

Forum:[Hack Forums](#)

Thread: [Maintaining Privacy and Security Online](#)

SUI-3183372 - August 16, 2016, 6:53 pm

Quote:If you think privacy is unimportant for you because you have nothing to hide, you might as well say free speech is unimportant for you because you have nothing useful to say.

Edward Snowden

I got asked about privacy online for the average user, and I ended up compiling some info regarding such. This is a broad topic and most of this information isn't coming directly from me, rather it is being compiled from multiple sources. I won't take credit for anything, and I'll attempt to link to sources where I can.

Encryption of data

I use [VeraCrypt](#) full disk encryption for all of my drives and partitions, not just my OS. VeraCrypt adds enhanced security to the algorithms used for system and partitions encryption making it immune to new developments in attacks.

VeraCrypt also solves many vulnerabilities and security issues found in TrueCrypt, the old industry standard for full disk encryption.

Key disclosure law - Who is required to hand over the encryption keys to authorities?

Mandatory key disclosure laws require individuals to turn over encryption keys to law enforcement conducting a criminal investigation. How these laws are implemented (who may be legally compelled to assist) vary from nation to nation, but a warrant is generally required. Defenses against key disclosure laws include steganography and encrypting data in a way that provides plausible deniability.

Steganography involves hiding sensitive information (which may be encrypted) inside of ordinary data (for example, encrypting an image file and then hiding it in an audio file). With plausible deniability, data is encrypted in a way that prevents an adversary from being able to prove that the information they are after exists (for example, one password may decrypt benign data and another password, used on the same file, could decrypt sensitive data).

Virtual Private Networks

I always recommend using a good VPN, even for normal every day browsing. [View more information on how VPNs work and why using one is important here.](#)

View my [other thread for my personal VPN suggestions](#). Or view this [large spreadsheet that I put up on Google Docs](#) (note that I did not compile this data, source is at the bottom of the spreadsheet).

And here is a [good guide on making VPNs more secure](#).

Random Note: I strongly recommend using wired connections for your internet connection at home as opposed to wireless. There have been many cases of government snooping by them breaking into networks and collecting wireless data. A classic example is the arrest of Iserdo, the creator of the Butterfly Botnet (Mariposa). Ultimately his arrest and conviction was solidified when Law

Enforcement broke into his Wireless Network and monitored him, gathering all the evidence necessary.

Browser Choice and Security

First things first, I will never recommend using Google Chrome and nothing any of you can say will change my mind on this.

[Firefox](#) is fast, reliable, open source and respects your privacy.

[Tor Browser](#) is your choice if you need an extra layer of anonymity. It's a modified version of Firefox, it comes with pre-installed privacy add-ons, encryption and an advanced proxy.

Browser Fingerprint - Is your browser configuration unique?

When you visit a web page, your browser voluntarily sends information about its configuration, such as available fonts, browser type, and add-ons. If this combination of information is unique, it may be possible to identify and track you without using cookies. EFF created a Tool called [Panoptick](#) to test your browser to see how unique it is.

WebRTC IP Leak Test - Is your IP address leaking?

WebRTC is a new communication protocol that relies on JavaScript that can leak your actual IP address from behind your VPN. While software like NoScript prevents this, it's probably a good idea to block this protocol directly as well, just to be safe.

For Google Chrome users: There is no known working solution, only a plugin that is easily circumvented. Please use Firefox instead.

For Firefox users: [\(Click to View\)](#)

Code How to disable WebRTC in Firefox?

In short: Set "media.peerconnection.enabled" to "false" in "about:config".

Explained:

Enter "about:config" in the firefox address bar and press enter.

Press the button "I'll be careful, I promise!"

Search for "media.peerconnection.enabled"

Double click the entry, the column "Value" should now be "false"

Done. Do the WebRTC leak test again.

If you want to make sure every single WebRTC related setting is really disabled change these settings:

```
media.peerconnection.turn.disable = true
media.peerconnection.use_document_iceservers = false
media.peerconnection.video.enabled = false
media.peerconnection.identity.timeout = 1
```

Now you can be 100% sure WebRTC is disabled.

[Test for WebRTC leaks here.](#)

Improve your security with these Firefox add ons

[Stop tracking with "Disconnect"](#)

Founded in 2011 by former Google engineers and a consumer-and privacy-rights attorney. The addon is open source and loads the pages you go to 27% faster and stops tracking by 2,000+

third-party sites. It also keeps your searches private.

[Block Ads with "uBlock Origin"](#)

An efficient wide-spectrum-blocker that's easy on memory, and yet can load and enforce thousands more filters than other popular blockers out there. It has no monetization strategy and is completely open source. We recommend FireFox but uBlock Origin also works in other browsers such as Safari, Opera, and Chromium. Unlike AdBlock Plus, uBlock does not allow so-called "acceptable ads".

[Hinder Browser Fingerprinting with "Random Agent Spoofer"](#)

A privacy enhancing firefox addon which aims to hinder browser fingerprinting. It does this by changing the browser/device profile on a timer.

[Automatically Delete Cookies with "Self-Destructing Cookies"](#)

Automatically removes cookies when they are no longer used by open browser tabs. With the cookies, lingering sessions, as well as information used to spy on you, will be expunged.

[Encryption with "HTTPS Everywhere"](#)

A Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. A collaboration between The Tor Project and the Electronic Frontier Foundation.

[Block Content Delivery Networks with "Decentraleyes"](#)

Emulates Content Delivery Networks locally by intercepting requests, finding the required resource and injecting it into the environment. This all happens instantaneously, automatically, and no prior configuration is required. Source code: GitHub.

[Stop cross-site requests with uMatrix](#)

Many websites integrate features which let other websites track you, such as Facebook Like Buttons or Google Analytics. uMatrix gives you control over the requests that websites make to other websites. This gives you greater and more fine grained control over the information that you leak online.

[Be in total control with "NoScript Security Suite"](#)

Highly customizable plugin to selectively allow Javascript, Java, and Flash to run only on websites you trust. Not for casual users, it requires technical knowledge to configure.

[Content control with "Policeman"](#)

This addon has purpose similar to RequestPolicy and NoScript. It's different from the former in that it supports rules based on content type. For example, you can allow images and styles, but not scripts and frames for some sites. It can also be set up to act as a blacklist.

This is a collection of privacy related about:config tweaks. We'll show you how to enhance the privacy of your Firefox browser.

Code Preparation:

Enter "about:config" in the firefox address bar and press enter.
Press the button "I'll be careful, I promise!"
Follow the instructions below...

Getting started:

```
privacy.trackingprotection.enabled = true
```

This is Mozilla's new built in tracking protection.

`geo.enabled = false`
Disables geolocation.

`browser.safebrowsing.enabled = false`
Disable Google Safe Browsing and phishing protection. Security risk, but privacy improvement.

`browser.safebrowsing.malware.enabled = false`
Disable Google Safe Browsing malware checks. Security risk, but privacy improvement.

`dom.event.clipboardevents.enabled = false`
Disable that websites can get notifications if you copy, paste, or cut something from a web page, and it lets them know which part of the page had been selected.

`network.cookie.cookieBehavior = 1`
Disable cookies
0 = Accept all cookies by default
1 = Only accept from the originating site (block third party cookies)
2 = Block all cookies by default

`network.cookie.lifetimePolicy = 2`
cookies are deleted at the end of the session
0 = Accept cookies normally
1 = Prompt for each cookie
2 = Accept for current session only
3 = Accept for N days

`browser.cache.offline.enable = false`
Disables offline cache.

`browser.send_pings = false`
The attribute would be useful for letting websites track visitors' clicks.

`webgl.disabled = true`
WebGL is a potential security risk. Source

`dom.battery.enabled = false`
Website owners can track the battery status of your device. Source

`browser.sessionstore.max_tabs_undo = 0`
Even with Firefox set to not remember history, your closed tabs are stored temporarily at Menu -> History -> Recently Closed Tabs. Read these sources for more information on hardening FireFox:
<https://github.com/pyllyukko/user.js>
http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences

Email

Privacy Conscious Email Providers

[ProtonMail](#)

[CounterMail](#)

[NeoMailbox](#)

Email Clients:

[Mozilla Thunderbird](#) - Mozilla Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation. Thunderbird is an email, newsgroup, news feed, and chat (XMPP, IRC, Twitter) client.

[MailPile.is](#) (BETA) - A modern, fast web-mail client with user-friendly encryption and privacy features.

Privacy Email Tools

[gpg4usb](#) - A very easy to use and small portable editor to encrypt and decrypt any text-message or -file. For Windows and Linux.

[Mailvelope](#) - A browser extension that enables the exchange of encrypted emails following the OpenPGP encryption standard.

[Enigmail](#) - A security extension to Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

[TorBirdy](#) - This extension configures Thunderbird to make connections over the Tor anonymity network.

[Email Privacy Tester](#) - This tool will send an Email to your address and perform privacy related tests.

Email Alternatives

[Bitmessage](#)

Bitmessage is a P2P communications protocol used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need-not inherently trust any entities like root certificate authorities. It uses strong authentication which means that the sender of a message cannot be spoofed, and it aims to hide "non-content" data.

[I2P-Bote](#)

I2P-Bote is a fully decentralized and distributed email system. It supports different identities and does not expose email headers. Currently (2015), it is still in beta version and can be accessed via its web application interface or IMAP and SMTP. All bote-mails are transparently end-to-end encrypted and, optionally, signed by the sender's private key.

[RetroShare](#)

Retroshare creates encrypted connections to your friends. Nobody can spy on you. Retroshare is completely decentralized. This means there are no central servers. It is entirely Open-Source and free. There are no costs, no ads and no Terms of Service.

Privacy Respecting Search Engines

If you are currently using a search engines like Google, Bing or Yahoo you should pick an alternative here.

[DuckDuckGo](#) [[Tor Link](#)]

The search engine that doesn't track you. Some of DuckDuckGo's code is free software hosted at GitHub, but the core is proprietary. The company is based in the USA.

[Disconnect Search](#)

Search privately using your favorite search engine: Google, Yahoo, Bing and DuckDuckGo are available for selection. It masks your IP address, cookies, and other personal info.

[MetaGer](#)

A metasearch engine, which is based in Germany. It focuses on protecting the user's privacy. Supported by 24 own crawlers of small scale web search engines.

[ixquick.com](#)

Returns the top ten results from multiple search engines. It uses a "Star System" to rank its results by awarding one star for every result that has been returned from a search engine. Based in the USA and the Netherlands.

Password Managers

If you are currently using a password manager software like 1Password, LastPass, Roboform or iCloud Keychain you should pick an alternative here.

[Master Password - Cross-platform](#)

Master Password is based on an ingenious password generation algorithm that guarantees your passwords can never be lost. Its passwords aren't stored: they are generated on-demand from your name, the site and your master password. No syncing, backups or internet access needed.

[KeePass / KeePassX - Local](#)

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. All passwords in one database, which is locked with one master key or a key file. The databases are encrypted using the best and most secure encryption algorithms currently known: AES and Twofish. See also: KeePassX.

[Encryptr - Cloud Based - \(SpiderOak\)](#)

Encryptr is simple and easy to use. It stores your sensitive data like passwords, credit card data, PINs, or access codes, in the cloud. However, because it was built on the zero knowledge Crypton framework, Encryptr ensures that only the user has the ability to access or read the confidential information.

[Self Contained Networks](#)

[I2P Anonymous Network](#)

The Invisible Internet Project (I2P) is a computer network layer that allows applications to send messages to each other pseudonymously and securely. Uses include anonymous Web surfing, chatting, blogging and file transfers. The software that implements this layer is called an I2P router and a computer running I2P is called an I2P node. The software is free and open source and is published under multiple licenses.

[GNUnet Framework](#)

GNUnet is a free software framework for decentralized, peer-to-peer networking and an official GNU package. The framework offers link encryption, peer discovery, resource allocation, communication over many transports (such as tcp, udp, http, https, wlan and bluetooth) and various basic peer-to-peer algorithms for routing, multicast and network size estimation.

[The Freenet Project](#)

Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship. Both Freenet and some of its associated tools were originally designed by Ian Clarke, who defined Freenet's goal as providing freedom of speech on the Internet with strong anonymity protection.

[Tor Project](#)

Provides anonymity to websites and other servers. Servers configured to receive connections only through Tor are called hidden services.

[RetroShare](#)

Open Source cross-platform, Friend-2-Friend and secure decentralised communication platform.

[Domain Name System \(DNS\)](#)

[CloudNS - Service](#)

An Australian based security focused DNS provider. Features: DNSCrypt Support to provide confidentiality and message integrity, complete trust validation of DNSSEC enabled names, namecoin resolution of .bit domain names and no domain manipulation or logging.

[DNSCrypt - Tool](#)

DNSCrypt is a protocol for securing communications between a client and a DNS resolver. The DNSCrypt protocol uses high-speed high-security elliptic-curve cryptography and is very similar to DNSCurve, but focuses on securing communications between a client and its first-level resolver.

[OpenNIC - Service](#)

OpenNIC is an alternate network information center/alternative DNS root which lists itself as an alternative to ICANN and its registries. Like all alternative root DNS systems, OpenNIC-hosted domains are unreachable to the vast majority of the Internet. Only specific configuration in one's DNS resolver makes these reachable, and very few Internet service providers have this configuration.

[NoTrack](#)

A network-wide DNS server which blocks Tracking sites. Currently works in Debian and Ubuntu.

[Namecoin](#)

A decentralized DNS open source information registration and transfer system based on the Bitcoin cryptocurrency.

Encrypted Cloud Storage Services

If you are currently using a Cloud Storage Services like Dropbox, Google Drive, Microsoft OneDrive or Apple iCloud you should pick an alternative here.

Remember to manually encrypt your files before uploading them to the cloud!

Hosted

[Seafile](#) - 100 GB Storage for \$10/month

Seafile offers 100 GB Storage for \$10/month but also gives you the opportunity to host on your own server. Your data is stored in Germany or with Amazon Web Service in the US for the cloud version. Encrypt files with your own password.

[ownCloud](#) - Choose your hoster

Similar functionally to the widely used Dropbox, with the difference being that ownCloud is free and open-source, and thereby allowing anyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

[Least Authority S4](#) - For Experts

S4S4 (Simple Secure Storage Service) is Least Authority's verifiably secure off-site backup system for individuals and businesses. 100% client-side encryption and open source transparency. \$25/month for unlimited storage. Servers are hosted with Amazon S3 in the US.

Self Hosted

[Seafile](#)

Seafile is a file hosting software system. Files are stored on a central server and can be synchronized with personal computers and mobile devices via the Seafile client. Files can also be accessed via the server's web interface.

[Pydio](#)

Pydio is open source software that turns instantly any server (on premise, NAS, cloud IaaS or PaaS) into a file sharing platform for your company. It is an alternative to SaaS Boxes and Drives, with more control, safety and privacy, and favorable TCOs.

[Tahoe-LAFS](#)

Tahoe-LAFS is a Free and Open decentralized cloud storage system. It distributes your data across multiple servers. Even if some of the servers fail or are taken over by an attacker, the entire file store continues to function correctly, preserving your privacy and security.

