

Forum:[Hack Forums](#)

Thread: [\[DETAILED\] Complete Anonymity/OPSEC Guide](#)

?A?O - July 1, 2015, 2:10 am

Table of Contents

1. Secure Operating Systems
2. Virtual Private Networks
3. TOR Related
4. Encryption
5. File/Download Security
6. Social Related
7. General Computer Security
8. Useful Guides/Threads

Preface *NOTE* Nothing will 100% secure you online, this is only meant to help.

This guide is here to help the general user better understand some aspects of anonymity. I understand there are more advanced methods but I thought this content would be most suitable for the users of HackForums as a whole. I also plan on updating this thread when newer methods and content become available or more widely used.

Disclaimer

I take no responsibility if this information or these methods do not prevent you from getting caught doing something you shouldn't have been doing to begin with.

Secure Operating Systems

Aside from the normal, everyday Windows, Macintosh, or Linux distros, these are operating systems that are renowned for the security pre-built within them.

Tails

Tails, also known as The Amnesic Incognito Live System, is an open-source OS designed to predominantly be ran via live disc like a CD/DVD, USB, or SD card. The main operation of Tails is aimed at keeping your privacy and anonymity safe while leaving as little trace of use as possible. Since it is an amnesiac OS, nothing is left behind every time you reboot such as save files, new software, and realistically leaves a clean slate when you need to power down. Tails default networking application is TOR (TheOnionRouter) which allows the user to stay encrypted through whatever network they are currently connected to. Many of Tails pre-installed software come pre-configured with security in mind such as the Pidgin IM client which is setup up with OTR for Off-the-Record Messaging or the TOR Browser with all the necessary plugins already added into it. There are many more features to this amazing OS found on their website.

Tails Link: <https://tails.boum.org/>

Whonix

Whonix is another operating system which is aimed on your privacy, security, and anonymity. It is based on three things: The TOR network, Debian Linux, and security by isolation. The creator's of Whonix stand by the fact that DNS leaks are not possible and malware with root privileges can not find out the user's real IP according to their website. There are two different parts to Whonix itself: Whonix-Gateway & Whonix-Workstation which is on a completely isolated network with TOR as its only connection possibilities. The Whonix-Gateway is exactly as it sounds, the gateway to the internet and all TOR connections. The Whonix-Workstation is the actual desktop environment you

as a user will interact with during daily usage. The two parts of Whonix sync with each other to make sure the connection is secure as possible while also making sure the two are coinciding correctly. This OS is mainly used within Virtual Machines but can be applied in many different ways. ADD-IN WHONIX PIC SPOILER.

Whonix Link: <https://www.whonix.org/>

Virtual Machine Software

VMware Link: <https://my.vmware.com/web/vmware/downloads>

VirtualBox Link: <https://www.virtualbox.org/wiki/Downloads>

USB Live Disc Software

Win32 Disk Imager: <http://sourceforge.net/projects/win32diskimager/>

Will add more Live Disc Software.

Virtual Private Networks (VPNs)

Virtual Private Networks intertwine a private network into a public network. This enables the user's computer or personal device to send and receive encrypted data as if it were connected directly to the private network. VPNs are created by making a virtual point-to-point connection through the use of dedicated connections and traffic encryption. Here is my list of the VPNs I believe to be good enough for the average user.

Note All VPN's listed advertise that they keep ZERO logs of what users do while accessing the VPN.

Proxy.sh

Proxy.sh is a well known and reputable Seychelles-based VPN with a very friendly graphical user interface. This VPN comes with truly offshore locations with the option to have discrete onshore tunneling if wanted. Besides being compatible with just about every OS and device platform out there, Proxy.sh comes alongside Safejumper, a custom OpenVPN client with many benefits. Proxy.sh is also known for having a huge array of payment options available, 80+ different options, and only requiring an email along with the payment. They offer a few varying packages to choose from but from personal experience, I'd suggest going with at least their Basic package because it starts giving you more node (location) options to choose from. Proxy.sh has 24/7 customer service and ticketing system which you may access from their control panel on the website.

Proxy.sh Link: <https://proxy.sh>

Private Internet Access

Private Internet Access, also known as PIA, is a very common VPN used by many due to how easy it is to use and select features and options. PIA boasts about its many layers of security including IP cloaking, strong encryption, firewall, identity protection, and uncensored access anywhere. In addition to this, PIA uses PPTP, OpenVPN, IPSEC/L2TP, and SOCKS5 (proxy). One of the reasons I like this VPN is due to the options you can choose from simply through the GUI located in your active task-bar. By right clicking the GUI, you can choose your data encryption, data authentication, handshake, DNS leak protection, VPN kill switch, node locations, and many more options. PIA is another VPN that is compatible with most OS's and devices. Even with all the features this VPN comes with, it is on the cheaper side only being \$6.95 a month if you pay month by month and accepts all major payment options.

PIA Link: <https://www.privateinternetaccess.com>

ZorroVPN

ZorroVPN is the lesser known of these VPNs but is just as secure if not more secure than others. Zorro's main features include AES-256 encryption, 4096-bit authentication keys, switching IP on-the-fly, VPN chains (DoubleVPN, TripleVPN, QuadroVPN), and the ability to set the VPN to "Tor" which allows you to transparently connect to the TOR network. The main downside to ZorroVPN is the limited payment options which used to only accept Bitcoin but now expanded to other options including PayPal & Credit Card with only an email being needed alongside the payment. One thing ZorroVPN states specifically is "ZorroVPN is independent service and it's out of jurisdiction of any government" which may show the thought into how much they care for your privacy and security. ZorroVPN is compatible with most common Windows, Linux, and mobile devices.

ZorroVPN Link: <https://zorrovpn.com/>

Other Notable VPNs (for additional levels of security)

CryptoStorm Link: <https://cryptostorm.is/>

DNS Leaking

While you are on a VPN, you want all traffic coming from your computer to go through the encrypted network. If any of your traffic leaks outside this encrypted network, people can then log that information which is not good at all. The Domain Name System (DNS) translates domain names such as HackForums.net into IP addresses such as 190.93.250.145 which is required to send packets of data on the Internet. When you try to access a specific website, before you go there your computer must interact with the DNS server to request the IP address. Internet service providers (ISPs) usually use specific DNS servers which log and record specific activities you do while on the Internet. The main issue here is when you use a VPN, sometimes the OS will default to the normal DNS servers instead of the DNS servers your VPN provides. DNS leaks while using a VPN can make you feel safe while you are truly leaking data that you don't want leaked. This is a major issue which is why all VPNs I listed above have some sort of DNS Leak protection, a must have when stay anonymous. You can test to see if you are DNS leaking at the links below.

