the name, I'm using "**veracrypt**_file_cont" for now. Then you need to specify the size of the storage - this is also your choice. So think about what you want to use it for. If you want to store everything here, several GB is recommended, if you want to store sensitive files, 3-4 GB is enough.

Then you need to enter a password. It is worth generating a strong password in **KeePassXC** or using Kundalini-Pass. You can also specify an additional security step - PIN, "Keyfiles", which I also recommend to consider. You can save all your data in a file, which you can then encrypt with **GPG**.

For the "Keyfiles" you need to generate - choose as many as you want, which you also need to store in a folder - this might be stored in a hidden folder independent of **VeraCrypt** [But don't delete the folder, you might screw it up].

Then you have to choose the file system, I leave that to you. Then you need to format the volume - you can do this by moving the mouse systematically and randomly - wait until the strip ends and says "Done: 100%". Then you are ready to use your container!

Go back to the **VeraCrypt** home screen and select "Select File". Here you need to enter the **VeraCrypt** file you saved at the very beginning, in my case it's "**veracrypt**_file_cont". Then click on the "Mount" button and follow the instructions. Enter your password, enter your PIN and "Keyfiles" if you have chosen and then click "Ok". Then you need to enter your system password and you're done!

If something is wrong, you probably misspelled your password or PIN. Once you've done that, your container folder will appear. You can put whatever files you want in it and keep them encrypted and hidden. If you want to unmount it, just go back to **VeraCrypt**, select the container, click "Dismount" and you're done.

You can also store your passwords here, but it's a good idea to store your passwords in a separate, encrypted location, such as KeePass. The method is also simple, just follow it.

Open **KeePassXC** and click on the "Create a new database" button. Enter a name for the database and add a description if you wish. You can increase the value of "Decryption time" up to 5s. You may want to set this to 3-4, this will increase the

security of your container.

Click on the "Advanced settings" button to choose encryption - I recommend Twofish, but you can also use the default AES if you want. You will then need to enter a password. Again, you'll need to use a strong password. An example of password generation with Kundalini-Pass:

$ kundalini-pass -g

Password generation...

Password: *UTi{9_B<mTj+(Y_LS/+b7/yf84uWwaU)T27B3gw

You can save this encrypted in a folder or in **VeraCrypt** itself. It is recommended to use **GPG** encryption on the file where you store the passwords. After entering the password, the program will ask you where you want to save the KeePass file. Do the same as for **VeraCrypt**. And that's it!

Your passwords are now secure and encrypted.

You can also use **GPG** and Kundalini-Crypt to make your files even more secure. Let's take a simple example - the file name will be "super_secret_file" in this example, the content should be "Hi, I'm BrightSpace666 From The **Joy Of Satan**.", and you want to keep this file very secure. Starting with Kundalini-Crypt, we first encode the contents of the file:

$ kundalini-crypt --encode super_secret_file encoded_super_secret_file

The newly encoded files will have the file extension ".kundalini" [encoded_super_secret_file.kundalini]. You can see that the contents of the files have been completely changed:

$ cat encoded_super_secret_file.kundalini

We will see that the file contains symbols, characters and everything else - our file is encoded. Then:

$ gpg -c encoded_super_secret_file.kundalini

Here we choose a strong password like the one I just generated with Kundalini-Pass: "*UTi{9_B<mTj+(Y_LS/+b7/yf84uWwaU)T27B3gw"

Our file was first encoded and then encrypted with **GPG**. If you want to decrypt:

$ gpg encoded_super_secret_file.kundalini.gpg

We entered the password [In my case - *UTi{9_B<mTj+(Y_LS/+b7/yf84uWwaU)T27B3gw] and got the decrypted file. However, here we do not see what we typed, but the encoded content. In order to get the content back permanently:

$ kundalini-crypt --decode encoded_super_secret_file.kundalini decoded_super_secret_file

You can see the contents of the file:

$ cat decoded_super_secret_file

"Hi, I'm BrightSpace666 From The **Joy Of Satan**."