[ownCloud](#) - Host your own

Similar functionally to the widely used Dropbox, with the difference being that ownCloud is free and open-source, and thereby allowing anyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

Related Information

[Cryptomator](#) - Free client-side AES encryption for your cloud files. Open source software: No backdoors, no registration.

Text and Video Messaging

Secure your text messages, Instant Messaging and Chat

[Pidgin](#) + [OTR](#) (Windows)

Pidgin is a popular free and open source IM client that lets you chat to users on AIM, Google Talk, MSN, Yahoo and many more. OTR (Off-the-road) is a plugin that combines AES encryption, perfect forward secrecy, and the SHA-1 hash function to ensure strong encryption for IM sessions. As with GnuPG for emails, initial setup is a bit of a pain, but once done operation is seamless (we now have a detailed guide for this).

Tox.im / Tox.chat is not a secure solution any longer. There is internal conflict between the devs, a break off with IP being stolen, and some devs claiming the NSA have been pushing bug fixes (open source) with exploits that allow them to monitor things. If anyone knows more about this, let me know. Information isn't very clear, but due to everything that has been happening, I would not trust my privacy with them.

[Adium \(OSX\)](#)

Adium is a free and open source messaging client for Mac that also lets you talk to friends on lots of different networks. Even better, Addium comes with OTR support built-in!

[TorChat](#)

[ChatSecure](#)

[SilentCircle](#)

[Surespot](#)

[Jitsi](#)

[Textsecure](#)

[Cryptocat](#)

Most info here is directly taken from PrivacyTools at this point.

Update 10/26/16

Thread will be updated in the coming days.
test

SUI-3183372 - August 16, 2016, 7:05 pm

(Aug 16, 2016 07:02 PM)Mr. Robot Wrote: [\[CITE\]](#) More than happy to delete my messages if you make a couple of posts to reserve space.

Yeah that would be great to be honest. These two posts should be enough for me. Everything after this should be fair game.

Update 10/26/16

Thread will be updated in the coming days.

? **[\$(1000)\$]** ? - August 16, 2016, 7:14 pm

Wow great thread brother!

5 Star and +repp'd

Mr. Robot - August 16, 2016, 7:21 pm

(Aug 16, 2016 07:05 PM)Previously Known As.... Wrote: [\[CITE\]](#) Yeah that would be great to be honest. These two posts should be enough for me. Everything after this should be fair game.

There you go mate. Hope that's enough room for ya to work with.

Zombie? - August 16, 2016, 7:22 pm

Thanks so much for this! Posting to come back to it later on :)

Koolsami7 - August 16, 2016, 9:52 pm

Lots of good information here, thanks!

Kyzr - August 17, 2016, 2:39 am

Read it through, it's a really good and informative thread for people who want to know more about privacy online, and it's really in depth too. Hands down one of the greatest I have seen in a long time ?

d000nt - August 17, 2016, 2:47 am

privacytools.io, you got that info from there right?

lorraine walsh - August 17, 2016, 2:58 am

i found this post to be thoroughly helpful. Online security is something that is a must nowadays. If you can't keep your data secure these days than the user is in serious trouble since there are many chances that hackers might be busy to crack your sensitive records. I personally for this reason use data encryption tools to lock my folders and for online privacy, I use some good vpn providers for say PureVPN. This gives me safer and secure browsing experience.

Eagle 95 - August 17, 2016, 3:11 am

Finally, got it bookmarked as a topic. Good job compiling all of it.

Description - August 17, 2016, 8:18 am

Thanks for the HQ info.

Should help people.

Erich Himmler - August 17, 2016, 2:33 pm

This is good info, but most of it could be bypassed on the local machine by Windows 10 Spying.

SUI-3183372 - August 17, 2016, 2:53 pm

(Aug 17, 2016 02:33 PM)Erich Himmeler Wrote: [\[CITE\]](#) This is good info, but most of it could be bypassed on the local machine by Windows 10 Spying.

When I post about OS's I'll mention why Windows 10 should never be used.

SUI-3183372 - August 17, 2016, 9:33 pm

(Aug 17, 2016 06:17 PM)Max The GOD Wrote: [\[CITE\]](#) For those of us who are curious now, what would you briefly say is the best OS to use?

If you have to use Windows, Windows 7.

I do recommend Linux Distro's though. I'm a gamer so my desktop is Windows 7, but everything else I own is Linux.

Debian is my OS of choice, although Qubes is a strong choice for those who are really security minded. Arch Linux is a good choice too, as it is light weight and if choosing the Parabola version, you have a completely open source version of Arch.

Finally, whatever your choice is, I recommend installing a VM on the machine using Whonix. Familiarizing yourself with Whonix is a good step towards ultimate security, but it is not for beginners, it takes work to set up.

~ Left HF For Good ~ - August 17, 2016, 11:33 pm

(Aug 17, 2016 09:33 PM)Previously Known As.... Wrote: [\[CITE\]](#) If you have to use Windows, Windows 7.

I do recommend Linux Distro's though. I'm a gamer so my desktop is Windows 7, but everything else I own is Linux.

Debian is my OS of choice, although Qubes is a strong choice for those who are really security minded. Arch Linux is a good choice too, as it is light weight and if choosing the Parabola version, you have a completely open source version of Arch.

Finally, whatever your choice is, I recommend installing a VM on the machine using Whonix. Familiarizing yourself with Whonix is a good step towards ultimate security, but it is not for beginners, it takes work to set up.

What about tails, would you recommend that OS?

meimei - August 18, 2016, 1:41 am

Hey bro can you do a one on one lesson with me I can pay

~ Left HF For Good ~ - August 18, 2016, 1:42 am

(Aug 18, 2016 01:41 AM)meimei Wrote: [\[CITE\]](#) Hey bro can you do a one on one lesson with me I can pay

Why not just read his thread very carefully? It has plenty of details, which should help you a ton.

SUI-3183372 - August 18, 2016, 3:44 am

(Aug 17, 2016 11:33 PM)ChilledWhiteHat Wrote: [\[CITE\]](#) What about tails, would you recommend that OS?

I have no TAILS experience personally, but I've heard good enough things and have seen smart enough people recommend it. Look at the four operating systems below, all can be launched off of a live cd or live usb.

[Tails](#)

Tails is a live operating system, that starts on almost any computer from a DVD, USB stick, or SD card. It aims at preserving privacy and anonymity, and helps to: Use the Internet anonymously and circumvent censorship; Internet connections go through the Tor network; leave no trace on the computer; use state-of-the-art cryptographic tools to encrypt files, emails and instant messaging.

[KNOPPIX](#)

KNOPPIX is an operating system based on Debian designed to be run directly from a CD / DVD (Live CD) or a USB flash drive (Live USB), one of the first of its kind for any operating system. When starting a program, it is loaded from the removable medium and decompressed into a RAM drive. The decompression is transparent and on-the-fly.

[Puppy Linux](#)

Puppy Linux operating system is a lightweight Linux distribution that focuses on ease of use and minimal memory footprint. The entire system can be run from RAM with current versions generally taking up about 210 MB, allowing the boot medium to be removed after the operating system has started.

[Tiny Core Linux](#)

Tiny Core Linux is a minimal Linux operating system focusing on providing a base system using BusyBox and FLTK. The distribution is notable for its size (15 MB) and minimalism, with additional functionality provided by extensions.

~ Left HF For Good ~ - August 19, 2016, 2:47 am

(Aug 18, 2016 03:44 AM)Previously Known As.... Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)

I have no TAILS experience personally, but I've heard good enough things and have seen smart enough people recommend it. Look at the four operating systems below, all can be launched off of a live cd or live usb.

[Tails](#)

Tails is a live operating system, that starts on almost any computer from a DVD, USB stick, or SD card. It aims at preserving privacy and anonymity, and helps to: Use the Internet anonymously and circumvent censorship; Internet connections go through the Tor network; leave no trace on the computer; use state-of-the-art cryptographic tools to encrypt files, emails and instant messaging.

[KNOPPIX](#)

KNOPPIX is an operating system based on Debian designed to be run directly from a CD / DVD (Live CD) or a USB flash drive (Live USB), one of the first of its kind for any operating system. When starting a program, it is loaded from the removable medium and decompressed into a RAM drive. The decompression is transparent and on-the-fly.

[Puppy Linux](#)

Puppy Linux operating system is a lightweight Linux distribution that focuses on ease of use and minimal memory footprint. The entire system can be run from RAM with current versions generally taking up about 210 MB, allowing the boot medium to be removed after the operating system has started.

[Tiny Core Linux](#)

Tiny Core Linux is a minimal Linux operating system focusing on providing a base system using BusyBox and FLTK. The distribution is notable for its size (15 MB) and minimalism, with additional

functionality provided by extensions.

Thanks, I to have heard good things about tails. And, quit frankly if someone is trying to maintain complete privacy I would recommend it, as I have heard many good things. Anyways, thanks for the feedback, well reply.

Extroit - August 22, 2016, 2:37 pm

Thanks for all the info , will apply all all this now. Thanks for the detailed thread OP

~ **Left HF For Good** ~ - August 22, 2016, 10:06 pm

(Aug 22, 2016 02:37 PM)Extroit Wrote: [\[CITE\]](#) Thanks for all the info , will apply all all this now. Thanks for the detailed thread OP

I am not OP, obviously but I like to see people thank some one for their hard word. ?

mistarp - October 18, 2016, 9:52 pm

can anybody tell me why lastpass isnt a good choice?

?**Criminal** - October 19, 2016, 5:34 pm

(Oct 18, 2016 09:52 PM)mistarp Wrote: [\[CITE\]](#) can anybody tell me why lastpass isnt a good choice? It's all stored in a centralized place if someone wanted to hack it again they will, it's been compromised once before but the database is super private and all the passes are useless anyways it would only be good for emails at this point.

Mi2414 - October 19, 2016, 5:38 pm

Really wanna setup NoScript but running into trouble, can I Pm you about this?

Forc?d - October 19, 2016, 5:43 pm

Did a fast read thru, looks all go. however i think i would remove TrueCrypt completely as its basically poses a security risk.

VeraCrypt is basically the same but with the latest security/bug fixes and dedicated dev's updating it.

Eternal. - October 19, 2016, 8:49 pm

A VPN is a good idea, careful browser settings and wired networking are great as well. I would also recommend you use XMPP Off The Record for communication.

<http://hack.training/setup-xmpp-off-the-record/>

HIGH PAID FELLA - October 21, 2016, 1:56 pm

Use multiple VPN's and instances of TOR by virtualizing, use Qubes and encrypt EVERYTHING. From live communication to data, I make use of VeraCrypt (hidden volume for plausible deniability). Then be paranoid and in case someone busts down your door plug out everything so it's useless at its current state, don't share personal information, don't share pictures, videos and metadata leaking piece of shits such as smartphones.

METADATA is one of the most dangerous threats, don't know what it is? Imagine someone calling the suicide line at a specific time and looking back his location was near a high bridge. You don't need to know the content of conversation to know what was going on.

Don't fall into honeypots, use secure mediums such as specific forums which are hosted in the CIS (RU mainly) and/or are reputable such as darknet markets. Don't fall into new revolutionary markets or sites. They might be traps depending how big of a fish you are.

Also don't try to be the smartass to setup your own services/servers and then to notice after it has been vulnerable to whatever I know what.

I would personally only use bitcoin as payment as it's easy to move and sell. The price is stable and is a currency not just known to be used for criminals (such as Monero, which I personally avoid). Mix every payment, use different addresses and host your wallet locally (and back-up your private keys somewhere safe and encrypted).

This was kinda one of the most important points I wanted to discuss.

?Criminal - October 21, 2016, 4:58 pm

(Oct 21, 2016 01:56 PM)Rabby Racks Wrote: [\[CITE\]](#) Use multiple VPN's and instances of TOR by virtualizing, use Qubes and encrypt EVERYTHING. From live communication to data, I make use of VeraCrypt (hidden volume for plausible deniability). Then be paranoid and in case someone busts down your door plug out everything so it's useless at its current state, don't share personal information, don't share pictures, videos and metadata leaking piece of shits such as smartphones.

METADATA is one of the most dangerous threats, don't know what it is? Imagine someone calling the suicide line at a specific time and looking back his location was near a high bridge. You don't need to know the content of conversation to know what was going on.

Don't fall into honeypots, use secure mediums such as specific forums which are hosted in the CIS (RU mainly) and/or are reputable such as darknet markets. Don't fall into new revolutionary markets or sites. They might be traps depending how big of a fish you are.

Also don't try to be the smartass to setup your own services/servers and then to notice after it has been vulnerable to whatever I know what.

I would personally only use bitcoin as payment as it's easy to move and sell. The price is stable and is a currency not just known to be used for criminals (such as Monero, which I personally avoid). Mix every payment, use different addresses and host your wallet locally (and back-up your private keys somewhere safe and encrypted).

This was kinda one of the most important points I wanted to discuss.

Yeah honeypots tend to get even the savvy people to fall from anonymity.

SUI-3183372 - October 21, 2016, 11:54 pm

(Oct 21, 2016 01:56 PM)Rabby Racks Wrote: [\[CITE\]](#) I make use of VeraCrypt (hidden volume for plausible deniability).

I've always wondered about True Crypt and VeraCrypts plausible deniability claims. In small cases, I believe you'll be fine and it will hold up in a court. In large cases against a government who really wants to bring you down, I don't think TrueCrypts/VeraCrypts claims of plausible deniability are accurate.

Researchers at the University of Washington teamed up with Bruce Schneier, the god of cryptography, and basically broke the claims that TrueCrypt were making regarding plausible deniability. You can read the full paper here:

<https://www.schneier.com/academic/paperfiles/paper-truecrypt-dfs.pdf>

Essentially, "even when the file system may be deniable in the pure, mathematical sense, we find that the environment surrounding that file system can undermine its deniability ..."

Another good read on the subject that leads me to believe plausible deniability may be broken:

<https://defuse.ca/truecrypt-plausible-deniability-useless-by-game-theory.htm>

Conor McGregor™ - October 22, 2016, 7:50 pm

Very interesting read.. Thanks for sharing this.

Prominent - October 22, 2016, 9:20 pm

Just read it. There's a lot of information I didn't know. Do you plan on keeping this thread updated?

SUI-3183372 - October 22, 2016, 9:40 pm

(Oct 22, 2016 09:20 PM)Prominent. Wrote: [\[CITE\]](#) Just read it. There's a lot of information I didn't know. Do you plan on keeping this thread updated?

Calculus and Physics are kicking my ass right now so I haven't been updating my threads. I'll do so in the future though.

Ghotst_honey - October 22, 2016, 9:44 pm

How can I withdrawal from subscriptions and websites if I don't remember all of them? Is there a way to find all of them through an associated email?

When I was younger I've joined a lot of websites.

I'm looking to remove myself from as much history as I can if it's possible.

SUI-3183372 - October 22, 2016, 9:59 pm

(Oct 22, 2016 09:44 PM)Ghotst_honey Wrote: [\[CITE\]](#) How can I withdrawal from subscriptions and websites if I don't remember all of them? Is there a way to find all of them through an associated email?

When I was younger I've joined a lot of websites.