IPLeak Link: <https://ipleak.net/>

LeakTest Link: <https://www.dnsleaktest.com/>

For anyone not using a VPN with DNS Leak Protection, try using one of these DNS servers:

OpenDNS: 208.67.222.222 and 208.67.220.220

ComodoDNS: 156.154.70.22 and 156.154.71.22

UltraDNS: 156.154.70.1 and 156.154.71.1

NortonDNS: 198.153.192.1 and 198.153.194.1

SOCKS4/SOCKS5 Servers

SOCKS, which stands for Socket Secure, is an Internet Protocol that routes network packets between a client and server through a proxy server and allows you for sessions to traverse securely across firewall security. SOCKS4 & 5 are different types that do slightly different things. The main difference between the two is SOCKS4 only supports TCP application while SOCKS5 supports both TCP and UDP. With added supports, authentication methods, and domain name resolution, the main outgoing SOCKS proxy are SOCKS4 proxy. You won't be able to use UDP applications but it will be to your benefit overall. So if you are in need of a proxy instead of a VPN for a specific application, try to keep this in mind.

Tor Related

What is Tor?

Tor, which stands for 'The Onion Router', is a non-profit group of volunteer-operated servers that allows people to improve their privacy, privacy tools, and security on the Internet. The Tor network works by moving your traffic across various nodes through a series of virtual tunnels rather than making a direct connection, allowing anyone to share vital information without compromising one's

identity. Anyone trying to trace you would see the traffic going through various Tor nodes on the network rather than directly from your computer. All that is needed to access the Tor network and .onion links (hidden service sites only accessible on Tor network) is the Tor Browser. The Tor Browser comes ready to use and routes everything you do through the Tor network without any configuration needed although I'd recommend a few steps to take which you will see later in this thread.

Tor Benefits

Tor has many benefits for all kinds of privacy issues people face in the world we live in. Many journalists, hackers, or people living in a dictatorship with a lot of censorship can use the Tor network to anonymize your traffic and access sites you may not have been able to before all while being absolutely FREE. Tor is also very useful for anyone looking to keep their online activity hidden from other people or your ISP. Tor can also be used to host sites which contain hidden services only accessible by other Tor users and sometimes needing an invitation to access for added security.

Browser Configuration

Although the Tor Browser comes pre-configured and can be used right away, there are a few more steps that people should take to secure it even more. Here is a list of addons which should be used within the Tor browser:

NoScript - an open source FireFox extension which allows you to restrict JavaScript, Java, Flash, and other plugins from only being executed by trusted web sites of your choice. Tor already has this installed in its browser by default but there are a few settings which you will need to enable/change. Firstly, open up the NoScript options and go to the Embeddings tab. From here you want to make sure everything on that page is checked on. Then, we are going to go to the Advanced tab. When there, go to the Untrusted sub-tab and make sure everything is checked on. Your NoScript is now more secure than the default configuration.

Ghostery - Ghostery is a privacy based browser extension used to block specific tracking cookies along various sites. Ghostery does not come pre-installed on the Tor browser so download it from the addon page in the browser by searching it. Once installed, we have to change some things. Once installed, clicked the Ghost icon located on the browser toolbar and once the Ghostery mini-page pops up, click the gear wheel in the upper-right hand corner and go to options. Under sharing options, make sure GhostRank is disabled. Scroll down to the bottom where you see three tabs: Trackers, Cookies, & Whitelisted Sites. Make sure your on the Trackers tab and check everything on (should be 5). After doing that, make sure to click SAVE at the bottom of the page or this will not stay configured correctly.

RefControl - RefControl is an extension for FireFox that lets you control what things gets sent as the HTTP Referer on a per-site basis. Basically, when you access a site, you may not want a webmaster to know where exactly you found the link to access their site. This mitigates that completely.

HTTPS Everywhere - HTTPS Everywhere is an open-source extension created in collaboration by the Tor Project and the Electronic Frontier Foundation. It allows you to automatically make any website which supports HTTPS, use the secure HTTPS connection instead of the normal HTTP.

Disconnect - Disconnect is an open source addon which allows you to visualize and block invisible websites that track both your search and browsing history. On top of that, this also allows your page to load faster. Just make sure all sites are blacklisted at all times.

Search Engine - Although many people use Google as their main search engine for normal web

browsing, Google shows a lack of care for users privacy in general. Also, Google is notorious for tracking clicks on result pages that you search with alongside sometimes having you log into GMail to access certain things. To prevent that here are a few search engines you can set to default instead. DuckDuckGo.com
Ixquick.com
Etools.ch

WebRTC Fix - This fixes a big security hole that can reveal your IP address to websites through WebRTC. Regardless if you're on Tor or on a VPN, if your browser doesn't prevent this, someone can still grab your real IP behind all that security. To fix this issue, open up your Tor Browser and type "about:config" into the URL bar. After doing that, in the search bar, search for "media.peerconnection.enabled" and make sure it is set to FALSE. You will then be set.

Another suggested extension but not needed is AdblockPlus.

Exit Node Security Warning

One thing I need to talk about is how other entities may be able to see your traffic over the Tor network. On Tor, instead of taking a direct route from your computer to the destination, the Tor network routes a random path through many Tor relays to encrypt and hide your data. Once your at the last relay of the path, this is called the exit node. The exit node is the one that actually makes the connection to the destination server. Tor, by design, cannot encrypt data between the exit node and destination server so whoever may be in control of the exit node has the ability to capture the traffic passing through it. The best way to combat this is to use End-to-End encryption which I will explain more about in the Encryption section later on in this thread.

Invisible Internet Project (I2P)

I wasn't sure about adding this in but I think it needs to be explained and talked about a little bit. I2P is a decentralized anonymizing network built on similar principles to Tor except was designed to be a self-contained darknet. Users still connect using P2P encrypted tunnels but there are still many differences. Distributed peer-to-peer model.

- Garlic routing (encrypts multiple messages together, harder traffic analysis).

- Uni-directional tunnels so incoming and outgoing traffic are seperate.

- Uses packet switching instead of circuit switching.

- Uses its own API rather than SOCKS like Tor. This makes it technically more secure than Tor.

Aside from being very secure, it will also be much faster than Tor overall. The best way to explain I2P is as a internet within an internet. One thing to mention is I2P does not hide the fact you are using the service at all. If you don't like Tor for some reason, this is another option to check out.

I2P Link: <https://geti2p.net/en/>

?A?O - July 1, 2015, 2:11 am

Tor through VPN vs. VPN through Tor

Many people aren't aware that by using these in different orders really alters your privacy/anonymity quite a bit. Here I'll talk about the pros and cons of each side along with my final thought on the matter.