This is a double protection for the content of your files [It is more secure if you store these files in your encrypted **VeraCrypt** container]. Note that if you encode a file using Kundalini-Crypt, it will have the suffix ".kundalini" at the end of its name. Don't forget this when you want to recover the contents [just write .kundalini after the file as shown above].

Let Us Be Clear About A Few Things

Original Post -> https://ancient-forums.com/threads/let-us-be-clear-about-a-few-things.96554/#post-1072914

As the title says, I would like to give some explanations/information about some things, as well as things in the pipeline.

First of all, I'm fine - I hope you're fine too. This post should have been written earlier, but I felt I had time to work on it a bit now.

As many of you know, this is important to me, and I place great emphasis on the anonymity and security of SS. Now, there have been some minor misunderstandings about this - I've received some emails that I've been thinking about.

It's great that you care about your security. That's one of my goals, to encourage you to do that. I have spoken to my **Guardian Demon** about the **Kundalini-Project** and She has given me advice about this and also about a new job I am planning.

Everything I do for SS I do with all my heart and dedication.

No need to be so "paranoid" about anonymity/security. Unfortunately, we live in a world where it is inevitable that we will be in contact with the internet and virtual space.

We have accounts, bank accounts, things, and they are all in virtual space. This is perfectly normal. Technology is evolving and we are evolving as a human race and as a society - I am not against technology, make no mistake.

I despise exploitation, lies, data collection and the like. On the Internet, you have

the right to freedom and anonymity, and no one can interfere - if they do, it is called censorship.

Accept that the internet has been taken over by jews on a monumental scale, because in today's world it is the easiest way to track someone. I will go into more in this post, read on.

When you're online, a lot is happening in the background, without your knowledge - many browsers phone home, this includes your data. Many browsers collect and share data about your habits, your system, your location, etc.

When you type search values into the browser bar and they are displayed to you before you click to search - you are making a request to the search engine, which selects the values for you. You have done nothing, you have already sent the information about yourself.

And that's how the whole internet works - you don't have to consciously do anything, your data is sent. **JavaScript** is one way that site owners can collect very, very relevant and a lot of information about you.

The ads that are displayed can also store data about you and can further track your browser session. Not to mention the rest. The point of my posts on anonymity/security is to raise awareness of this danger and to pass on information. Yes, sometimes in a crude way, but the point should get across.

When I talk about "be safe", "use **Tor**, **VPN**, **Linux**" etc., I am specifically referring to SS. Keep your SS secure - everyone's data is collected and stored by companies. This happens from the moment you first go on to the internet.

Your SS life should be completely separate from your more "open" life. You should use the programs/software you use for SS.

For example - don't use the same **VPN** server for forums as you do for **Twitter** for example. Use servers in other locations. Don't use **Pale Moon** for banking if you

use **Pale Moon** for forums - **User-Agent** manipulation can get around this, but many people don't know this.

Another question I am often asked - **social media**. It is entirely your personal choice whether or not to use it. If it's the only place you can keep in touch with your friends or girlfriends, then it's your responsibility whether you use it.

Social media is under monumental jewish influence - they collect everything they can about you. They put viruses on your system, they share monumental amounts of data in the background without your knowledge - they have no respect for you.

If you must use them, you should do so through a browser. Don't download it to your phone! The browser does most of the processing, while on your phone has access to everything - files, contacts, pictures, music, kittens, puppies, everything.

It is not necessary [or even recommended] to use a real name here. You can give a completely unrealistic name - for example, if your name is Thomas, use Gordon. The point is clear - also in terms of email address, never use an email address on social media that you use on SS.

If you use **Disroot** on SS, don't use **Disroot** here either - the point is clear.

So my Cyber Security, anonymity posts are for your SS life! Everyone lives a public life to some extent, but keep your SS private! You are needed, needed by humanity, by me, by High Priest, by everyone - be safe!

I am not encouraging you on social media - however I am not your boss to tell you what to do. The responsibility is your. You can apply the knowledge I give you to all aspects of your online life.