I'm looking to remove myself from as much history as I can if it's possible.

Maybe log into that email and search for 'unsubscribe' but I'm not really sure.

Rubixa - October 26, 2016, 2:18 am

A well deserved sticky my friend :)

xX_l337_h4x0r_Xx - October 26, 2016, 10:49 am

This is the thread that gets a sticky? Seriously?

SUI-3183372 - October 26, 2016, 7:05 pm

(Oct 26, 2016 10:49 AM)xX_l337_h4x0r_Xx Wrote: [\[CITE\]](#) This is the thread that gets a sticky? Seriously?

As compared to..?

It is what it is. [I pushed for a sub-forum](#), I got a sticky. It works though, I'd like to try to influence higher quality discussion in this sub-forum.

If people have good content and want to collaborate on this thread, I'm willing to work with them.

Retribute - October 27, 2016, 12:14 am

(Aug 17, 2016 02:47 AM)riu_neo Wrote: [\[CITE\]](#) privacytools.io, you got that info from there right?

(Aug 17, 2016 01:05 PM)Previously Known As.... Wrote: [\[CITE\]](#) Yes, and related sites that they suggest. I'll be branching out a bit, but their info will always be a central theme.Right. Then why haven't you cited privacytools.io as a source? ?

Because at the end of the day that is where you are drawing most of this thread's content from thus far.

lagos - October 27, 2016, 12:20 am

hi how are you? am bula and wil like to know about kazy crypter

SUI-3183372 - October 27, 2016, 12:23 am

(Oct 27, 2016 12:14 AM)Retribute Wrote: [\[CITE\]](#) Right. Then why haven't you cited privacytools.io as a source? ?

Because at the end of the day that is where you are drawing most of this thread's content from thus far.

You're coming off as if I'm trying to hide that?

Not sure if you've seen this (<https://i.imgur.com/HfZIJiM.png>), but I'm happy to admit that pt.io is and will always be a great place to gain information on this subject. They'll most certainly always be a heavy influence on this specific thread.

Give it a week, the thread will have a major overhaul and I'll make it a bit more clear where information comes from. However, I will not have a credits section, as it'd be absolutely massive and I state clearly this is a compilation of data from numerous sources. Never once will I claim any of this work as my own. The first sentence of the OP states:

Quote: This is a broad topic and most of this information isn't coming directly from me, rather it is being compiled from multiple sources. I won't take credit for anything.

Retribute - October 27, 2016, 12:34 am

(Oct 27, 2016 12:23 AM)Previously Known As.... Wrote: [\[CITE\]](#) You're coming off as if I'm trying to hide that?

Not sure if you've seen this (<https://i.imgur.com/HfZIJiM.png>), but I'm happy to admit that pt.io is and will always been a great place to gain information on this subject.

Give it a week, the thread will have a major overhaul and I'll make it a bit more clear where information comes from. However, I will not have a credits section, as it'd be absolutely massive and I state clearly this is a compilation of data from numerous sources. Never once will I claim any of this work as my own. The first sentence of the OP states: Yes, I am. And no, I don't want to see it that way because I'm sure you have a lot of knowledge to spread. I simply see no reason for you to not use up a line or two to post your source. Even the structure of your post highly resembles PT's. It's an injustice to not give credits to them.

Yes I've seen those quotes in your image. In fact that's exactly what I quoted in my initial reply.

Stating you're compiling data from numerous sources without giving credit is a disservice. Perhaps it's passable if the information is fragmented in numerous sources, but the fact that you're drawing such a vast amount of content from a single source should warrant a cite.

SUI-3183372 - October 27, 2016, 12:48 am

(Oct 27, 2016 12:34 AM)Retribute Wrote: [\[CITE\]](#) Yes, I am. And no, I don't want to see it that way because I'm sure you have a lot of knowledge to spread. I simply see no reason for you to not use up a line or two to post your source. Even the structure of your post highly resembles PT's. It's an injustice to not give credits to them.

The OP can not fit a single additional character, it's literally full. It wasn't until last night that multiple posts were deleted from this thread so I could have the top 3 posts.

(Oct 27, 2016 12:34 AM)Retribute Wrote: [\[CITE\]](#) Yes I've seen those quotes in your image. In fact that's exactly what I quoted in my initial reply.

Stating you're compiling data from numerous sources without giving credit is a disservice. Perhaps it's passable if the information is fragmented in numerous sources, but the fact that you're drawing such a vast amount of content from a single source should warrant a cite.

Maybe I'll consider a credits sections once everything is done, considering there is room for it, but expect the trend of using PT.io primarily to end. There is more from that site that I'll make use of, but

the next two posts will have a lot more specific content, and won't be as broad. The main OP will never have a credits sections, I won't remove info to make room for it, and stating sources will simply be included in a follow up post.

I missed these posts, sorry.

(Oct 19, 2016 05:38 PM)Amidst Wrote: [\[CITE\]](#) Really wanna setup NoScript but running into trouble, can I Pm you about this?

Yes, feel free to PM me any time. I also sit in your Discord server, just kind of waiting to see topics I can contribute to. You can message me there. My name is Priv8.

(Oct 19, 2016 05:43 PM)Forc?d Wrote: [\[CITE\]](#) Did a fast read thru, looks all go. however i think i would remove TrueCrypt completely as its basically poses a security risk.

VeraCrypt is basically the same but with the latest security/bug fixes and dedicated dev's updating it.

You're right. All mentions of TrueCrypt will be removed. I just haven't been around through out the development of VeraCrypt, I went away right before TrueCrypt reached EoL. Using TrueCrypt in present day opens you to numerous security risks and should be avoided.

Designer - October 27, 2016, 1:10 am

Good thread, posting to come back to it.

SUI-3183372 - October 27, 2016, 1:38 am

By using encryption you are only protecting what already belongs to you.

Conor McGregor™ - October 27, 2016, 9:00 pm

Really interesting read. Thanks for sharing this brother.

????? - October 29, 2016, 8:07 am

Why is ownCloud in the list of Encrypted Cloud Storage Services twice?

Pretty sure that's not intentional :)

Great post! Bookmarking this.

SUI-3183372 - October 29, 2016, 10:50 am

(Oct 29, 2016 08:07 AM)Gryff Wrote: [\[CITE\]](#) Why is ownCloud in the list of Encrypted Cloud Storage Services twice?

Pretty sure that's not intentional :)

Great post! Bookmarking this.

I didn't make it clear enough. Encrypted Cloud Storage is split into two sections. Hosted, and Self Hosted. OwnCloud falls under both categories, as you can host it yourself on your own server/hardware, or you can have one of the providers host it for you ([List of providers](#)).

SteinX - October 29, 2016, 3:45 pm

Thank you for creating this thread, exactly what I needed. I wish there would be a way to save all the text + links

Heartfire - October 30, 2016, 9:22 am

Thanks for the Thread, might need some of the tools listed that i don't have yet some day.

waltsai - November 2, 2016, 8:19 pm

Thank you very much. I will read it again.

soft_boy - November 4, 2016, 2:52 am

Thanks man this really help

fannas1 - November 4, 2016, 2:59 am

Interesting, thank you. Will come back and read when I need to.

xfiler - November 4, 2016, 5:21 pm

5/5 star thread, thank you very much buddy! learned alot.

Riggs - November 4, 2016, 5:26 pm

Bookmarked this thread. Thought I was familiar with most privacy-centric services in the online market until I saw this. Quite a few mentioned that I wasn't aware of or never properly considered. Appreciate the insight.

?now - November 4, 2016, 5:36 pm

Great post man, HQ as always!

Blxck - November 5, 2016, 5:11 am

Lots of good information here, thanks!

SkriptSkiddies - November 5, 2016, 8:43 am

I want to stay hidden and under the radar. While streaming i get booted offline and it's quite frustrating. I understand i need a vpn, but it seems all free vpns aren't strong enough to withstand some of the people who stress me. I'd also just like to be protected in general. Any help would be greatly appreciated due to the fact I'm new to this side of the world.

Thanks for the help!

Wakka - November 5, 2016, 8:46 am

Excellent high quality post, really enjoyed reading this. Thanks OP +3 later.

johnripper - November 6, 2016, 1:47 am

Sorry to say you no one can stay anonymous.

No one.

How much you try to hide

One fine day they will caught you

pahapoika91 - November 7, 2016, 1:05 am

Mega aint safe cloud storage?

SUI-3183372 - November 7, 2016, 9:14 am

(Nov 7, 2016 02:05 AM)pahapoika91 Wrote: [\[CITE\]](#) Mega aint safe cloud storage?

No.

Lot's of controversy over the ownership of mega and what they're going to do with the site:

<https://torrentfreak.com/kim-dotcom-warns-mega-users-to-backup-their-files-160421/>

<http://www.wired.co.uk/article/kim-dotcom-mega-3>

ArabKat - November 9, 2016, 7:10 am

Thanks bro! This thread has been a big help to protecting my privacy!

equi_gonzales13 - November 11, 2016, 4:59 pm

Great work! Thank you for investing all that time to create this thread. You really helped me find out things i didn't know.

I would like your opinion on this: Do you think that browsing through "Tor" is enough for all the "Browser Choice and Security" steps to be omitted??

Keep up the good work..

Luciferum - November 12, 2016, 11:17 am

This HQ thread will help a lot of people, thanks.

TabbyTeCat - November 12, 2016, 8:40 pm

this is a great post. but as many people point out anonymity is not really achievable. there are extra precautions you can take like listed in this post but if you are on the internet you cant be anonumus. but for beginners trying to hide there going on's this is a brilliant start

pahapoika91 - November 13, 2016, 3:47 am

Is startpage.com good search engine?

SaintJimmy - November 13, 2016, 5:45 am

A good lot of information you've here. Most of your arguments are really convincing. I'll be making sure that I go through most of these and implement them when I do a clean OS install on my Laptop.

SUI-3183372 - November 13, 2016, 7:21 pm

(Nov 13, 2016 04:47 AM)pahapoika91 Wrote: [\[CITE\]](#) Is startpage.com good search engine? Yes, I would recommend them.

However, there is discussion going on right now regarding the way startpage serves Google's ads. As of two weeks ago, identifying browser information was been sent back to Google. I don't know Startpage's stance on this, and if it will be fixed.

reonordo - November 15, 2016, 3:33 pm

One of the best and well thoroughly written threads I've seen. Great job. ?

yaropolk - November 15, 2016, 11:45 pm

Thanks Frd, which is very helpful to me for anonymously surffing on internet, and i got new application,softwares nad technic by this post

user088 - November 18, 2016, 11:56 am

This is good info, but most of it could be bypassed

bzr? - November 18, 2016, 5:48 pm

This thread has been incredible informative to me, thank-you for writing it.

I had a question about the password managers; I'm currently using 1Password, what security issues lie with this in your opinion, and why should I choose an alternative like Encryptr?

SpiritMind - November 22, 2016, 3:59 pm

Greetings! I've been going through your information here and following steps. This is a great thread. I would like to thank you for taking the time to put this together!

However, it may be a little out of date as of 11/22/2016.

Here is what I have gathered so far.

Browser Choice and Security

Quote:Automatically Delete Cookies with "Self-Destructing Cookies" -
addons.mozilla.org/firefox/addon/self-destructing-cookies

Works with Firefox 38.0a1 - 51.*

Quote:Block Content Delivery Networks with "Decentraleyes" -
addons.mozilla.org/firefox/addon/decentraleyes

Works with Firefox 38.0a1 - *

Quote:Stop cross-site requests with uMatrix - addons.mozilla.org/firefox/addon/umatrix
Works with Firefox 24.0 - 46.0

Quote:Be in total control with "NoScript Security Suite" - addons.mozilla.org/firefox/addon/noscript
Works with Firefox 45.0 - *

Quote:Content control with "Policeman" - addons.mozilla.org/firefox/addon/policeman%20
Works with Firefox 29.0 - 43.*

There is the ability to 'Download Anyways' with all of these add-ons. Is this the action I should take?

In the second about:config coding and explanation, this is what I found to no longer be available.

Quote:browser.safebrowsing.enabled = false

Disable Google Safe Browsing and phishing protection. Security risk, but privacy improvement.

This is what I've found so far. If I find anything else in the process of finishing this tutorial I'll be sure to add it to this post.

Thanks again!

SUI-3183372 - November 22, 2016, 7:33 pm

(Nov 22, 2016 04:59 PM)SpiritMind Wrote: [\[CITE\]](#) Greetings! I've been going through your information here and following steps. This is a great thread. I would like to thank you for taking the time to put this together!

However, it may be a little out of date as of 11/22/2016.

Here is what I have gathered so far.

Browser Choice and Security

Works with Firefox 38.0a1 - 51.*

Works with Firefox 38.0a1 - *

Works with Firefox 24.0 - 46.0

Works with Firefox 45.0 - *

Works with Firefox 29.0 - 43.*

There is the ability to 'Download Anyways' with all of these add-ons. Is this the action I should take?

In the second about:config coding and explanation, this is what I found to no longer be available.

This is what I've found so far. If I find anything else in the process of finishing this tutorial I'll be sure to add it to this post.

Thanks again!

Where are you seeing those warnings?

I went to those pages and they seem fully up to date for me.

They all work as intended currently anyways.

dean094 - November 23, 2016, 11:26 am

thanks a lot of information about being secure.

RedstoneMC - November 24, 2016, 1:46 pm

Wow nice info!

I think I need to bookmark this :)

blacktern - November 24, 2016, 1:58 pm

Very useful information thank you.

Toxic Impact - November 24, 2016, 5:10 pm

very usefull thanks looks good

Backopy - November 24, 2016, 8:55 pm

It'd be nice if you added TAILS to this.

Awesome stuff

SUI-3183372 - November 24, 2016, 10:01 pm

(Nov 24, 2016 09:55 PM)Backopy Wrote: [\[CITE\]](#) It'd be nice if you added TAILS to this.

Awesome stuff

Ran out of room in the OP and haven't finished with the 2nd post yet.

TAILS is mentioned in post #21 for now:

<https://hackforums.net/showthread.php?tid=5377222&pid=52133519#pid52133519>

Quote:[Tails](#)

Tails is a live operating system, that starts on almost any computer from a DVD, USB stick, or SD card. It aims at preserving privacy and anonymity, and helps to: Use the Internet anonymously and circumvent censorship; Internet connections go through the Tor network; leave no trace on the computer; use state-of-the-art cryptographic tools to encrypt files, emails and instant messaging.

[KNOPPIX](#)

KNOPPIX is an operating system based on Debian designed to be run directly from a CD / DVD (Live CD) or a USB flash drive (Live USB), one of the first of its kind for any operating system. When starting a program, it is loaded from the removable medium and decompressed into a RAM drive. The decompression is transparent and on-the-fly.

[Puppy Linux](#)

Puppy Linux operating system is a lightweight Linux distribution that focuses on ease of use and minimal memory footprint. The entire system can be run from RAM with current versions generally taking up about 210 MB, allowing the boot medium to be removed after the operating system has started.

[Tiny Core Linux](#)

Tiny Core Linux is a minimal Linux operating system focusing on providing a base system using BusyBox and FLTK. The distribution is notable for its size (15 MB) and minimalism, with additional functionality provided by extensions.