Tor through VPN - This is the method most people use because of it's convenience. The connection for this way of doing things is: Your Computer -> VPN -> Tor -> Internet. This is what it looks like when you connect to Tor while already on a VPN, since most people always have a VPN turned on already. One of the main advantages to this is that you can keep Tor hidden from your ISP, but your ISP will instead see you using a VPN which in most cases is much better. Also, if you're going through a bad Tor exit node, if you're using a good VPN, they will not keep logs yet still keep your data encrypted as well. The main disadvantage to this method is that a malicious Tor exit node can still monitor your traffic and trace it back to the VPN provider. This will be okay so long as your VPN provider keeps no logs or IP addresses of clients. The only other downside is that a lot of exit nodes

on Tor will be blocked while using a VPN in this manner. This method mainly rides on how much you trust your VPN provider, otherwise is a very safe option.

VPN through Tor - This is a less used method but still used by many. The connection using this method looks like this: Your Computer -> encrypt with VPN -> Tor -> VPN -> Internet. The only way for this method is to use a VPN client which works directly with Tor and only two known VPNs work with Tor in this way: [AirVPN](#) and [BolehVPN](#). This method really doesn't have any cons to it, only pros. The first pro being that because you are connecting to the VPN server through Tor, even the VPN provider will have no idea what your real IP address is. If you were to pay with BTC and use this method, there would be absolutely no way for the VPN provider to identify you in anyway. This method bypasses all blocks on Tor exit nodes as well as making all traffic through the Tor exit nodes completely encrypted. Finally, this method allows for geo-spoofing (Geo-Location) since you can choose the server location.

Overall, both methods of connection are going to be more secure then only using one. My suggesting would be to use the first method since it is convenient but only if you really trust your VPN provider. If you don't and want added security, use the second method which ensures that none of your privacy or anonymity will be compromised.

Tor Bridges

Tor Bridges (Bridge Relays) are Tor Relays that aren't listed on the main Tor directory. The main reason to use Tor Bridges is if you think your Tor connection is being blocked by something such as your ISP because even if they were to filter all the connections of known Tor relays, all bridges will not be blocked. I'm not going to go in-depth into this but I will leave a few links to find out where to get Bridge Relay IPs and how to install/configure them correctly.

Configuration Link: <https://www.torproject.org/docs/bridges.html.en>

Bridge Relays: <https://bridges.torproject.org/>

Proxychains with Tor

Proxychains is a tool that takes all TCP connections made by an application and pulls them through a proxy like Tor or SOCKS4/5 proxies. The cool thing about proxychains is you can have a random order and as many proxies as you want. It works with all applications but in this case, we'll be talking about it directly interacting with Tor. Most people use Proxychains on Linux OS's but you can use a program like [Proxifier](#) to do the same on Windows. By using Proxychains alongside Tor, it allows you to have an extra hop after the exit node before getting to the destination. This way, it doesn't look sketchy if you are leaving a French exit node and going to a US destination because with Proxychains, you can come from the French exit node, to a US proxy, then to the US destination making it much smoother overall. Here is are a few links to install/configure Proxychains, proxy lists, and how to check blacklists.

Proxychains Guide:

<http://null-byte.wonderhowto.com/how-to/hack-like-pro-evade-detection-using-proxychains-0154619/>

Socks Providers: [Vip72](#) & [WinSocks](#)

Blacklists: [IP-Score](#) & [Whoer](#)

Tortilla

Tortilla is an open source tool which users can use to transparently and securely route all TCP/IP and DNS traffic through Tor, regardless of client software, and without relying on VPNs or additional hardware or virtual machines. When this first came out, the creator pointed out two very undeniable facts about this tool. One, that it fixes "the Firefox problem" which is that FireFox has a ton of new vulnerabilities being discovered throughout each year which is a big security flaw. Two, being able to untangle the SOCKS server issue which wasn't allowing users to use TCP proxying via SOCKS. Tortilla solves these issues and allows Tor to be used with virtual machines which is why this tool works so well with TailsOS and can allow you to connect to Tor over top of Tor. This is software I

haven't fully tested yet and will update with more if needed.

Tortilla Link: <http://www.crowdstrike.com/community-tools/>

Tortilla Github: <https://github.com/CrowdStrike/Tortilla>

Tor over the top of Tor:

<https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/how-to-connect-to-tor-over-to-p-of-tor/>

Encryption

Encryption is a vital part of computer security when it comes to important documents, personal data, or internet traffic. It allows you to securely protect data that you don't want anyone else to see or have access to. When it comes to privacy and anonymity, encryption plays one of the most important roles possible for securing data being transferred over the internet. Here are just a few types of encryption which everyone should be using.

PGP Encryption

PGP, Pretty Good Privacy, is a program used for the encryption/decryption of email over the Internet but also serves as a way to authenticate messages with digital signatures and encrypted stored files. PGP uses a variant on the public key system. It starts with each user having an encryption key that is publicly known and a private key only that user has. Each person sends a message, encrypting it with their public key. Then when the message is received, the message is decrypted using the user's private key. To make this the encryption process much faster, PGP uses an algorithm which encrypts the message, then uses the public key to encrypt the shorter key. There are two versions of PGP available: RSA & Diffie-Hellman. Both of these have different algorithms for encryption but as just as secure as the other. Sending digital signatures is a similar process but creates a hash using the user's name and other signature information. The hash is encrypted with the user's private key. The recipient uses the sender's public key to decrypt the hash code. If it matches, the recipient knows that this is an authentic file.

Here are some links to PGP software and guides.

Guide on PGP: <http://www.bitcoinnotbombs.com/beginners-guide-to-gpg/>

Guide on File Encryption with GPG: <https://hackforums.net/showthread.php?tid=4600720> - .Web

GNU Privacy Guard (alternative): <https://www.gnupg.org/>

GPG for Windows: <http://www.gpg4win.org/>

GPG for USB: <http://www.gpg4usb.org/>

Another good site but is currently invite only is Keybase.io which allows you to confirm someone else's PGP key, fingerprint, BTC address, social media accounts, etc.

Keybase: <https://keybase.io/>

Whole Disk Encryption

Disk encryption is software which protects your information by turning it into unreadable code which can't be cracked easily by unwanted users. Disk encryption uses specific software or hardware to encrypt all data that goes on a disk or a disk volume. Whole disk encryption is when everything on the disk is encrypted as well as all the programs that can encrypt bootable OS partitions. One thing to note is computers using Master Boot Record (MBR) will NOT have that part of the disk encrypted. Whole disk encryption has many benefits to it. Number one is ALL parts of the disk are encrypted, even the swap space and temporary files which may contain sensitive information. By using full disk encryption, you don't have the chance of accidentally not encrypting a file since everything is indeed encrypted regardless. Lastly, by destroying the cryptography keys, it will render the data completely useless. It's not needed on everybody's computers since everyone has different need, but definitely recommended. Most people have used software called TrueCrypt in the past but that software is no longer being developed. Instead, new software called VeraCrypt has taken its place and is a very

useful encryption tool.

VeraCrypt Link: <https://veracrypt.codeplex.com/>

Another good piece of encryption software is DiskCryptor which has similar functions to VeraCrypt.