You can contact me by email. Not just IT/programming questions, you can contact me with any questions. I have recently brought the IT part of SS to the forefront, I have written several important posts in the past - there is no end to them.

My life has just taken a different direction - I have to do what the **Gods** and **Satan** Asks me to do. There have been many times when I didn't listen to **Satan** or **Gods** because of the superiority of my own personal ego - that was a big mistake.

The **Kundalini-Project** has a purpose - initially to spread **JoS**, to bring Knowledge to people and to inspire Truth. Our society is in decline and has the potential to get worse.

As long as people will exist as slaves, they will not find Truth. When I talk to people, I often have to realize how much difference there is between us. We have completely different values.

Do not worry that everything will go to shit - **The Gods Will Not Leave Us Alone**! There will come a time when we will win, but every single day you have to get off your ass and do what you have to do.

A large percentage of people will go their whole lives having done nothing for humanity. Before the **Gods**, when my time comes, I will have to answer with a clear conscience and that I have done all I can for SS, my **Brothers** and **Sisters**.

The **Kundalini-Project** is also expanding outside SS - my website has a good number of visitors and it is only systematically growing. These people are finding not only the **Kundalini-Project** but also **JoS**.

If the **Kundalini-Project** brings up to 1 person a day to **Joy Of Satan**, I'm already happy - that's one person's life changed in a positive direction.

Also a message to those rats who want me to die and disappear - you are wasting your time.

Remember one thing - the enemy's strength and importance is nowhere compared to Ours. In the end it will be the **Gods** and **Satan** who will decide, because They and We have the Truth. Enemy programs are just ridiculous efforts without

substance or benefit. This is called pathetic.

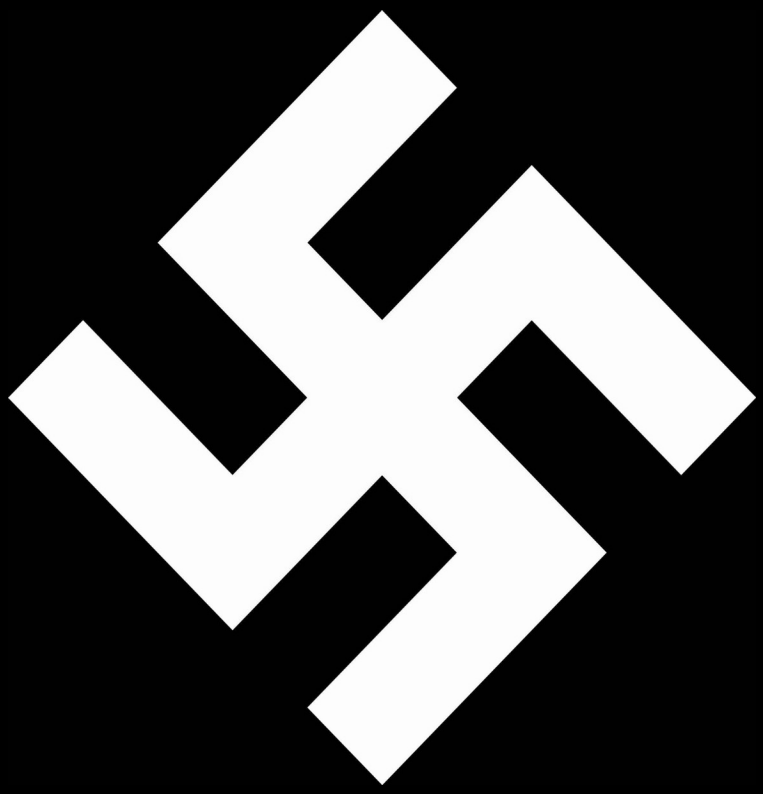
Be strong,

Sieg Heil!

Contact

My I2P Mail → BrightSpace666@i2pmail.org

My Disroot Mail → BrightSpace666@disroot.org



Without Knowledge, Power Is Lost, As Power Is Lost, So Is Understanding Lost And So Is True Knowledge Lost.

Hail Satan!

BrightSpace666