Legionhoster - November 25, 2016, 1:07 am

Good. Thank you for sharing such a wonderful information with us.

worldwindows - November 30, 2016, 1:20 pm

Thanks so much for this! Posting to come back to it later on :)

k0spwn - December 11, 2016, 2:59 am

Thanks a lot for this guide, it's well written and very useful !

eSiaEZmQ - December 18, 2016, 1:02 am

Useful thread, keep it updated !

Morozevich83 - December 19, 2016, 9:54 am

This is really interesting and useful, i'll try to learn from this and improve my privacy level and other stuff aswell

SUI-3183372 - December 19, 2016, 10:29 pm

(Dec 18, 2016 02:02 AM)H3lios Wrote: [\[CITE\]](#) Useful thread, keep it updated !

Yeah, I had been meaning to update the entire thread but uni and finals got in the way. I've never spent so much time studying in my life. On winter break now, I'll make some necessary changes.

TrueCrypt has been removed as per your PM.

Default08 - December 21, 2016, 7:56 am

Is there any way that you could help me use VeraCrypt? My Discord is: Flexx#8378

Sundaybest - December 21, 2016, 8:43 am

Amazing, so helpful! Thank you :)

DoxProxy - December 22, 2016, 9:50 pm

Lots of good info here man thank you HQ post!

jahrasta - December 24, 2016, 4:49 pm

Hello I made this post but found out I can't post links :(

pastebin.com/XavzDXhf

It is my alternative/overlap for chrome extensions I think it would be great to keep a thread updated of just extensions :)

girn10 - January 5, 2017, 2:45 pm

Good information and really helpful, thanks!

Xual - January 5, 2017, 4:14 pm

Is mega.co.nz safe to use? Great thread btw.

SUI-3183372 - January 5, 2017, 5:22 pm

(Jan 5, 2017 05:14 PM)Xual Wrote: [\[CITE\]](#) Is mega.co.nz safe to use? Great thread btw.

Mega is kind of sketchy. A Chinese corporation ousted Kim Dotcom and he's making claims that data stored there is not safe. May just be him being childish about losing the company though.

Nina.Lopez - January 6, 2017, 2:23 am

Thank you for posting this thread. This is exactly what everyone need to know nowadays. A must for computer security.

TAOofHacking - January 8, 2017, 6:58 pm

Very in-depth post, helped me a lot. Thnx M8 ?

Also, Cloudns seems to not be up anymore

frsnix - January 10, 2017, 6:31 am

Thank you for the post, I'm spending hours on it making sure that my computer bends to this very thread and what it showcases. Though, my question is; what do you think about Dashlane? Should I continue using it?

girn10 - January 10, 2017, 1:19 pm

such a useful thread. TYSM

xanity - January 10, 2017, 2:47 pm

I wish there would be a way to save all the text + links

SUI-3183372 - January 10, 2017, 8:05 pm

(Jan 10, 2017 03:47 PM)xanity Wrote: [\[CITE\]](#) I wish there would be a way to save all the text + links
If you quote the topic, you can pull all the links that way.

Oxyd - January 11, 2017, 5:52 am

Awesome detailed thread, thank you very much.

Actually posting here so that I can come back to take notes.

monkeybitch2 - January 11, 2017, 3:16 pm

damn bro great post and really helpfull!

pretty sure i am gonna use this!

volkhv0 - January 12, 2017, 9:06 am

Thank you for this! This is was an extremely helpful compilation.

bear18 - January 13, 2017, 9:34 am

which proxy can i use with hackforums? I'm struggling to find one hackforums is happy with.

CREEPLYHAPPY - January 13, 2017, 9:41 am

Thank you man, This is probably one of the best post on this site.

SUI-3183372 - January 14, 2017, 1:01 am

(Jan 13, 2017 10:34 AM)bear18 Wrote: [\[CITE\]](#) which proxy can i use with hackforums? I'm struggling to find one hackforums is happy with.

Can't help you there. Omni does not publicly reveal what is and is not allowed.

A9x3 - January 15, 2017, 4:16 pm

I have heard a lot about these tools secondhand but not fully understanding the purpose or usefulness. Thanks for the info!!!

ogbenjamin - January 18, 2017, 7:09 am

5 Star thread. Thanks OP.

?eptic - January 19, 2017, 8:49 am

This was a nice read. Thank you for this comprehensive and helpful thread. ?

browndev123 - January 19, 2017, 12:29 pm

Any way to log into a MMORPG with a different IP then mine?

SUI-3183372 - January 19, 2017, 6:36 pm

(Jan 19, 2017 01:29 PM)browndev123 Wrote: [\[CITE\]](#) Any way to log into a MMORPG with a different IP then mine?

Simple route, VPN.

JackRed - January 20, 2017, 8:45 am

The article was very informative and useful! Thank you! ?

Gizmo - January 20, 2017, 8:49 am

Posting to check back later. Thanks for the share.

Praet0rian - January 21, 2017, 2:13 am

Note to everyone concerning VeraCrypt, the system encryption feature ONLY WORKS on WINDOWS, for Linux you will need to use another program.

I personally only use open source programs for everything, and if it isn't open source, I run it inside a VM with a snapshot beforehand and no networking, and once I am done using it I revert back and nothing happened.

Learning416 - January 27, 2017, 8:10 pm

A ton of amazing useful information. Thank you

WeeZick - January 28, 2017, 5:05 pm

Very well written and done, thanks!

Toby Flenderson - January 29, 2017, 8:50 am

Well done! Thanks for the tips :)

F11 - January 30, 2017, 10:11 pm

I could definitely learn a lot from this. Thank you OP.

A NEW ERA... - February 4, 2017, 11:15 am

Just installed Ubuntu last night, and i've used this thread to harden my security, it's wonderful. Thanks.

zerocool1245 - February 5, 2017, 1:07 am

Yo bro, congratulations for your guide and for your hints, im really new to this and want to improve my privacy online. Thumbs up!!

goran84 - February 6, 2017, 2:23 am

What do you think is VeraCrypt better then BitLocker ?

tonypres - February 8, 2017, 11:34 pm

Really good post. It's a great starting point for anyone looking to get into this. The right tools, good preparation and an overview of the principles. Solid. Thanks a lot. ??

LadybirdMilkshake - February 11, 2017, 6:19 am

A lot of great information that someone with a tech background or not can understand and utilise to have better privacy online and offline! Thank you for all your effort.

gitclone - February 26, 2017, 6:03 am

riseup.net not mentioned?

I think that it deserves spot on the list

SUI-3183372 - February 26, 2017, 3:28 pm

(Feb 26, 2017 07:03 AM)gitclone Wrote: [\[CITE\]](#) riseup.net not mentioned?

I think that it deserves spot on the list

Riseup data is not yet encrypted on their servers. Right now, as of Feb 16, 2017, all new accounts that register on Riseup will now have their email data encrypted, but existing accounts still do not. Until the storage of mail on Riseup's servers becomes more secure, I'd prefer not to list them.

Quote:We have taken action to ensure that Riseup never again has access to a user's stored email in plaintext. Starting today, all new Riseup email accounts will feature personally encrypted storage on our servers, only accessible by you. In the near future, we will begin to migrate all existing accounts to use this new system.

To be absolutely clear, this type of encryption is not end-to-end message encryption. With Riseup's new system, you still put faith in the server while you are logged in. For full end-to-end email encryption, as before, you must use a client that supports OpenPGP (and is not web-based).

The Kraken - February 26, 2017, 3:33 pm

Thanks for sharing this too the community, really cool man. Btw I love that quote on the beginning. Golden words from Mr. Snowden.

gitclone - February 27, 2017, 5:08 am

I think that atleast riseup.net should be mentioned as great VPN.

Black uses AES-128-CBC. It's free and it comes with 23-download and 18-upload.
(It needs to be used with Bitmask tho)

Red will use AES-128-CBC. (Should work with even better encryption) when the OpemVPN 2.4 will

come for Debian.

Works with OpenVPN and comes with 32-download and 27-upload.

It's also free but requires 2-invitations.

Riseup doesnt keep logs ("but we do keep a record of which users accounts have used the VPN on which days.")

fatal-bert - March 1, 2017, 12:10 pm

this is awesome thank you

true4life - March 2, 2017, 7:57 am

Thanks for this my man.!!

Bigbadjohn - March 2, 2017, 2:25 pm

I have been looking at Tails, it doesn't look that easy to download requiring 2 USB's but wondered how secure it is and how big is the privacy/use ability trade off? Thanks guys and gals

Check The Name - March 3, 2017, 8:57 pm

Great high quality thread. I've seen it before, but never bothered posting.

thelou - March 6, 2017, 10:37 pm

(Mar 2, 2017 03:25 PM)Bigbadjohn Wrote: [CITE](#) I have been looking at Tails, it doesn't look that easy to download requiring 2 USB's but wondered how secure it is and how big is the privacy/use ability trade off? Thanks guys and gals

Nah, just guys

Reaperofhell666 - March 7, 2017, 7:25 am

Thank you, I found this very interesting and plan on using this information in the future.

PhalleN - March 7, 2017, 7:27 am

A lot of this comes down to common sense and being smart when using the internet. Very good thread however, I enjoyed the read and learned a thing or two.

bgd1988 - March 7, 2017, 12:47 pm

I knew a bit of this and learned what I didn't know from this. A great post man!

xreD - March 8, 2017, 9:43 am

very helpful stuff man...

thanks a ton for taking time to write all this :)

After reading this I feel like stupid af that i use chrome, gmail etc shit, Although I dont do anything related to hacking or any thing like that...

leastway - March 10, 2017, 4:20 am

Thanks for the useful and well compiled information.

Keep up the good work.

bdawn - March 21, 2017, 11:51 am

Hope I won't get in trouble for bumping this but I just wanted to say that I really enjoyed how you formatted and layed this all out. Keep it coming :)

abbyz_l337bb - April 4, 2017, 7:32 pm

Great thread! Lots of useful information and I have a new list of programs to install!!! Thanks heaps ?

rome1 - April 5, 2017, 8:59 am

Perfect! This helped me a lot.

I thank people like you who share his knowledge

asdoqew1 - April 9, 2017, 7:34 am

Thanks for such important and well explained thread. Everybody should think about this topic nowadays.

FelixTheCat - April 11, 2017, 5:04 am

Thanks for this guide! Really helpful, +1

Hipricedlowlife - April 19, 2017, 1:18 pm

Awesome thread it is well put together and had some stuff i have not seen before. 5 star post and i would +rep if i had the access to.

ß|?cksí-í?d?w™ - April 19, 2017, 7:10 pm

best guide ever , thank you PKS ?

__khan__ - April 20, 2017, 3:32 am

Thank you for the Information.

Encyclic - April 23, 2017, 8:14 am

Great thread full of useful information to use and put into practice from now on!

Memoranda - April 24, 2017, 7:57 pm

Hey, thank you for sharing this info. I was considering taking a "class" on this type of info about privacy and anonymity. Thanks again !! Extremely useful

kileraptor1 - April 30, 2017, 2:09 pm

Hello,

What is your opinion on Keybase?

Regards,

kileraptor1

Ghostzapper - May 1, 2017, 8:28 pm

Excellent Info. Much appreciated.

SUI-3183372 - May 1, 2017, 10:03 pm

(Apr 30, 2017 02:09 PM)kileraptor1 Wrote: [\[CITE\]](#) Hello,

What is your opinion on Keybase?

Regards,

kileraptor1

Not a fan anymore. I don't trust uploading my private key to their website, a feature that should not exist.

They had an opportunity to make a revolutionary chat client, then chose not to.

Quote:Does this use PGP?

No. Even if you have a PGP key on your Keybase profile, these messages are only encrypted with your Keybase device + paper keys. People aren't so great at managing and moving PGP private

keys around, so PGP keys are not included in our chat or filesystem. You can read more about our key model [here](#).

The basic idea here is that non-technical people won't get confused and do something irresponsible. (emphasis mine)

This makes it no different than Telegram, Vox, etc. And those are already established. They also collect more meta data than I'm happy with.

skynet7 - May 11, 2017, 10:27 am

WoW!!

Thats graet info!

Thank you so much!

pokego709 - May 13, 2017, 2:07 pm

Wow this is great, glad I found this.

SerCoDev - May 14, 2017, 7:41 am

Great Post. I would like to contribute to this post with 3 additions.

Block adds with:

EFF's Privacy Badger: a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it's like you suddenly disappeared.

Free

Encrypted Cloud Storage

Spideroak are very active as a company advocating for privacy and security. They advertise that they have no knowledge of their users content because it stores encrypted files that only you can decrypt. They also sponsor/sign most (if not all) of the EFF's Petitions.

Full encryption

21 day free trial (no cc needed)

Secure chat: also offered by spideroak is a service called 'semaphor' that features:

- Password-less design for added security
- Unlimited teams & channels
- Join with email address or a username
- Every message & file is cryptographically secure
- Always-available offline mode
- Large file support, up to 2 GB
- Open Source

Free / premium options starting at \$9m

StackFramed - May 14, 2017, 8:44 am

Amazing tutorial. Haven't heard of some of those Firefox plugins before, might give them a try.

IzumiChan - May 16, 2017, 11:02 am

Subscribed to this thread!

Thank you for taking the time to put this together I appreciate it!

goondu - May 18, 2017, 6:15 am

is this combo good enough?

noscript and ublock

zephyrs - May 19, 2017, 6:09 am

DNSleaktest.com is also a good site for testing for DNS leaks while using your VPN.

Forgot to mention. There's another good tool out there for maintaining privacy. Although it falls under the heading of a privacy tool, it's actually more of an anti-profiling tool.

For those of you who might have run/used a cypherpunk/mixmaster remailer back in the day, (I ran one from 1999 to 2000), your familiar with the concept of "chaff" and "decoys." Chaff/decoys were simply null emails, created in a random fashion, that were encrypted and sent along to X number of remailers in a chain. By "gunking up the pipeline" with legit looking garbage, it increased the difficulty of tracking the emails that people didn't want tracked.

There's a plug for Firefox (and I believe Chrome) which uses the same concept with search engines. It's called "TrackMeNot," something I've been using for a while. Essentially, every time you boot up your browser, it fetches a list of current keywords and phrases (to add to its persistent and evolving cache) from news/RSS feeds which you can configure. It will use these keywords and phrases to generate random searches on Google, Bing and Yahoo (you can select search engines you want or don't want to use). You can also select the timing of the searches from 1 per hour, to 10 per minute. It can also use a "burst search" feature, to help thwart algorithms which might try to detect automated search queries.

There's a number of other interesting features as well, such as an option to NOT use keywords which are monitored by DHS, etc. An astute coder can increase its functionality. Might be worth a look.

cs.nyu.edu/trackmenot/
addons.mozilla.org/en-US/firefox/addon/trackmenot/

BravoAlpha - May 20, 2017, 4:30 pm

Effectively, clearly and simply! Thks!

wolker - May 22, 2017, 2:53 pm

It's incredible how much: google chrome, firefox and other browser provide informations to be able to be tracked

why i have to become crazy and implement a series of behaviors, when our browsers can help us by avoiding make available lot of detailed informations.. (starting to cite the fingerprint)

ninjutsu - June 1, 2017, 5:11 pm

PM me about this thread, please? Have some questions.