Diskcryptor Link: <https://diskcryptor.net/wiki/Downloads>

Disk Encryption Wiki Info: https://wiki.archlinux.org/index.php/Disk_encryption

Warning Please make sure to backup your entire system before attempting to do whole disk encryption in the case of a failure during the process.

File Encryption

File encryption follows the same procedure as whole disk encryption but instead of the whole disk, you are specifically encrypting an individual file or a whole folder. File encryption is a much simpler process than whole disk encryption and can be done with the same software, VeraCrypt. One thing to note is that with VeraCrypt, you can make a much larger encrypted volume (basically extra storage) to put files in and encrypt it as a whole. For instance, I have an external hard-drive which I made a 200GB encrypted volume for so once I type the password for that volume, I can drop anything in and close it. It will now be encrypted until I unlock that volume at another point in time. Here is a guide on how to use it with another VeraCrypt download link.

VeraCrypt Link: <https://veracrypt.codeplex.com/>

VeraCrypt Guide: <https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial>

Encrypted Backups

I won't be saying much about backups but I suggest everyone to keep backs and then encrypt them with this software for added security and to have that safety of being able to restore your system if something were to go wrong.

File/Download Security

File and download security is not something the average user thinks about which is why I wanted to write this section to explain a little bit about it. Hopefully after reading this section you'll understand more about why file and download security should be a higher priority than most since it's something the average user will use most.

Metadata

Metadata is data that describes other data. Now that may sound confusing but think about it from a file's perspective. Author, date created, date modified, and file size are simple examples of metadata that almost all documents carry. On top of that, images, videos, Excel sheets, and web pages all carry their own personalized metadata. Metadata is something which could easily give away personal information that you wouldn't even realize is there. The biggest one that people don't realize is simple pictures taken on your cellphone camera. Here is an example of EXIF (exchangeable image file format) data which shows exactly some of the metadata you'd find within a picture taken on a cellphone:

There is a lot more information where that came from. Depending on if you have location on or not, metadata can even give GPS coordinates of where the picture was taken. All files contain this sensitive information within them and most people don't even realize it exists. Thankfully, there are tools out there which can be used to find and delete that information from files. This software is called MAT: Metadata Anonymization Toolkit and will help aid in the removal of metadata from the files that you want to clean.

MAT Link: <https://mat.boum.org/>

Deleting Files/Information Correctly

I feel like there are many users currently out there who think that by simply deleting a file, it's magically gone from your computer. This is NOT true! When you delete something from your computer, the only thing you are doing is deleting where it was located on the drive. It's still within the drive but the location data is no longer there. This is the reason why file recovery software exists, to grab those files you "deleted" and get them back. The correct way to delete something (file shredding) is by overwriting the data. One thing you must understand is that by overwriting previous data/files, this doesn't remove a file's location but instead makes it unrecoverable. For the average user, overwriting a file once should be enough although the NSA recommends 3 times, while the DoD recommends 7 times. It all comes down to preference but some people believe that when you only go over a file once, you miss some of the data so by going over it many times, you get rid of the data that is left over. Here are some of the tools many people use for correct file cleaning and deletion.

Darik's Boot and Nuke: <http://www.dban.org/>

File Shredder: <http://www.fileshreder.org/>

CCleaner: <https://www.piriform.com/ccleaner>

For people who want an extra step to stay safe, every time you empty your recycling bin, you should shred all files within it.

MD5/SHA-1 Checksums

Before learning what a checksum is, you first need to know what MD5 & SHA-1 are first. MD5 & SHA-1 are common cryptographic hash functions with MD5 being a 128-bit (16-byte) hash value while SHA-1 is a 160-bit (20-byte) hash value. With these two hash types, we can use them to verify data integrity of a file/download. After downloading a file or software is when you are able to check the checksum of the file. The checksum is where the contents of the file get thrown into a mathematical algorithm and output a specific MD5/SHA-1 string. This method of verifying downloads/files is not as good as PGP + signature file but if you cannot use that method, this is a good second. Almost all Linux distros have the commands sha1sum and md5sum built into it. All you do is run these commands against the file in question and it will output the checksum string for you. Once you do this, all you do is compare that to what the download should have been and you should be able to verify if the download was authentic or not. For most users who use Windows, I will leave a link for you to Microsoft's own checksum integrity verifier.

Windows Checksum Link: <https://www.microsoft.com/en-ca/download/details.aspx?id=11533>

MD5/SHA-1 Hash Verification Software:

<https://www.raymond.cc/blog/7-tools-verify-file-integrity-using-md5-sha1-hashes/>

One thing to note is that MD5 has known collisions. With enough force, this allows MD5 to be broken into.

?A?O - July 1, 2015, 2:12 am

Social Related

Within this section I will be talking about everything related to interacting with people socially via messaging of some sorts. This section is my opinion on what should be used and may differ from person to person. This will give you a general idea of what you want to be doing while using social related messaging services.

XMPP

XMPP stands for Extensible Messaging and Presence Protocol and is used for communications for message-oriented middleware based on the Extensible Markup Language (XML). Many more people are starting to use this as a main way of communication using programs such as Pidgin to accomplish this. Pidgin is an open-source multi-platform IM client which most people will recommend for XMPP. The main reason is because Pidgin has a simple plugin which you can

download that allows you to incorporate Off-the-Record (OTR) messaging into it. OTR allows you to have private conversations over XMPP by using encryption, authentication, and the fact that messages you send do not have digital signatures that a third party can check for. This is a must use plugin/step you need when using any type of XMPP client.

Pidgin Link: <https://pidgin.im/>

Pidgin Secure Messaging Guide: <https://securityinabox.org/en/guide/pidgin/windows>

Good XMPP Servers

- riseup.net

- xmpp.ninja

- darkness.su

- captio.ch

- thedark.army

IRC

IRC, which stands for Internet Relay Chat, is an application layer protocol that facilitates the transfer of messages in the form of text. IRC has been around for a very long time but is still widely used by people all over. Most IRCs consist of a community or group of people with a specific goal/topic in mind. To connect to a specific IRC, you need two main things: the IP to the server and the channel (which has a # in front of it like #channel). There are plenty of public IRCs but most will be private depending on the topic of conversation. When it comes to security and IRC, there are more steps that need to be taken than with XMPP, so I will link a good guide to follow when setting up IRC and explain some good IRC clients to use.