SUI-3183372 - June 1, 2017, 7:03 pm

(Jun 1, 2017 05:11 PM)ninjutsu Wrote: [\[CITE\]](#) PM me about this thread, please? Have some questions.

You can't PM until you have 25 posts. Ask your questions here I suppose.

FPrism - June 5, 2017, 3:31 am

Very usefull, Thank you so much..

Etataglia12 - June 12, 2017, 7:03 am

Awesome info there. Thanks!

SIM-3589147 - June 13, 2017, 3:45 pm

Great Info! Thanks for the information, One thing as well Protonmail has released a beta for their VPN and I love it so far! Pretty fast as well, which I was quite surprised. One thing though whenever I use a VPN I can't access Hackerforums does anyone know why? I would appreciate the help!

Mirakuru - June 15, 2017, 11:58 am

(Jun 13, 2017 03:45 PM)Vipernet1220 Wrote: [\[CITE\]](#) Great Info! Thanks for the information, One thing as well Protonmail has released a beta for their VPN and I love it so far! Pretty fast as well, which I was quite surprised. One thing though whenever I use a VPN I can't access Hackerforums does anyone know why? I would appreciate the help!

<https://hackforums.net/showthread.php?tid=5642995>

predatorvj - June 18, 2017, 10:27 am

One of most exhaustive detailed tutorial

chris101 - June 20, 2017, 11:10 am

I think online security is very important nowadays because of a lot of things happening on the internet. Keep me updated with online security...

TacticalChicano - June 20, 2017, 1:59 pm

Thanks nice information, for those who know little about how to maintain their privacy a bit more secure.

shifty1337 - June 25, 2017, 12:27 pm

Quote:Block Ads with "uBlock Origin"

An efficient wide-spectrum-blocker that's easy on memory, and yet can load and enforce thousands more filters than other popular blockers out there. It has no monetization strategy and is completely open source. We recommend FireFox but uBlock Origin also works in other browsers such as Safari, Opera, and Chromium. Unlike AdBlock Plus, uBlock does not allow so-called "acceptable ads".

for how long have I searched for something like this thank you OP!??

L4nd0 - June 28, 2017, 1:13 am

Awesome post! Found a few things that I did not know about.

retic3nt - June 29, 2017, 11:29 am

Cheers, gonna implement these now. Let the eWhoring commence

ActFast - June 29, 2017, 11:41 am

I know this thread is pretty old but thanks so much for this OP. I was using a VPN only now I think i'm going to up the security.

impose - July 8, 2017, 9:45 pm

Thanks for this, found it really helpful!

test - July 8, 2017, 9:48 pm

One of the very few people on here I trust to know what they are talking about. Some extremely useful information for anyone concerned about Privacy, Anonymity and Security online.

bouldog - July 14, 2017, 3:55 am

thank you very interesting

FadedUploads - July 15, 2017, 5:03 am

encrypted cloud storage? is it just encrypted in the cloud or does the user also need the key? im sorry i know you mentioned it but imma bit cunfused o_O

Sparker - July 16, 2017, 4:26 pm

Thank you for your efforts providing us with great info. Today's Technology is very beneficial and dangerous. Online privacy is a must be configured properly when browsing even for general browsing purpose. This is very helpful and great info.

dipen11.patel - July 16, 2017, 11:06 pm

can anyone please suggest if this training is worth persuinging?
iantindia - CYBERSECUREUSER

SUI-3183372 - July 16, 2017, 11:22 pm

(Jul 16, 2017 04:26 PM)Sparker Wrote: [\[CITE\]](#) Thank you for your efforts providing us with great info. Today's Technology is very beneficial and dangerous. Online privacy is a must be configured properly when browsing even for general browsing purpose. This is very helpful and great info. Depends on the service. Most just offer you encrypted spaces where you don't have access to the keys and you need to trust the company.

You can however, use [Cryptomator](#), which is client-side encryption for your files in the cloud. It's actually pretty cool, I recommend checking it out.

(Jul 16, 2017 11:06 PM)dipen11.patel Wrote: [\[CITE\]](#) can anyone please suggest if this training is worth persuinging?

iantindia - CYBERSECUREUSER

Are you from India?

I don't know anything about iantindia, but I wouldn't suggest it unless you're Indian yourself.

Rubixa - July 16, 2017, 11:23 pm

(Jul 16, 2017 11:06 PM)dipen11.patel Wrote: [\[CITE\]](#) can anyone please suggest if this training is worth persuinging?

iantindia - CYBERSECUREUSER

I personally wouldn't take a course from somewhere if their site can't even spell.

Ethical Vox - July 20, 2017, 6:19 pm

Does anyone have suggestions for a secure cloud storage? I know of next cloud but I believe that requires me to have my own server.

elpapugomez - July 21, 2017, 6:55 pm

after reading a little bit: I understood I need to do something for my privacy (sorry...I'm just a newbie)

SIM-3162965 - July 22, 2017, 8:21 am

How important is the operating system? For example, should I use the web-version of my apps or can I remain anonymous using a VPN over the installed apps in Windows?

Also, can I use the add-ons you recommended for Firefox on the tor browser? I don't see why I can't just do everything over one browser.

capt.j - July 23, 2017, 6:19 am

That's a really good information. Thank you for this.

SUI-3183372 - July 23, 2017, 8:41 am

(Jul 22, 2017 08:21 AM)verify360 Wrote: [\[CITE\]](#) How important is the operating system? For example, should I use the web-version of my apps or can I remain anonymous using a VPN over the installed apps in Windows?

Also, can I use the add-ons you recommended for Firefox on the tor browser? I don't see why I can't just do everything over one browser.

It really depends on the application. I think in some cases the application its self will prevent excess data from being leaked, but in other cases, it can probably be the total opposite.

A VPN is always useful at keeping your location / IP anonymized, but it does not stop you, yourself, from sharing too much information. Randomizing/faking information that you submit online is also necessary.

I don't use TOR browser a lot due to circumstances unique to myself, but I do believe most add ons can be used in the TOR browser. However, the TOR browser out of the box already comes pre-installed with some of the add ons listed in my OP.

gitclone - July 25, 2017, 10:29 am

Hey!

Any plans to add Keeper as password manager.

It's also zero knowledge, multi Device, SOC2 certified, AES 256-bit encryption and PBKDF2 (up-to 100k rounds) with HMAC-SHA256 protected, supports 2FA and data is encrypted and decrypted at the device level

SUI-3183372 - July 26, 2017, 4:12 pm

(Jul 25, 2017 10:29 AM)gitclone Wrote: [\[CITE\]](#) Hey!

Any plans to add Keeper as password manager.

It's also zero knowledge, multi Device, SOC2 certified, AES 256-bit encryption and PBKDF2 (up-to 100k rounds) with HMAC-SHA256 protected, supports 2FA and data is encrypted and decrypted at the device level

I haven't looked into it at all. I'll check it out this weekend.

Thanks for the tip.

Couple questions.

Is it free? I see paid options but I think you can download it for free too. Is functionality reduced for the free version?

Is it open source? I like to stick to open source solutions but make exceptions from time to time.

gitclone - July 27, 2017, 7:13 am

(Jul 26, 2017 04:12 PM)Previously Known As.... Wrote: [\[CITE\]](#) I haven't looked into it at all. I'll check it out this weekend.

Thanks for the tip.

Couple questions.

Is it free? I see paid options but I think you can download it for free too. Is functionality reduced for

the free version?

Is it open source? I like to stick to open source solutions but make exceptions from time to time. Sadly there's only trial and after that it costs, but I find 30e/year to be reasonable.

And its not open sourced, which was huge problem for me at the beginning, but I haven't found anything I could use as replacement.

Breekee - July 31, 2017, 4:20 am

I guess you could add Tutanota.com on the e-mail provider list

Edit: Also,if anyone needs a good free VPN windscribe.com (10GB/month FREE) has passed my evaluation criteria so I recommend you using it. Even if they are inside the 5 eyes(Canada) they DO NOT store any kind of information about you so there is nothing to give out if requested.

For those asking how do they survive if they don't track you : You will get your answer if you use the FREE version. People are so pleased by the free version that they are paying for the monthly subscription.

leounishar - August 9, 2017, 12:51 pm

What do you think about Tutanota for email?

SUI-3183372 - August 9, 2017, 1:18 pm

(Aug 9, 2017 12:51 PM)leounishar Wrote: [\[CITE\]](#) What do you think about Tutanota for email?

I've only heard good things about Tutanota. However, they don't accept Bitcoin, so I've never looked into using them. If I'm going for anonymity, I want a service that's not going to blow that due to the way they accept payments.

Their free plan seems decent though.

Forc?d - August 9, 2017, 2:09 pm

One of the most in-depth and well made privacy security related threads to date. Great work!

Also only heard good things about Tutanota, they recently implemented built in End-to-End encryption options based on a shared key.

Built in PGP would be next.

still_free - August 11, 2017, 1:12 pm

Very nice information from this thread.Thank you good sir!

LyfHax - August 16, 2017, 5:47 am

would all of these steps be enough protection when you're doing stuff like ewhoring or botnet shop selling?

Angel - August 16, 2017, 9:15 pm

This thread is the most HQ i've ever seen on HF.

Posting to come back later to read it all.

Maichg - August 18, 2017, 5:44 am

This has been Truly informative.!! Thank you.

Mr. Moth - August 19, 2017, 1:01 am

Thanks for the high quality information, appreciate it heaps!

undernation - August 21, 2017, 11:02 am

Online security is something that is a must.. THanks alot

Kekdem - August 22, 2017, 10:52 pm

Thank you for this thread on methods to stay secure online.

Atom™ - August 24, 2017, 3:46 am

I'd like to know why you're recommending not using LastPass and other popular password managers. Aren't they secure as well?

?

SUI-3183372 - August 24, 2017, 4:01 am

(Aug 24, 2017 03:46 AM)Atom™ Wrote: [\[CITE\]](#) I'd like to know why you're recommending not using LastPass and other popular password managers. Aren't they secure as well?

?I had a big discussion about this 9 months ago, but I can't find it anymore. I avoid LastPass like the plague. Nothing about it is good from a security perspective.

1. Closed Source - I very rarely recommend closed source software, you place your faith solely in the company developing the software.
2. Password databases are stored online - This seems ludicrous to me. I understand needing to get your password database to other devices, but permanently keeping your password DB online with million of others, that's asking for catastrophe.
3. Ran by LogMeIn - The biggest thing to keep in mind is that commercial products like LogMeIn are under intense economic pressure to continually grow their user base. They can only do that by making their products easier and easier to use, on more and more platforms, and adding more and more features that differentiate them from competitors. ALL of these tendencies run contrary to good security. The product might be fine now, but if they ever get desperate for new users, it's easy for products like this to turn into a bloated nightmare.
4. History of bad vulnerabilities - Remote Code Execution vulns have been found various times. These are very bad.
5. History of breaches - Google LogMeIn breach. They're notoriously bad at their security.

I could debate all day about why LastPass should never be touched and solutions such as KeePass should be used.

Atom™ - August 24, 2017, 4:22 am

(Aug 24, 2017 04:01 AM)Previously Known As.... Wrote: [\[CITE\]](#) -snip-
Thank you for the enlightenment!

Now what would you recommend instead, I've gone thru the list and I'm a bit confused as to which one to pick. I'd like something that's like LastPass, i.e, on multiple platforms & cloud.

Excuse me if I'm sounding dumb.

Thanks,
?

SUI-3183372 - August 24, 2017, 10:48 pm

(Aug 24, 2017 04:22 AM)Atom™ Wrote: [\[CITE\]](#) Thank you for the enlightenment!

Now what would you recommend instead, I've gone thru the list and I'm a bit confused as to which one to pick. I'd like something that's like LastPass, i.e, on multiple platforms & cloud.

Excuse me if I'm sounding dumb.

Thanks,
?

I use KeePass on my computers and phones. Open source, easy to use. It doesn't look as nice, but it's very secure.

If you really must have your database in the cloud, then use Dropbox if you're not willing to set up your own cloud storage. However, if you're going to keep your password database in the cloud, make use of Cryptomator: <https://cryptomator.org/>

The Cobra - August 26, 2017, 5:19 am

Great thread! Thanks for the info.

SpyralScanner - August 26, 2017, 7:13 am

Great thread brother, thank you!

alibabka - August 28, 2017, 8:06 am

Thanks, bro!

I set up my PC

G3yb01 - August 30, 2017, 11:37 am

Tuatanota for secure email also.

SUI-3183372 - August 30, 2017, 6:43 pm

(Aug 30, 2017 11:37 AM)G3yb01 Wrote: [\[CITE\]](#) Tuatanota for secure email also.
Convince them to accept Bitcoin or other cryptos.

phenasty - September 8, 2017, 8:45 am

bitcoin is wonderful. convince them to use it.

SUI-3183372 - September 9, 2017, 7:42 pm

(Sep 9, 2017 03:24 PM)Suboptimal Wrote: [\[CITE\]](#) What about Google Chrome?

I know they are collecting data for Google but is it really that bad?

Realistically, not really. But if you truly want to take a pro-privacy stance, it should be avoided.

plpatel - September 11, 2017, 4:30 am

can you suggest the best VPN I could use

SUI-3183372 - September 11, 2017, 3:02 pm

(Sep 11, 2017 04:30 AM)plpatel Wrote: [\[CITE\]](#) can you suggest the best VPN I could use
I can't say what the best one is.

I can tell you the ones that I would recommend:

CryptoStorm
[censored]
Mullvad
BlackVPN

Pre-eminent - September 11, 2017, 3:07 pm

Very high-quality thread with a lot of good content, currently use some of these tools myself.
Thanks for the share OP.

KelseyM - September 22, 2017, 3:47 pm

Wondering when the next HQ thread by this user will come out.

M?xim - September 22, 2017, 5:06 pm

(Sep 22, 2017 03:47 PM)KelseyM Wrote: [\[CITE\]](#) Wondering when the next HQ thread by this user will come out.

Expectations will be high for something to beat this.

SUI-3183372 - September 22, 2017, 6:41 pm

(Sep 22, 2017 03:47 PM)KelseyM Wrote: [\[CITE\]](#) Wondering when the next HQ thread by this user will come out.

(Sep 22, 2017 05:06 PM)Maxim Wrote: [\[CITE\]](#) Expectations will be high for something to beat this. You're asking one of the laziest members when their next big thread is going to be....

I have ideas for threads, but actually coming up with a thread I'm happy with will take a lot of time. A lot.

Plus this one is well overdue for a serious update. Lots of stuff I've been compiling to add. Just again... the lazy thing..

Dorum - September 26, 2017, 6:31 pm

Nice post, I would add Wire to the list

devh5002 - September 30, 2017, 9:55 am

Thanks for this man,

really informative and helpful!

xADHDx - October 2, 2017, 9:01 am

Great guide! I learned a bit from this myself. Thanks for contributing to the forum with this :)

bobulous - October 5, 2017, 6:53 am

Thank you! This is an easy to search guide and I'll be referencing this in future.

ink666 - October 5, 2017, 5:42 pm

Really interesting read. Thanks for sharing this brother.

Hustla - October 7, 2017, 11:49 am

Thanks for the share. I'll have to switch over to Firefox soon.

AJ911 - October 13, 2017, 5:09 pm

Great information. Anything that applies to android phones regarding encryption?

dd1991 - October 14, 2017, 12:05 am

(Sep 26, 2017 06:31 PM)Dorum Wrote: [\[CITE\]](#) Nice post, I would add Wire to the list I wouldn't. Certainly it's nice looking but it's been known to store more metadata than Whatsapp so what's the point?

I am not allowed to post links directly but if you want more info you can find it here:

reddit.com/r/privacytoolsIO/comments/766vzk/is_anything_wrong_with_wire_the_messaging_app/dobu872/

darkklok - October 15, 2017, 2:02 am

GOOOD thanks you for all informations

reapingtheuprise - October 20, 2017, 3:35 am

Hands down, absolutely the best most in-depth post I have yet to see on this website on Cyber-Security. This is truly a work of art.

Alien8ed - October 24, 2017, 5:21 pm

Thank you for useful post. Looking to read more from you. ?

Null911 - October 27, 2017, 7:11 am

Nice thread !! Thx for all infos :)

meatyklackers - November 2, 2017, 11:16 am

Thank you very much for this thread. So much good information. Big fan of the Vera Crypt software and a bunch of the browser plug in features were a much needed improvement for me.

suomynonayats - November 3, 2017, 10:08 am

Thanks! Very useful ! BTW: Has any of the information changed, or have new solutions come since: This post was last modified: 12-29-2016, 12:06 AM ?

Julius Caesar - November 6, 2017, 3:29 pm

+rep very good guide for starting out ?

Winston Churchill - November 6, 2017, 5:37 pm

+rep || Great quickstart guide for people looking to protect themselves on the web ?

Lyric - November 6, 2017, 10:07 pm

Great! Thank you for the tips

OGMadcow - November 18, 2017, 7:26 pm

Absolutely fantastic guide, very informative and helpful thank you definitely going to use some of this.

Anonimite - November 19, 2017, 6:42 am

Thank you for this guide!

xFeng - November 21, 2017, 1:35 am

damn, what a great list definitely bookmarking this

meatyklackers - November 21, 2017, 4:04 pm

Every thread I have read so far from you has been a game changer. Perfect for new folks that just want to learn. Thank you!

uvd6zv2 - November 22, 2017, 9:52 am

This thread is old now but it still contains a lot of very useful information. Thank you for your time and knowledge.

AntiTrust-86 - November 23, 2017, 10:33 am

Great post this will help me a lot as a starter

Lisaito - November 24, 2017, 1:55 pm

When his usertag says back from the dead, but he is dead.

dazzleE - November 28, 2017, 8:57 pm

Great work bro! Its rilly helpfull keep up the good work

Exuberance - November 29, 2017, 8:34 pm

Very well explained, would you bank on tor and vpn along with a couple of add ons that prevent cookie tracking, slippage, etc.?

Misbehave - December 8, 2017, 5:45 am

This is extremely useful and helpful, thank you.

scatwin - December 8, 2017, 2:08 pm

Hello Everyone,

I am new here and have been reading this thread and trying to implement the good things mentioned here...

I have now started using a TOR browser and when i try to access the forum it thinks that I am a bot and asks me to verify the if i am human, but no captcha or other validation things are displayed so not able to access this site using TOR browser.

Need some guidance on what i should do to get this fixed.

Best...

lohith - December 13, 2017, 1:09 am

Amazing work.. Could anyone kindly help me out the way to know whether pc and android are hacked or not? I have checked netstat -ano but it is returning active connections. I have turned on my windows updates. What is the perfect way to know whether hacked or not? In case hacked what are the steps to be followed to get rid of that exploitation. Thanks in advance!

eth1 - December 13, 2017, 10:41 pm

Very well made. Nice post.

Bg420 - December 16, 2017, 2:28 pm

hi guys i am wanting to setup a vpn on my network. and i am having issues getting my vpn to conect have linux mint os, usign openvpn but no luck to coneect to severs. helppppp please im naked ??? ?

thenativ - December 23, 2017, 9:36 am

One of the most informative posts I've seen on the security topic. Thanks for this post, I've been recently been looking for additional ways to improve my home network security and this helped a lot. Definitely worth spreading this information, as many people disregard the value of privacy and security in the internet.

JustFamous - December 29, 2017, 2:39 am

Posting to be able to come back to this. Nice info though

ghost0108 - January 4, 2018, 8:56 pm

Anyone .. please post code for Meltdown exploit. Wanna test them on my network of Computers and wanna patch them on my own.

Zanidd - January 16, 2018, 3:51 pm

Really helpful guide! And seems to be updated recently. I like that!

tassilo - January 17, 2018, 5:49 am

this is a really nice and reminds me to privacytools.io
is that your site?

tiitteet28 - January 26, 2018, 5:01 pm

Thanks for the great guide!

SIM-3795472 - January 29, 2018, 2:28 am

Thank you for this one!

Will help me in my endeavor to stay safe on the web.

chiffre - February 1, 2018, 3:57 pm

This is a great list of resources. Thank you for taking the time to compile it.

I believe that StartPage would be a good addition to the privacy-respecting search engine section.

Ki11Mach - February 3, 2018, 11:53 am

This is a fantastic collection of information and it will be Bumped!

Zaccharias - February 7, 2018, 4:16 pm

Thank you very very much for this guide!

Got a question: If I install all the addons for firefox you recommend, isn't my fingerprint very individual then?

Wouldn't it be better to just install 2-3 of the most important ones to get a standardised anonymous browser ?

Thanks in regard!

Zac

Rixmainn - February 18, 2018, 9:02 am

Thanks for all these recommendation.
that was very helpful for me :)

hdbt - March 4, 2018, 3:13 am

hi am new member please i want to learn the penetration please

Trapezoid- - March 7, 2018, 6:44 pm

A lot of good info here. Saving this for reference Thanks!!

boshaft - March 15, 2018, 1:24 pm

great info for a beginner like me, thanks

boisenative88 - March 24, 2018, 9:15 am

This is incredibly helpful. I appreciate the time put into this thread !

mariobrossss - March 25, 2018, 9:23 pm

Great informations Thank you for useful post.

XwhoXamXiX - March 27, 2018, 5:31 am

Fab thread posting so I can come back to it

.Ares - April 3, 2018, 1:26 pm

Wonderful post! Outlines all the tools to use and services to remain anonymous. ?

JOYIHONG - April 23, 2018, 11:11 pm

Hey all masters , i would like to know is that possible phone get hacked with the phone will be auto run voice record ?without i knowing ?

colonel.mortimer - April 27, 2018, 6:40 am

.....

Vyzerr - April 29, 2018, 1:01 am

good post. checked out veracrypt and im loving it for being free thanks abunch

TBeasts - May 6, 2018, 11:40 pm

Thank you for this very useful information! I'm especially going to check out the Firefox plugins.

SeekerOfPandora - May 8, 2018, 8:39 am

Great thread, thanks for the guide :)

wesbroo00 - May 9, 2018, 1:36 pm

Great thread ! thank you for the hard work

Zaki2297 - May 10, 2018, 9:54 am

Any opinions on the app "Mutter" for iOS?

phype - May 11, 2018, 3:35 am

Great info! As I'm pretty paranoid about things, is running a vpn sufficient to remain anonymous on a computer I've heavily been using for the last two years? Do I need to go into task manager every time I want to run it to make sure my background apps aren't trying to log into a website and this giving away that matching user ip?

alcaponemv - May 12, 2018, 11:31 am

Hello, what thing about anonabox pro? It enough using this and paid vpn, tails os and tor. For good anonymous? Or this item not good and was better way to be anonymous in tor product? I'm green on this but searching info of that. And if here who can help me with that in there? ?

cyber_magus - May 14, 2018, 2:16 pm

On a chromebook will i ever have real privacy? i orbotVPN and duckduckgo.

thanks for the help in advance

Forkroad - May 15, 2018, 9:42 am

Wow, thank you and good work!!

Mjood2 - May 16, 2018, 7:18 am

Really interesting read. Thanks for sharing this brother.

fy1337 - May 18, 2018, 6:54 pm

Wow this is a really detailed guide. Thanks for the post

2xqz - May 21, 2018, 9:27 am

Security is just a myth :)

ericweisz - June 1, 2018, 2:00 pm

Hey, thanks for the security list my friend.

9h05t - June 3, 2018, 1:51 pm

Nice list of add-ons for safety. Didn't know a lot of those, but as you said even your plugins can be used to track you so I don't know how useful those could be considering that fact.

DetectiveDecker - June 4, 2018, 5:04 am

Thanks for this post... i've gained some great insights from it

Smart Swag - June 8, 2018, 10:13 am

Thanks for your contribution,
really helpful.

Monne80 - June 21, 2018, 6:22 am

Great read, thnx for the input!

houssemh - June 24, 2018, 5:43 pm

thank you so much , we need another post for android Privacy

H4sh3d - June 27, 2018, 4:38 pm

Excellent post, provided me with a few new options to check out.

Thanks

kashyyy - July 3, 2018, 10:39 pm

this seems pretty cool will check out

WageWolf - August 16, 2018, 9:34 am

Looks like some great information here, the only thing I cannot agree with is the usage of Tor Browser in 2018. ?

zoloboz - August 19, 2018, 10:20 am

High quality information right here, gave you an reputation!

Greetings,
zoloboz

Zatmate - August 22, 2018, 2:17 pm

Wow, awesome thread! Thank you very much for all this information!

Mrs Paranoia - August 28, 2018, 5:21 am

(Aug 16, 2018 09:34 AM)WageWolf Wrote: [\[CITE\]](#) Looks like some great information here, the only thing I cannot agree with is the usage of Tor Browser in 2018. ?

Why is this? I'm curious to know if anything has been brought to light recently.

OP: Great thread, with a lot of useful information. Thank you ?

WageWolf - August 28, 2018, 7:41 am

(Aug 28, 2018 05:21 AM)Mrs Paranoia Wrote: [\[CITE\]](#) Why is this? I'm curious to know if anything has been brought to light recently.

OP: Great thread, with a lot of useful information. Thank you ?
It has been common knowledge that it is not as secure as most people expect.

n1k3 - September 3, 2018, 2:04 pm

Thanks a lot mate. This helped me out greatly!

Amphitrite - September 8, 2018, 9:02 pm

This is HQ Tips. The OP really did some research. I cant say i did not gain greatly from this

Edit:

Hinder Browser Fingerprinting with "Random Agent Spoofer" - addon outdated.

Automatically Delete Cookies with "Self-Destructing Cookies" - addon outdated. I used Self-Destructing Cookies (WebEx), dont know if it is ok.

Some of the parameter to be changed in about:config are no longer in firefox or Tor.

Thanks a lot. Its still an HQ Guide

Gert - September 9, 2018, 11:39 am

Holy cow this guide is top notch, made a persons life so scary that hes willing to co-operate in every scenario, got my money that promised luv ya

Forfun - September 10, 2018, 2:32 pm

Great thread, thanks for this.

SUI-3183372 - September 11, 2018, 10:38 am

Major vulnerability in TOR versions 7.x, the NoScript plugin leaks identifying information.
Ensure you are using TOR version 8.x.

couchmoneycrew - September 12, 2018, 11:37 pm

looking for someone for long term business with w.u transfers and dumps+pins and accounts have fulls snn and more work legit vendors only

bragado1 - September 13, 2018, 6:02 pm

Nice TUT and educative to stay anonymous

k511 - September 18, 2018, 7:53 pm

Nice post.. Got alot of information as well as the most of my questions were answered.

BrianP88 - September 19, 2018, 12:20 pm

TOP quality post. Thank you for providing so much useful information. Will definitely try a few tools and methods you provided here. Good guide to be untracked

Blackhawke2002 - September 29, 2018, 8:37 am

So after a few days on this site, and getting familiar with bitcoin, tor, and vpns, i had someone try to get into my email. fortunately i got the notification that it was blocked, and i went in to change the password. does anyone have any general ideas for where i can start looking to figure out where i went wrong?

clrake - September 30, 2018, 12:23 am

Nice information, since I think we haven't privacy

seafko - October 11, 2018, 6:43 am

Just read it. There's a lot of information I didn't know. Do you plan on keeping this thread updated?

KnownActivity - October 14, 2018, 4:02 am

Hi there I just stopped by to mention that this thread is informative as fuck and I'm happy I got to re-read it again.

ZionBless666 - October 15, 2018, 11:27 pm

Install Libreboot

That is all

Divided_Device - October 16, 2018, 10:59 am

Thanks for the information provided!

mrjohnson55 - November 1, 2018, 8:37 pm

Great post enjoyed reading it

TheDuckDuckGoGuy - November 6, 2018, 7:15 pm

What is wrong with using True Crypt in 2018? From what I've read it's still safe to use. Do you have any sources to proven vulnerabilities "released in the wild"?

SUI-3183372 - November 6, 2018, 11:53 pm

(Nov 6, 2018 08:15 PM)TheDuckDuckGoGuy Wrote: [\[CITE\]](#) What is wrong with using True Crypt in 2018? From what I've read it's still safe to use. Do you have any sources to proven vulnerabilities "released in the wild"?

<https://www.pcworld.com/article/2987439/encryption/newly-found-truecrypt-flaw-allows-full-system-compromise.html>

<https://seclists.org/oss-sec/2016/q1/58>

https://en.wikipedia.org/wiki/VeraCrypt#Security_improvements

I don't have any knowledge of these vulnerabilities or weaknesses being exploited. However, I'd rather use software that has identified these issues and fixed them than software that has these issues, hasn't been updated in 4 years, and never will be updated again. VeraCrypt has very talented developers and they do good work, I'd recommend looking into it.

Taustray92 - December 11, 2018, 5:58 am

It is an alternative to SaaS Boxes and Drives, with more control, safety and privacy, and favorable TCOs.

mesy1312 - January 11, 2019, 10:02 pm

Thanks so much for this! ? ?

misterchoc - January 26, 2019, 9:30 am

Good post but little update would be good aswell :P

kibishibi - January 26, 2019, 10:55 am

Super helpful. Thank you so much. Didn't even know some of these extensions existed.

sgtfacepunch - January 27, 2019, 2:03 am

Excellent thread. I definitely learned a lot and still have to implement some of these techniques. I have fully secured my browser and email, now I need to get the master passwords going. Thanks for putting this together.

OnikageO - January 28, 2019, 12:06 pm

Just joined.

Lot to read.

Thanks for sharing.

Metrole - February 3, 2019, 6:01 pm

Thanks for the tips! Really appreciate this long thread!