IRC Clients

- X-chat

- mIRC

- HexChat

- irssi (Linux cli)

IRC Anonymity Guide: https://encrypteverything.ca/IRC_Anonymity_Guide

Skype

Skype is an application that specializes in video chat and voice calls from pretty much any device out there and also allows for text IM as well. Skype is by far the most insecure IM method but since people tend to use this a majority of time, I figured I'd give you a few examples of what you should do. The main issue I see people having is having their Skype resolved giving someone your IP. The first thing that should be done is changing a single setting on the Skype client itself. Once in the client, go to Tools -> Options -> Advanced Tab -> Connection, then within the Connection section, make sure to check mark the box that says, "Allow direct connections to your contacts only." This will help against most online resolvers but not ones which have a DB of old IP entries. To make sure you are even more safe with Skype, one thing I recommend is blacklisting your Skype account on the main Skype resolvers people use. Yes it will cost a little bit of money but in the end will benefit you completely. Another thing to note you should never go on Skype unless you are currently on a VPN or have Skype setup with SOCKS5 proxies.

Sites to Blacklist Skype From

- Skypegrab

- ResolveItPLZ

- GoResolver

Secure Email Providers

There is no such thing as a 100% secure email although there are email providers out there that take security much more seriously than others. Many of which have much more encryption, multiple authentication types, secure servers, etc. Here is the list of email providers which I believe are more secure than the average email provider such as Gmail or Hotmail. Also, if you need to send an email

but don't want to create a new one, there are such things as throw away emails which you can use that automatically are destroyed after sending a message or a certain amount of time.

Email Providers
protonmail.ch
mail.riseup.net
cryptoheaven.com
GnuPG - for any email service

General Computer Security

This is a section I just wanted to throw in to have my opinion on security related applications for both Windows and Linux. This doesn't have to do with anonymity but will help users who aren't sure what type of applications they should use when browsing the web and making sure they don't get infected as much as they may have using crappy software.

Anti-Virus
Comodo Internet Security Pro (recommended)
Bitdefender Total Security
ESET Nod32 Smart Security

Active Applications
Hitman.Pro Alert (a must have)
KeyScrambler Pro
Malwarebytes Anti-Exploit

Other Applications to Have
CCleaner
Malwarebytes Anti-Malware
RogueKillerX64
Spybot-S&D

Linux Applications
Lynis
ClamAV
rkhunter

Useful Guides/Threads

For the last section I just wanted to add links to guides, threads, and sites I thought users would find useful or things I may not have had enough space in this thread to write about

[OPSEC for Hackers](#) - grugq
[Opt out of global data surveillance](#) - prism-break.org
[Forensic Fails](#) - Defcon 21 Talk
[Dropping Docs on Darknets](#) - Defcon PDF
[NSA-proof your email in 2 hours](#) - sealedabstract
[Tor Operations Security](#) - cryptome
[Advanced Anonymity \(packet steganography\)](#) - crazyycast13

I will constantly be upgrading this thread whenever possible. If you feel as though you think something should be added, please feel free to PM me.

?A?O - July 1, 2015, 2:14 am

This is the first placeholder post.

Goodies - July 1, 2015, 2:16 am

Vouch. Good luck with sales.

Th3PonyWizard - July 16, 2015, 9:48 am

Incredibly detailed, bravo it is :)

Vinnie - July 16, 2015, 10:47 am

Good shit too bad the forum is full of retards and nobody will understand this even though it's in plaintext

Aurora - July 16, 2015, 8:30 pm

An incredibly high quality guide. Appreciate the amount of effort you put into this zer0.

PhantomElite - July 16, 2015, 8:33 pm

Really nice post, looked over it and is HQ.

Also one thing to note is that if you get a bad exit node, not only can they sniff your traffic, but apparently they have been known to maliciously patch your Tor downloads. This makes checksums even more important I suppose.

One question: How do you deal with Tor blocks and stuff for websites, especially with Whonix? A problem I don't have the solution to.

ZuGgY - July 16, 2015, 8:36 pm

Bookmarked. Very nice and high quality tutorial IMO.

Thank you mate!

grady - July 16, 2015, 8:37 pm

Why isn't this guide encrypted?

You'll have the NSA on our ass now.

?A?O - July 16, 2015, 8:40 pm

(Jul 16, 2015 08:33 PM)PhantomElite Wrote: [\[CITE\]](#) Really nice post, looked over it and is HQ.

Also one thing to note is that if you get a bad exit node, not only can they sniff your traffic, but apparently they have been known to maliciously patch your Tor downloads. This makes checksums even more important I suppose.

One question: How do you deal with Tor blocks and stuff for websites, especially with Whonix? A problem I don't have the solution to.

I'll try to answer some questions tomorrow. Also a thing to note is since Null is closing, I kind of rushed parts of this so that I could get it out of the sub-forum and into the public forum. Tomorrow I'll be editing, adding, taking out parts, etc. Feel free to leave any feedback, I plan on constantly editing this thread whenever possible.

Schatten - July 16, 2015, 8:43 pm

Great tutorial, everything is nice except exploit.im isn't a good XMPP service as it's been rooted many times.

Rokushi - July 16, 2015, 8:45 pm

Not even Omni post got 5 star rating lmao good shit Zer0, I hope some people learn from this (:

SILVERHAWK - July 16, 2015, 8:47 pm

Subscribed to the thread. Best info I have read on here for being invisible on the web!

Awesome job mate!

SILVERHAWK

l33tsec - July 16, 2015, 8:58 pm

I would also like to recommend the following tools for OSX users:

Little Snitch 3

Personal firewall for outgoing connections. Must have.
obdev.at/products/littlesnitch/index-en.html

Micro Snitch

New tool which protects from cam/mic spying.
obdev.at/products/microsnitch/index-en.html

OSX Rkhunter

Rkhunter version for OSX with UI and updater.
antirootkit.com/software/OS-X-Rootkit-Hunter.htm

Stay safe!

HIGH PAID FELLA - July 16, 2015, 9:06 pm

You didn't cover everything, but that's normal since that would be a ton.
Don't forget to mention web.skype, another server list for XMPP.

WebRTC isn't a bug/exploit/w.e, it's just something based on three things mainly:
getUserMedia, PeerConnection and DataChannels just to retrieve data or get access to third party hardware from browser. Only Firefox, Google Chrome* and Opera* support it.
(* = partly supported)

For PGP I would suggest adding keybase.io to confirm somebody's PGP key, fingerprint, bitcoin address, twitter, github, reddit, etc.

Regarding disk encryption I would add DiskCryptor as an alternative.

For IRC try always to use SSL on port 6697 so your chat/text is not plain text.
A web-based IRC client could be Kiwiirc or Mubbit.

For e-mail I would add the tip to setup your own mail server and to warn people for killer.org, people have been saying they steal e-mail's and other data from their users.

An alternative for Hitman.Pro would be Malwarebytes Anti-exploit.

Really, you could write a book of 1000 pages regarding OPSec and online security but this is a good sum of basic information to have in mind.

Also the usage of iOS is very bad since the applications can ignore the PTPP settings or any other VPN or proxy.