SUI-3183372 - February 3, 2019, 7:31 pm

(Jan 26, 2019 10:30 AM)misterchoc Wrote: [\[CITE\]](#) Good post but little update would be good aswell :P

I know I know... for a year I've wanted to update this. I have a lot of good sources of information ready for a full overhaul, but the thread is going to span 3 or 4 posts now and I haven't been able to motivate myself to spend the time to update it.

frsnix - February 18, 2019, 2:30 pm

Despite how much work you put into the thread, I gotta give it to you for including the website of Privacytools, as I wouldn't have been learned about it if it weren't for you. Thanks man.

ModernDayCatfish - February 26, 2019, 6:06 pm

(Feb 3, 2019 08:31 PM)Previously Known As.... Wrote: [\[CITE\]](#) I know I know... for a year I've wanted to update this. I have a lot of good sources of information ready for a full overhaul, but the thread is going to span 3 or 4 posts now and I haven't been able to motivate myself to spend the time to update it.

Perhaps spending a little less time on runescape and a little more time on Hackforums would be beneficial.

Nice thread :)

SUI-3183372 - February 26, 2019, 6:38 pm

(Feb 26, 2019 07:06 PM)ModernDayCatfish Wrote: [\[CITE\]](#) Perhaps spending a little less time on runescape and a little more time on Hackforums would be beneficial.

Nice thread :)

╰_ (?) _╯

ModernDayCatfish - February 26, 2019, 6:44 pm

(Feb 26, 2019 07:38 PM)Previously Known As.... Wrote: [\[CITE\]](#) ╰_ (?) _╯
Touché.

And I act like I know your life ?

? **Heisenberg ?** - February 26, 2019, 8:00 pm

Great thread mate. Got some of the addons. Also got Keepass.
Thanks.

BTC - February 27, 2019, 3:22 pm

I am not sure if it has been talked about, but there is a nice preconfigured browser with a lot of things included in this thread like HTTPS everywhere, script blocking, cookies blocking / self destruct, encrypted connection, device recognition block, ads/tracker blocks. And also one great feature is the addition of their wallet service integrated into the browser, and allows for auto-contribution to verified publishers. One verified publisher I always auto-contribute to is of course, Hack Forums :)

I love Chrome, this is why I prefer it over any firefox configuration with plugins, and other things. Most of these things are also available in chrome, that along side DNSCrypt with some agent-spoofing and you have a decent setup for anonymity in my mind :) I love the fact it has global defaults for settings, then you can set defaults for specific sites as you browse and keep the settings saved under profiles.

What do you guys think of it?

<https://brave.com>

visarena - March 12, 2019, 12:26 pm

thanks you very much . It is very useful for newbies like me .

shownuff00 - March 15, 2019, 6:58 am

(Aug 17, 2016 02:33 PM)Erich Himmler Wrote: [\[CITE\]](#) This is good info, but most of it could be bypassed on the local machine by Windows 10 Spying.

Windows 10 is known for collecting data and sending it back to the Microsoft mothership. Find out which settings to tweak to keep Windows 10 .

Microsoft Windows 10 basically a spying operating system?

Toscan - April 4, 2019, 8:09 pm

This is a very helpful thread. Will be coming back to this often. :)

UKevin - April 13, 2019, 7:15 am

Such a great thread! Outdated but still gold

Spaark - April 13, 2019, 7:59 pm

years on and somehow only now am i making use of this. Great work mate, much appreciated :)

M e l l o - April 15, 2019, 3:15 am

thank you very much. it was really helpful. :D

Ex Nihilo - May 1, 2019, 7:11 pm

I thought password managers were an unsecure tool.

Nallasboy - May 2, 2019, 4:19 am

I appreciate your work, thanks for this thread. Do its still getting updated?

Afkanitroll - May 3, 2019, 4:37 am

Awesome post and helpful, Thanks

hose10 - May 9, 2019, 3:04 pm

Learned a lot and from now on i am using many of what you mentioned. Great guide!

zero_code29 - May 10, 2019, 2:21 am

Good and Detailed information for those who are mainly concerned about their privacy online. Nice post buddy.

work4tacos - May 16, 2019, 7:40 am

awesome thread i just came back onto pc after 6 years i dont remember anything i want to protect myself online and this helped me a lot

duplex - May 18, 2019, 1:18 am

Quick question, when I crypt my D drive, it says 11 hours, and that's with it formatted too, any ideas on how to make this quicker?

ririki - May 18, 2019, 1:22 am

(May 18, 2019 01:18 AM)Duplex Wrote: [\[CITE\]](#) Quick question, when I crypt my D drive, it says 11 hours, and that's with it formatted too, any ideas on how to make this quicker?
Get smaller size and faster D Drive.

duplex - May 18, 2019, 1:23 am

(May 18, 2019 01:22 AM)ririki Wrote: [\[CITE\]](#) Get smaller size of your D Drive.
It's 1tb, not SSD, I was wondering if a different encryption would perhaps speed it up?

Really need a high storage SSD don't I..

ririki - May 18, 2019, 1:24 am

(May 18, 2019 01:23 AM)Duplex Wrote: [\[CITE\]](#) It's 1tb, not SSD, I was wondering if a different encryption would perhaps speed it up?
Really need a high storage SSD don't I..
I am not acknowledged about any.
Run it overnight. that's best solution.
Mine 1TBs usually take around 6 to 8 hours.

duplex - May 18, 2019, 1:25 am

(May 18, 2019 01:24 AM)ririki Wrote: [\[CITE\]](#) I am not acknowledged about any.
Run it overnight. that's best solution.
Alright thanks man, appreciate it!

ririki - May 18, 2019, 1:26 am

(May 18, 2019 01:25 AM)Duplex Wrote: [\[CITE\]](#) Alright thanks man, appreciate it!
I've also made a small change in my last post, my 1TBs usually takes around 6 to 11 hours too, it should settle down but I don't think you will get near 2 hours, you can probably also speed it up with 0 phases or 1 phase (wipe mode) but that's not so secure.

SUI-3183372 - May 18, 2019, 9:22 am

(May 18, 2019 01:18 AM)Duplex Wrote: [\[CITE\]](#) Quick question, when I crypt my D drive, it says 11 hours, and that's with it formatted too, any ideas on how to make this quicker?
What are you using to encrypt it?

ririki - May 18, 2019, 9:28 am

(May 18, 2019 09:22 AM)BV1 Wrote: [\[CITE\]](#) What are you using to encrypt it?
Good question, I myself thought or think he is using veracrypt.

santosDrT - May 20, 2019, 4:41 am

good information here, thanks very much !

3xploit - May 25, 2019, 5:55 am

This guide is quite amazing. Most people think if they get a free vpn they are super anonymous. In fact, most people seem to underestimate how many information your device is sending when using the Internet.

?

duplex - May 25, 2019, 10:54 am

(May 18, 2019 09:22 AM)BV1 Wrote: [\[CITE\]](#) What are you using to encrypt it?
Veracrypt, it takes forever to try and encrypt my 1TB HDD

SUI-3183372 - May 25, 2019, 11:24 am

(May 25, 2019 10:54 AM)Duplex Wrote: [\[CITE\]](#) Veracrypt, it takes forever to try and encrypt my 1TB HDD

Are you encrypting in place, or are you encrypting a new drive.

If you're encrypting in place (encrypting a drive already [partially] filled with data), then yeah, I know it used to take me about 24 hours to fully encrypt a drive, with hardware increasing or decreasing this time.

If it's a new drive, then it should be a lot quicker. You mentioned 11 hours before, that still seems a bit long to me but I haven't encrypted an HDD in a few years now, so maybe my memory is a bit off. If speed is an issue and you need a faster solution, you could resort to just using encrypted containers within the hard drive. Full disk encryption is nice, but there's nothing wrong with storing sensitive information within an encrypted container as well.

duplex - May 25, 2019, 11:50 am

(May 25, 2019 11:24 AM)BV1 Wrote: [\[CITE\]](#) Are you encrypting in place, or are you encrypting a new drive.

If you're encrypting in place (encrypting a drive already [partially] filled with data), then yeah, I know it used to take me about 24 hours to fully encrypt a drive, with hardware increasing or decreasing this time.

If it's a new drive, then it should be a lot quicker. You mentioned 11 hours before, that still seems a bit long to me but I haven't encrypted an HDD in a few years now, so maybe my memory is a bit off. If speed is an issue and you need a faster solution, you could resort to just using encrypted containers within the hard drive. Full disk encryption is nice, but there's nothing wrong with storing sensitive information within an encrypted container as well.

Well, I did have data used on the HDD, but I tried encrypting it and it changed it to the FAT format and removed everything. I tried encrypting after the data wipe as I thought why not? It just removed it all, but the encryption time was around 11/12 hours even after a wipe?

What could it possibly need to encrypt?

SUI-3183372 - May 25, 2019, 12:06 pm

(May 25, 2019 11:50 AM)Duplex Wrote: [\[CITE\]](#) Well, I did have data used on the HDD, but I tried encrypting it and it changed it to the FAT format and removed everything. I tried encrypting after the data wipe as I thought why not? It just removed it all, but the encryption time was around 11/12 hours even after a wipe?

What could it possibly need to encrypt?

When you format a drive, the data is still there, it's just essentially marked as junk and any new data

is free to overwrite it, it's not actually deleted. I think you'd see these encryption times go down if you zero'd out the drive first (overwrite the entire drive with just 0's), however, zeroing out a drive is another somewhat lengthy process in itself.

I've never messed around with timing encrypting different drives before, so this is more of just my best guess.

Dollar Signs - June 2, 2019, 10:24 am

Still waiting on that update.

SUI-3183372 - June 2, 2019, 11:44 am

(Jun 2, 2019 10:24 AM)Dollar Signs Wrote: [\[CITE\]](#) Still waiting on that update.

Just finished up my school semester last week. I'll get around to it soon now that I have time.

elbone - June 3, 2019, 3:20 am

Good information and I'll be waiting for that update

hassankai2 - June 11, 2019, 6:38 pm

Please how can I Divert client phone calls and sms to another phone number?

Can you move Verycrypt from one computer to another?

Can you move Verycrypt from one machine to another?

K4LI0 - July 10, 2019, 2:07 pm

I have a question for OP. Why is not Tails Live distro on this list? It's an extremely interesting tool.

Chyrk - July 14, 2019, 7:43 pm

Very good information, thanks a lot.

Mafulen - July 27, 2019, 7:01 pm

Lot's of good quality information here, thanks for that thread!

Magictabz - July 29, 2019, 10:08 am

good information thanks allot!

Ivex - July 29, 2019, 7:58 pm

Hi, you don't trust chrome.

What do you think of Brave?

SexyCole - August 11, 2019, 6:33 am

Thanks for the HQ guide! I really appreciate it!

bbarr - August 11, 2019, 9:02 am

You wrote a great guide.

Hope to see the upgrade soon.

Ironman - August 11, 2019, 3:22 pm

thanks for the info about the privacy, but one question is there any search engines, besides google that you can recommend?, because I heard that google keeps some info about what you search and don't respect the privacy.

majorlybored - August 14, 2019, 8:06 am

any one have a full set up for a laptop step by step to make it safe by default aka the cover your ass hacker plan not for the skiddies ?

CertifiedNamer - August 15, 2019, 11:41 am

Very helpful and well written. Thank you for this post.

SUI-3183372 - August 26, 2019, 1:49 pm

(Aug 26, 2019 12:48 PM)contrapak Wrote: [\[CITE\]](#) Three years later, and this guide is still relevant.

My question is what's the issue with using a cloud-based password manager like 1password or Bitwarden?

Simply increased risk.

Is it a risk that the average user has to worry about? No. However, there are still a few concerning aspects to storing your data in the cloud.

Let me preface by saying I am not entirely up to date on my password managers. It sounds like both Bitwarden and 1password make use of a cloud that they host/manage, and we simply stored our encrypted password database in it. Correct me if I'm wrong.

My concerns

1. I don't like the idea of a list my passwords being stored online, encrypted or not. I get that even if these password manager's clouds get compromised that my passwords won't be decrypted, but it won't stop an agency like the NSA from grabbing all these password databases and sitting on them until they can be decrypted. The less attack vectors against my passwords the better.

2. Bitwarden is open source, but is 1password? If 1password is not, can you even be sure that your passwords are being encrypted in a manner that can't be decrypted? Is their crypto implemented properly? Have they been swayed by a government to install a backdoor? Because then your passwords are online AND can potentially be decrypted TODAY.

3. Somewhat recently we found out that when served with a court order to hand over all data they had on an individual, LastPass (I know you didn't mention LastPass, but this is an example of why I want to be the only person watching my passwords) did something pretty scary. LastPass was unable to hand over passwords to Law Enforcement, as they are encrypted and LastPass don't have the keys, however last pass did give Law Enforcement the times that passwords were accessed and by what IP address. Doing such, Law Enforcement or any other spying eyes can correlated where you use your passwords, and potentially where you use specific passwords.

4. Even if open source, we're seeing an increased level of malicious actors slipping malicious into popular but poorly maintained libraries. If a password manager were to make use of one of these backdoored libraries, one that perhaps breaks the crypto implementation in the password manager, then your decryptable password db is again floating around in a cloud, all you can do is hope no one malicious gets to it. If you're using KeePass then at least you know that if the crypto implementation breaks in it, they still need to extract your password DB from YOUR computer, something that you control.

I really recommend keeping your passwords off the cloud. Use USB drives or some sort of trustworthy digital transfer of your encrypted password databases to all of your devices, keep away from services like Dropbox because even if you delete your DB from Dropbox it still exists on their servers for a fairly substantial amount of time.

SUI-3183372 - August 26, 2019, 2:23 pm

(Aug 26, 2019 02:06 PM)contrapak Wrote: [CITE](#) If this did happen, I'm hoping a brave soul at 1Password would be a whistle blower and let everyone know this happened. I'd hope that as well, but even so, it could already be too late at that point.

But yeah, a lot of hypotheticals that your average person very likely doesn't need to be overly concerned about, but it does increase the potential attack vectors against your passwords quite a bit, regardless of the viability of these attacks.

Airbandit - August 30, 2019, 3:11 am

Great job sir thanks for the post

w0nders - August 30, 2019, 3:40 pm

Thanks a lot for the easy-to-grasp info. This convinced me to finally use Firefox as my main browser, along with other practices you suggested. Stay safe :)

Xoro - September 2, 2019, 11:39 pm

Thank you for this! Posting so I come back to it.

t3ddyt0d0 - October 1, 2019, 2:27 pm

Thanks for this post. Useful tips.

osk4r - October 6, 2019, 10:06 am

Thanks for the Thread, really interesting to read.

Mafulen - October 13, 2019, 8:04 am

Great thread, lots of useful information. I recommend it to everyone follow it step by step.

Bumpy - November 2, 2019, 5:24 pm

thank you for the various information and helping hand with our privacy

BTCgo - November 11, 2019, 5:23 am

Thank you for the guide, look very interesting

Torrendo™ - November 13, 2019, 3:44 am

Helpful tips saves readers alot of research.

Jasonpoli - November 21, 2019, 8:03 am

thanks for all the tips there, were a lot of things i was missing!

missingNO - November 21, 2019, 3:24 pm

Well done.

Thank you very much for this.