?A?O - July 16, 2015, 9:07 pm

(Jul 16, 2015 08:58 PM)l33tsec Wrote: [\[CITE\]](#) I would also like to recommend the following tools for OSX users:

Little Snitch 3

Personal firewall for outgoing connections. Must have.
obdev.at/products/littlesnitch/index-en.html

Micro Snitch

New tool which protects from cam/mic spying.
obdev.at/products/microsnitch/index-en.html

OSX Rkhunter
Rkhunter version for OSX with UI and updater.
antirootkit.com/software/OS-X-Rootkit-Hunter.htm

Stay safe!

I'll check those out. I'll be honest, not a big OSX guy so anything I could add to this I'll look into.

PhantomElite - July 16, 2015, 9:09 pm

Also as a suggestion maybe sometime later on you could add a section on the more physical bits of OPSEC. Like what network to use, not bragging, not making a DPR mistake and using your email on shit. But this guide seems more technical in nature so if you want to keep it that way that's fine.

?A?O - July 16, 2015, 9:13 pm

(Jul 16, 2015 09:06 PM)Asterea Wrote: [\[CITE\]](#) -snip-

I'll go through some of this tomorrow. Like I said, some of it was rushed due to Null going up for sale but another part of it is opinion based. When it comes to the amount of detail, I could go very in-depth but if I did, it would of been 10+ posts long. It was actual hard to condense the most important information into the thread but any feedback I get will be look at and the thread will be constantly modified.

HIGH PAID FELLA - July 16, 2015, 9:14 pm

(Jul 16, 2015 09:13 PM)zer0 ? Wrote: [\[CITE\]](#) I'll go through some of this tomorrow. Like I said, some of it was rushed due to Null going up for sale but another part of it is opinion based. When it comes to the amount of detail, I could go very in-depth but if I did, it would of been 10+ posts long. It was actual hard to condense the most important information into the thread but any feedback I get will be look at and the thread will be constantly modified.

Alright, great to hear. Maybe parse all this information in a book in PDF format?

?A?O - July 16, 2015, 9:26 pm

(Jul 16, 2015 09:14 PM)Asterea Wrote: [\[CITE\]](#) Alright, great to hear. Maybe parse all this information in a book in PDF format?

I was thinking about doing this, once again the whole Null being sold made me rush so still plenty of things need to be added, configured, editing, etc. Tomorrow I plan on working out a lot of the kinks and looking at anything users have to say about the thread and ideas.

HIGH PAID FELLA - July 16, 2015, 9:30 pm

(Jul 16, 2015 09:26 PM)zer0 ? Wrote: [\[CITE\]](#) I was thinking about doing this, once again the whole Null being sold made me rush so still plenty of things need to be added, configured, editing, etc. Tomorrow I plan on working out a lot of the kinks and looking at anything users have to say about the thread and ideas.

If you need any help regarding subjects or things needing to get added in your book I won't hesitate to help you.

Emoticon - July 17, 2015, 2:02 am

How in the FUCK is exploit.im a good XMPP server?

<https://xmpp.net/result.php?domain=exploit.im&type=client>

Read in detail at how horrid it is.

Other than this, awesome and informative content.

For anyone that wants a good, privacy-supportive XMPP server, I own pod.so :^)

Perfectionist - July 17, 2015, 2:21 am

Bookmarked as I will continue reading this later. And thanks for telling about the different programs, I'll download a few of those for sure.

Mcbride - July 17, 2015, 3:20 am

Bookmarked. Learned a thing or two and linking required software? Brilliant! Very detailed as said thanks OP

Catfruit - July 17, 2015, 6:04 am

Wow, This helped me a lot!

Incredibly detailed and well written, You really do know how to teach people your stuff.

It's very easy to understand and easy to apply! And once again! Thanks! This is awesome!

sinmar - July 17, 2015, 6:26 am

I'd recommend adding [obfsproxy](#) which disguises Tor traffic using multiple methods.

(Jul 17, 2015 02:02 AM)Xerucide Wrote: [\[CITE\]](#) How in the FUCK is exploit.im a good XMPP server?
<https://xmpp.net/result.php?domain=exploit.im&type=client>

Read in detail at how horrid it is.

Other than this, awesome and informative content.

For anyone that wants a good, privacy-supportive XMPP server, I own pod.so :^)
you do realize that's only because of ssl

HIGH PAID FELLA - July 17, 2015, 6:29 am

(Jul 17, 2015 06:26 AM)sinmar Wrote: [\[CITE\]](#) I'd recommend adding [obfsproxy](#) which disguises Tor traffic using multiple methods.

you do realize that's only because of ssl

Yeah, my server is also perfectly setup using s2s, c2s and forced encryption but it gives me a F because I use a self-signed SSL which is ridiculous.

Emoticon - July 17, 2015, 8:48 am

(Jul 17, 2015 06:26 AM)sinmar Wrote: [\[CITE\]](#) I'd recommend adding [obfsproxy](#) which disguises Tor traffic using multiple methods.

you do realize that's only because of ssl

So it's alright to accept plaintext passwords pre-TLS?

You do realize Exploit.IM also stores passwords in plaintext and admins regularly hijack accounts.

You're literally standing up for a Jabber service solely because it has a "cool h4x0r name."

Read my full rant about Exploit.IM here: <https://hackforums.net/showthread.php?tid=4910065>

sinmar - July 17, 2015, 9:39 am

(Jul 17, 2015 08:48 AM)Xerucide Wrote: [\[CITE\]](#) So it's alright to accept plaintext passwords pre-TLS?
You do realize Exploit.IM also stores passwords in plaintext and admins regularly hijack accounts.
You're literally standing up for a Jabber service solely because it has a "cool h4x0r name."

Read my full rant about Exploit.IM here: <https://hackforums.net/showthread.php?tid=4910065>

I'm not defending it, I'm saying trying to say that calling it bad because their SSL isn't set up good is retarded. As for the plaintext comment, most all XMPP servers store plaintext passwords or unsalted MD5 because the popular XMPPd's don't have security in mind.

ZuGgY - July 17, 2015, 10:03 am

I have a question, if I just leave my DNS as is by default, is that bad? I haven't touched it, honestly...

Thanks.

Synapse - July 17, 2015, 10:20 am

Bookmarked very nice and hq thread

???? - July 17, 2015, 10:23 am

Great guide, took a while to read all the way through, but valuable information gained.

?A?O - July 17, 2015, 5:41 pm

Just updated the thread. Took a few things out, added a few other options and variants. Just going to keep on working on it slowly. Also going to put in a few OSX applications soon too along with also adding something about Torify/Torsocks.

xomk - July 17, 2015, 6:41 pm

Very nice, high-quality guide! Thank you for posting!

Inkling - July 17, 2015, 6:42 pm

This is an amazing guide.

Do you think you could add more?

I really enjoyed reading this.

Betty Blue - July 17, 2015, 6:49 pm

Awesome. Maybe the 80% of idiots in this section will learn something, hope to see some of the good suggestions I and others gave you added in!

Loki123 - July 17, 2015, 6:51 pm

I'm going over a few things,

For the first... All of your Disk image creators are bad except the Win32DiskImager.

Rufus, LinuxLiveUSB and Unetbootin are terrible because they overwrite your syslinux.cfg with their own. That can break the boot process.

There is an Icelandic VPN that is safe to use, the laws in Iceland do not require VPN services to keep logs.

<https://lokun.is/>

This one does not keep logs as well as it isn't expensive..

GoogleDNS at least is probably one that you don't want to use. As Google keeps logs

<https://developers.google.com/speed/public-dns/privacy>

With Full disk encryption you should link this

https://wiki.archlinux.org/index.php/Disk_encryption

A lot of important information on there. As well as mention that you NEED to encrypt your swap. If say, you keep an application open in SWAP and shut down your computer by unplugging the cable,

then data in swap is kept and can be seen. Thus; All type of information leaked, which is a breach into your privacy.

Overwriting data once with bunch of zeros is more than enough to make it unrecoverable. This has been proven as well as if you want to, I can find the research paper done on that subject. 3 times isn't really overdoing it but using something like the Gutmann method would be stupid. Yet even then, it is possible in theory to recover the data so you ain't perfectly safe until you have physically destroyed the hard drive.

I find it really amusing that you should mention Google as "not safe" search engine but yet you list their DNS as usable. heh. ;-)

If I see something more. I'll just let you know on IRC. I think I've covered what I saw when reading this now at 2am.

Zink - July 17, 2015, 7:23 pm

I just read through this thread,
great work zer0.
Actually learned something.

?A?O - July 17, 2015, 10:53 pm

(Jul 17, 2015 06:51 PM)Loki123 Wrote: [\[CITE\]](#) -snip-
Talked to you on IRC, fixed a lot of that.

Edited a bunch of things, will continue looking into adding a few more things.

Evil Corp - July 18, 2015, 2:39 am

Saving this for later read. Thanks for taking time doing this.

HIGH PAID FELLA - July 18, 2015, 6:57 am

OP, as linked before ArchLinux has a great documentation regarding applications, protocols and anonymity.

?A?O - July 18, 2015, 7:15 am

(Jul 18, 2015 06:57 AM)Asterea Wrote: [\[CITE\]](#) OP, as linked before ArchLinux has a great documentation regarding applications, protocols and anonymity.

I added a link to their encryption information under my Whole Disk Encryption section. Might add more soon, going to look through there Wiki today at some point.

???? - July 18, 2015, 9:44 am

One thing I am confused about is your VPN > Tor vs Tor > VPN.

As I understand, and as the OPSEC for Hackers link at the bottom of your post states around the middle of the slideshow (a bit before), Tor > VPN is okay, VPN > Tor = GO TO JAIL.

Loki123 - July 18, 2015, 9:53 am

(Jul 18, 2015 09:44 AM)???? Wrote: [\[CITE\]](#) One thing I am confused about is your VPN > Tor vs Tor > VPN.

As I understand, and as the OPSEC for Hackers link at the bottom of your post states around the middle of the slideshow (a bit before), Tor > VPN is okay, VPN > Tor = GO TO JAIL.

Tor > VPN

With this method you send data through tor and then to your VPN and out.

This method protects you from your VPN provider. They don't know who you are because you connect after going through Tor.

VPN > Tor

This method sends first data to your VPN then towards tor and then out.

This method means that your VPN provider can see what you are doing, what sites are requested and log your activity before you connect to tor.

That is a basic explanation of how it it.

?A?O - July 18, 2015, 10:01 am

(Jul 18, 2015 09:44 AM)???? Wrote: [\[CITE\]](#) One thing I am confused about is your VPN > Tor vs Tor > VPN.

As I understand, and as the OPSEC for Hackers link at the bottom of your post states around the middle of the slideshow (a bit before), Tor > VPN is okay, VPN > Tor = GO TO JAIL.

VPN > Tor means you better damn well trust your VPN provider, which no one can really so the other method is always suggested.

???? - July 18, 2015, 10:02 am

There are also methods like Tortilla, Tor > VPN > Tor, etc etc. I remember the whonix documentation saying something like running two instances of tor together is a no-no. I'll try to find it.

Edit: here it is.

<https://tor.stackexchange.com/questions/427/is-running-tor-over-tor-dangerous>

PhantomElite - July 18, 2015, 10:17 am

There's a really good DEFCON OPSEC talk you might walk to link to.

<https://www.youtube.com/watch?v=J1q4lr2J8P8>

Illuminaughty sent me it and it was very informative so I thought I'd post it as it fits the general theme.

HIGH PAID FELLA - July 18, 2015, 10:18 am

(Jul 18, 2015 10:17 AM)PhantomElite Wrote: [\[CITE\]](#) There's a really good DEFCON OPSEC talk you might walk to link to.

<https://www.youtube.com/watch?v=J1q4lr2J8P8>

Illuminaughty sent me it and it was very informative so I thought I'd post it as it fits the general theme.

I saw this one too, it's pretty old but it's concepts still apply.

?A?O - July 18, 2015, 10:24 am

(Jul 18, 2015 10:17 AM)PhantomElite Wrote: [\[CITE\]](#) There's a really good DEFCON OPSEC talk you might walk to link to.

<https://www.youtube.com/watch?v=J1q4lr2J8P8>

Illuminaughty sent me it and it was very informative so I thought I'd post it as it fits the general

theme.

I'll watch this in a bit, not sure if I've seen this one.

If I think it will help others and apply to my thread, I'll add it in for sure.

Goodies - July 18, 2015, 10:52 am

Given the size of the thread, I've only found like 8 or 9 mistakes which is pretty impressive. As an oxford comma user, I'd add more commas to sentences, paragraphs, and statements. :) see wut i did ther?

Anyways, onto the content. Just a quick comment on each of the topics:

1. Secure Operating Systems

As far as security goes, Tails and Whonix are certainly among the top in terms of anonymity, but I'd be careful calling them "secure." I'm aware that this is not meant to be an operating system security thread, but people can be identified by insane things like screen resolution or cursor movements. Everyone using Tor needs to ensure that they disable all client-side code execution (javascript, flash, etc...) as that is the #1 way of identifying Tor users. It seems to me that tunneling an entire TCP/IP stack via a single SOCKS proxy would lead to issues. Hats off to the Tails community for developing such a great product.

2. Virtual Private Networks

As a very pleased Proxy.sh user, I can personally attest to their security, anonymity, and simplicity. To point out the obvious, that picture with the 1's and 0's followed by a picture with ampersands and pound signs is obviously ridiculous. We know what they're trying to get across, but data shows up as 1's and 0's anyways. The only difference would be that the original picture would resolve to human-readable ASCII (assuming that was the original goal) and the other would be nonsense to a human. At any rate, I'm just happy you cleared up the misconceptions about DNS leaking. It's not some occultish, magical hack. It's just using local DNS servers to resolve things like PurchaseCreditCardsOnlineForCheap.com coming from your IP. The best thing to do is to use remote DNS lookups (which Proxy.sh supports) as opposed to using, say, Google's DNS servers. Your ISP will still get metadata, and I wouldn't be surprised if they captured all DNS requests. So thank you for giving a great explanation of DNS leaking.