Nonicox - November 21, 2019, 3:36 pm

i hope this can be really helpful

Seamus.Rahilly - November 28, 2019, 1:07 pm

Please i need help i made a meme acc on instagram and i need it made untraceable the account is @pallaskenrymemes and i need all the account records and everything deleted, i just made jokes about the teachers and now theyre pissed please, can someon hack the account and just make it untraceable or delete it

iRnx - November 28, 2019, 3:57 pm

Really helped, now have new options for staying secure, Cheers.

sammorrison9800 - December 28, 2019, 1:19 pm

Thank you so much. Was just wondering is it updated?

fullpain - January 11, 2020, 9:55 pm

Thanks for all this informations :)

No Skills Here - January 31, 2020, 12:53 pm

most of the "Firefox add ons" are removed...
what should i do?

Haeevia - February 3, 2020, 5:08 am

(Nov 28, 2019 02:07 PM)Seamus.Rahilly Wrote: [\[CITE\]](#) Please i need help i made a meme acc on instagram and i need it made untraceable the account is @pallaskenrymemes and i need all the account records and everything deleted, i just made jokes about the teachers and now theyre pissed please, can someon hack the account and just make it untracebale or delete it
LMAO. Dude I'd recommend just deleting the account all together and hope that no one will snitch on you.

Go to the Delete Your Account page. If you're not logged into Instagram on the web, you'll be asked to log in, since you can't delete your account from within the Instagram app

Answer the question on why are you deleting your account and re-enter your password. The option to permanently delete your account will only appear after you've selected a reason from the menu.

Click or tap Permanently delete my account.

Funniest post I've seen on this forum though, nice.

ndk58 - March 21, 2020, 9:53 am

Hi guys, I am new here. Question about being anonymous.

My setup is the following:

- Virtual machine, linux
- ExpressVPN running
- Fierfox with all addons and privacy settings set

My question is.... if on windows (where I have the VM) I run Chrome with my accounts opened (email, whatsapp etc), I think I can be traced right?

No matter I use the VPN, my ip address can be seen as used to login to my personal whatsapp or instagram.

Am I missing something here?

Basically, to be 100% not traceable, I should not open any account with my windows on the same IP I use on the Linux VM ? How about the live account related to the windows user ?

Thanks guys
cheers

loulou123456 - March 29, 2020, 11:11 am

nice is very important thanks you very much

Glossy - March 29, 2020, 12:41 pm

Awesome guide on privacy. Some of these tools I already knew about, some I found new here so thank you for that. I love Mozilla email client, I think it's the best on the market.

Iova67 - April 5, 2020, 11:48 pm

Wow, I think that I will reconfigure my system and I use windscribe as a vpn while waiting to have the means to pay the subscription on protonvpn or those of the mentioned list

ChiknNuggets - April 6, 2020, 1:40 am

Really nice and detailed information. Thanks for sharing mate.

dukt020 - April 9, 2020, 6:20 am

anonymity is everything nowadays for best opsec measures one shall use various techniques

Anabolic - April 12, 2020, 3:54 pm

Hi I added some of these add-ons and I did the config stuff on Firefox and now I get a 403 error when trying to use HF and GOOGLE. Any ideas on how I can fix this? I assume there's some settings not adjusted properly?

Motivated - April 12, 2020, 7:00 pm

good read thanks help me out

Anabolic - April 12, 2020, 8:05 pm

Yeah this helped some good add-ons and tools. I also got my previous issues all sorted out.

Tangyy - April 14, 2020, 4:06 pm

good post helped me out boss

Ice_Bear - April 16, 2020, 10:13 am

Question, is windscribe any good?

Anton Chigurh - April 17, 2020, 4:57 pm

Thanks for the post. Very good information, helped a lot

Juoku - April 18, 2020, 12:06 am

such an amazing guide mate, loved it!
I'm setting everything up atm :)

knowledge - April 26, 2020, 10:20 am

Wow, I was going through this guide
thank you so much for the info

marcfisher - April 29, 2020, 11:30 pm

Thank you very much for sharing this cool thread !

jassim3003 - April 30, 2020, 5:01 pm

i would recommend using QEMU/KVM for a VM also if u wana be extra secure, with KVM u should have native Speeds pretty good

this thread is pretty good +1

blackke - May 3, 2020, 7:27 pm

Hello and thank you very very much for the time spent into making this guide !

I am researching for days now on security tips and i find this very helpful.

Keep it up !

basseb - May 4, 2020, 8:22 am

Thank you for the post, I learned a lot

MarvinMalware - May 4, 2020, 5:14 pm

Amazing post, well written guide OP.

4751 - May 8, 2020, 3:28 am

This HQ thread will help a lot of people, thanks.

rapponchichi888 - May 16, 2020, 7:33 pm

Alot to digest here.. but thanks for this, great starting point in my journey here :D

dags1968 - May 26, 2020, 6:46 am

Thanks for this! I learned a lot of new privacy.

dan666cuk - May 27, 2020, 9:24 pm

thank you for this....

re-learning this again feels better

Dotexe - June 6, 2020, 2:47 pm

I will just give it a read, thanks for it [SUI-3183372](#) love your content !

renzojj - June 13, 2020, 5:31 pm

how likely will it be for fbi, cia, cops to find someone if they're hacking and following all privacy procedure?

qAzrael - June 19, 2020, 10:39 am

Still one of the better guides on here, highly recommend giving it all a read.

Racks - June 24, 2020, 2:21 am

All this information and still gets arrested by the FBI... Tisk tisk.

lol i'm just pulling your leg, thank you for the valuable information BV1!

Mind - June 28, 2020, 3:07 am

A grade threat mate! I've been looking for a detailed guide like this for some time now

SIM-4772474 - July 5, 2020, 9:34 pm

Most of the content listed here was already known to me. However there were some new things to me and I am thankful for that.

TitoLee - July 11, 2020, 2:17 pm

well tailored.....

A Bad Decision - July 16, 2020, 7:54 pm

I thought I knew a lot of tricks on maintaining my privacy online, but you've given me a few more. Thanks for the thread, it's super useful and I appreciate the hard work you did!

aphotic - July 23, 2020, 3:21 pm

This is chock full of so much useful information, thanks! There's a few things in here I didn't know

about.

cosmos - July 27, 2020, 7:08 pm

ty 100 this info come from God him self hackforum bible , keep blessing us with knowledge

amen

maleekberry - July 28, 2020, 10:13 am

Thanks for this , really enlightened me.

panman - August 26, 2020, 6:45 am

Thanks for the great info

darkcolossus - September 18, 2020, 1:02 am

Wow, amazing post, thank you very much

wanapux - September 23, 2020, 5:37 am

Thank you for interesting Info.

Proxied - September 23, 2020, 3:59 pm

You should mention DNS over HTTPs. Besides that, great information.

10tick - September 25, 2020, 10:48 am

everyone that uses the internet should see this, incredible!

LordDragon - September 26, 2020, 6:43 am

This is a great thread and very informative.

br3adman - November 17, 2020, 12:30 pm

Thank you for interesting Info.

zombie99 - November 20, 2020, 11:25 am

Thank you for update.

Big up

Thank you for update.

very good one

Big up

Thank you for update.

very good one

Big up

person666 - November 22, 2020, 12:26 am

Thank's for this "tutorial bro" thanks a lot :D

N00b5000 - December 2, 2020, 3:50 pm

Thank you so much for compiling and sharing this information. Very helpful!

expl0itzz - December 15, 2020, 11:01 pm

Thanks for the post. Its great to always revisit OPsec i often find my times getting careless sometime

joseph.a2343 - December 23, 2020, 11:20 am

I'm interested in this as well! , thank you

dyss - December 24, 2020, 7:49 pm

thanks for this helpful info

thievish_Rentner - June 12, 2021, 11:50 am

thanks, very helpful, but is it still current? Because it is from 2016.

fukudametro - June 21, 2021, 8:04 am

this is very useful! thanks for posting.

JackSailor - June 21, 2021, 8:06 am

Thanks for the HQ guide!!

True Detective - July 30, 2021, 7:14 am

It would be super interesting if you made a new version of this thread. It's super relevant, and important information.

But a lot things happened since 2016.

Zoeblow23 - August 14, 2021, 9:18 am

I have questions. So a VPN wouldn't be enough?

carngraph - August 15, 2021, 10:22 am

This is a great post - thank you

Scientia - August 27, 2021, 2:41 am

(Aug 16, 2016 07:00 PM)BV1 Wrote: [\[CITE\]](#) Update 10/26/16

Thread will be updated in the coming days.

test

Sorry to bother you in advance sir!

Firstly, very important thread! Secondly, can i "steal" this part for my compendium? :

"This is a broad topic and most of this information isn't coming directly from me, rather it is being compiled from multiple sources. I won't take credit for anything, and I'll attempt to link to sources where I can."

Sincerely, Scientia

SUI-3183372 - August 27, 2021, 9:13 am

(Aug 27, 2021 02:41 AM)Scientia Wrote: [\[CITE\]](#) Sorry to bother you in advance sir!

Firstly, very important thread! Secondly, can i "steal" this part for my compendium? :

"This is a broad topic and most of this information isn't coming directly from me, rather it is being compiled from multiple sources. I won't take credit for anything, and I'll attempt to link to sources where I can."

Sincerely, Scientia

Go ahead and borrow what you'd like. I'm always happy to see privacy tips being shared.

That being said, this thread is pretty dated now. I'd double check to make sure that anything borrowed is still relevant. It was always my intention to update the thread but life got in the way. Haven't had much time for any personal projects lately, let alone a writing project.

kagenomizu - August 27, 2021, 9:29 am

I really enjoyed this. Quite a great read. I am now looking at the various programs. Lots of good intel there. Thanks bro.

homophobiclol - September 6, 2021, 8:31 am

interesting post, thank you for the info

spongebob - September 13, 2021, 8:31 am

Thanks for the share bro. Really interesting info.

-=King=- - September 18, 2021, 6:56 am

Informative & useful . keep up your work .

Gnjak47 - September 19, 2021, 8:23 am

great guide, thank you very much

SIM-4773563 - September 22, 2021, 12:49 am

Nice... Every one of your posts is absolutely great

SynergizerX - October 31, 2021, 4:36 am

This is seriously what I was hoping to find when I came on to the site. You put a lot of clear, and concise information into this guide and I genuinely appreciate it. You goated ?

VNT - January 12, 2022, 1:46 pm

Thanks for the share, i already use some tools listed here but never thought about others ! :)

monkeymoo123123 - February 28, 2022, 9:45 pm

This is good info, but most of it could be bypassed on the local machine by Windows 10 Spying.

MR.L123 - March 2, 2022, 8:21 am

Definitely a good read. Thanks for sharing

nivlac10 - March 8, 2022, 4:09 pm

Great writeup, i believe everyone here in HF can take a page from your book!

pawio92 - March 13, 2022, 12:47 pm

very good job, all informations are clear and bright

OjeandoOjos - March 14, 2022, 5:29 am

That data is amazing. I want to know more of this.

SIM-4497143 - March 19, 2022, 10:12 am

What a amazing thread. Really helped me, I am thankful

Wafflemonger - March 19, 2022, 10:19 am

Seeing as how this was recently bumped, I'll take the opportunity to post on it. This thread, even though quite a number of years old, is surprisingly still extremely relevant. And while there now may be some alternatives to the software, the underlying foundation remains the same. Great post BV1.

EDIT: Still relevant and arguably more important than ever.

Stottts - April 3, 2022, 5:54 am

A lot of this is more relevant than ever these days. Really useful guide, and thanks for putting this together.

lynn x goli - April 10, 2022, 3:51 pm

thank you so much ? this really helped me become more secure +1 vouch thanks once again

N0r3lay - April 23, 2022, 1:45 pm

a lot of the stuff here is good but now in 2022 is out of date (regarding firefox only) I recommend using arkenfox's user.js which can be found on his github.

You should use that user.js template and only use ublockorigin. Firefox has come a long way and deal with loads of stuff there is no longer requirement of many addons.

Additional extra addons makes you even more unique and it adds extra attack surfaces.

Apart from that be careful of what providers/services you use stick with Open source. Use PGP encryption. Try to alter your writing and literacy style to give not accurate stylometry results.

Lobs - May 21, 2022, 9:03 am

Great thread , very detailed.

MoonKairiki - May 22, 2022, 2:27 am

Great job! Was wondering how to protect myself online.

TriPaGonski - May 25, 2022, 2:24 pm

Looks intrressing and awasome

i*am*satan - July 9, 2022, 5:17 am

really appreciate the post

thanks

SIM-5232013 - July 27, 2022, 1:16 pm

Great post! This can be great guidance for beginners.

Seiyoku - July 31, 2022, 1:20 pm

WOW, this is amazing! Super happy to find this!

Thank you!

ModernEHustle - August 12, 2022, 1:53 am

I can tell a lot of time went into this post, it's a great thread I enjoyed the read. Thank you.

triple3 - August 27, 2022, 5:37 am

Thank you for the guide, very useful!

Stogies - September 23, 2022, 1:37 pm

Amazing job, I appreciate your work!

HaD7 - October 1, 2022, 7:01 pm

It is really necessary to understand and put into practice all this very useful thanks

sparkrlight - *October 13, 2022, 8:58 am*

Very informative searching for this kind of information and its complete thanks

paragram - *February 22, 2023, 11:29 am*

Ay man, I love this post but couldn't help notice that simplelogin.io was not added. Its a email alias platform that is open source, I use it very often and I highly recommend it. Most websites seem to block temporary emails nowadays, but simplelogin emails tend to work around 99% of the time. This isnt advertising, just I highly recommend it if you've never tried it before.

Ly_y - *March 22, 2023, 11:36 pm*

thank you for information ... excellent !!

SIM-5296365 - *March 26, 2023, 5:52 am*

Am I able to use veracrypt to crypt a bootable USB drive done with Rufus? Will it still work?

Lavaduck - *April 18, 2023, 6:36 am*

wow this is nice, thank you for all the tips

UnstableKale - *April 28, 2023, 5:14 am*

Thanks for the info!

Ifyg - *May 18, 2023, 11:43 pm*

bookmarked already. a lot of them are still valid after all those years. thanks if you are still around!

locktheballs - *May 19, 2023, 11:22 am*

Thanks for the information. Some of them are unknown for me.

zohar00xc - *May 21, 2023, 3:12 am*

thank you that was very well written

Roku - *May 24, 2023, 5:25 am*

Thanks a lot for the guide!

Anonimsalike - *June 15, 2023, 7:00 pm*

thankyou for the information

SpectreFTP - *June 25, 2023, 1:58 pm*

appreciate the share. very informative.

highboy - *July 1, 2023, 12:37 pm*

You're a lifesaver! Your knowledge-sharing here has saved me hours of frustration. Thanks a bunch for sharing your expertise!

kikou981 - *July 29, 2023, 6:05 am*

nice article thank you very much!!

PANICK3D - *August 2, 2023, 5:25 am*

this is dope and very fuckin detailed thank you so much for this bro

JamesChoe - *August 27, 2023, 12:44 am*

Thanks for this detailed post mate

SUI-3183372 - *August 27, 2023, 12:30 pm*

Outdated guide. Tools listed here may no longer exist, may be broken, or may have changed stances on privacy. Do your own research and proceed at your own risk.