3. TOR Related

It looks to me like you've covered all the major topics (and more!). Quite simply, Tor is a multi-tiered encrypted communication network via numerous community-run overlays and a potentially malicious exit node ? Exit nodes really are a pain in the ass. NSA-run exit nodes that inject client-side scripts into unencrypted communication is a very real and unfortunately common activity. I know I mentioned client-side scripts in the Tails/Whonix part of my post, but it is very important and I think you clearly demonstrated the necessity for it. To give an example, the largest Tor-based child porn hosting service, Freedom Hosting, was taken down by a couple of lines of JavaScript.

4. Encryption

You're a bigger man than I if you want to tackle such an incredibly diverse, robust, and rigorous topic as encryption. Though I'm far from even pretending to understand the deeper mechanics of encryption, the mathematical Theory behind it is incredible. I would want to point out that even today's encryption is still subject to attack. Hopefully no one here actually needs to be told that with the POODLE's and the LOGJAM's and the HeartBleed's of the past few months. Obviously you want to stay encrypted, but since the majority of the population does not care enough to run encrypted email services, making the job of an attacker significantly easier, it gets annoying having to send passwords and the likes using <https://oneshar.es> and <https://privnote.com> and such. I would add in the software that KMS was talking about in the TeamSpeak that encrypts RAM. I am not familiar with cold-boot attacks (essentially blasting ice cold air into the RAM and preserving the state so that

you can move it into another computer and find the disk encryption keys) and their popularity in forensic environments, but it may be relevant to anonymity. I will say that Tails has protection against this attack. Kudos.

5. File/Download Security

I don't have much to say here. Several of the Next-Gen firewalls that I work with have the capability to perform malware analysis on files being downloaded; it's interesting to say the least. Metadata is always a problem, but there are many ways to change it (as you mentioned). Antiviruses, Rootkit protections, and host-based IDS's are imperative in a secure environment. If you have a ring-0 or kernel-land Rootkit, everything else is subject to the attacker's whim.

6. Social Related

I'm not much of a social media person, but don't post or message anything relevant to your passwords or security questions. It seems like it should be common sense, yet it remains elusive to the morons that, unfortunately, are allowed use the internet.

7. General Computer Security

Like encryption, this is too big a concept to discuss in such a limited space. I'd recommend putting in things like GRSec for MAC (mandatory access control) and RBAC (Role-based access control) as well as buffer overflow protection, and a myriad of other things. I also like OSSEC as an HIDS. It's cross-platform, centralized for simplicity and security, and is incredibly easy to deploy.

It's not much, but it's a quick Goodies' Goodies segment. Big thanks to Zer0 for creating such a unique and much-needed thread. I hope it gets the recognition it deserves.

PhantomElite - July 18, 2015, 10:58 am

(Jul 18, 2015 10:24 AM)zer0 ? Wrote: [\[CITE\]](#) I'll watch this in a bit, not sure if I've seen this one. If I think it will help others and applies to my thread, I'll add it in for sure.

It's the "7 Deadly Fuckups" one. The guy with spiky hair blonde mohawk thing, just in case that triggers something for you to remember it.

?A?O - July 18, 2015, 11:00 am

(Jul 18, 2015 10:52 AM)Goodies Wrote: [\[CITE\]](#) -snip-

I figured you'd write a book as a post. Anyways, about the Secure OS section, it would of sounded weird naming it "More Secure than a Normal OS". I hope people understand nothing is 100% secure so it was kind of a given.

About the encryption section, I was going to add in what KMS was referring too but completely forgot the application name and I can't ask him anymore due to obvious reasons.

General security section. I'd like to add a Mac related sub-section and am starting to put together more things in general for this section.

PhantomElite - July 18, 2015, 11:01 am

(Jul 18, 2015 10:52 AM)Goodies Wrote: [\[CITE\]](#) but people can be identified by insane things like screen resolution or cursor movements.

With the issue of screen resolution, that's why you keep the TOR browser at its default size as they tell you.

???? - July 18, 2015, 11:37 am

(Jul 18, 2015 11:01 AM)PhantomElite Wrote: [\[CITE\]](#) With the issue of screen resolution, that's why you keep the TOR browser at its default size as they tell you.

I remember reading that additional addons can also do the same for a browser signature (not sure if

I'm using the proper term), though I know there is yet another addon that can scramble that.

Also, about Tor > VPN again, this would prevent you from visiting onion websites. I assume Tor> VPN > Tor is necessary to access onion sites if you wanted to use a VPN? I haven't tried most of these but have only read about a lot of them. Does anyone have opinions about VPN > Tor > VPN > Tor as well? I can only find people mentioning it.

Also, as an interesting note, I read that setting tor to use a proxy that you've set to localhost running i2p can also work :)

HIGH PAID FELLA - July 18, 2015, 11:42 am

(Jul 18, 2015 11:37 AM)???? Wrote: [\[CITE\]](#) I remember reading that additional addons can also do the same for a browser signature (not sure if I'm using the proper term), though I know there is yet another addon that can scramble that.

Also, about Tor > VPN again, this would prevent you from visiting onion websites. I assume Tor> VPN > Tor is necessary to access onion sites if you wanted to use a VPN? I haven't tried most of these but have only read about a lot of them. Does anyone have opinions about VPN > Tor > VPN > Tor as well? I can only find people mentioning it.

Also, as an interesting note, I read that setting tor to use a proxy that you've set to localhost running i2p can also work :)

Your last note answered your own question, you can setup or use a tor proxy to visit those .onion's, such as <http://onion.to> provides these proxies but are not recommended since you don't use multiple Tor relay's if I'm not wrong.

???? - July 18, 2015, 11:45 am

Would configuring Tor to use proxy X not be X > Tor > VPN > onion.to? If so you would still only be able to access onion sites via onion.to, unless I misunderstood your post.

???? - July 18, 2015, 11:53 am

(Jul 18, 2015 11:48 AM)Asterea Wrote: [\[CITE\]](#) No, because the proxy you setup should be before the .onion

You > Tor > VPN > proxy > .onion

If you ment to use onion.to's proxy,

You > proxy > Tor > VPN > .onion.to > .onion

but the proxy can be put everywhere (inbetween these).

I thought you were mentioning the part where I said to edit Tor's proxy settings to run it through something.

I have not tested it, but would the first setup in your post not connect to .onion websites? Because to access onion sites, while you are still connected to tor, you are using a VPN before the onion site, and you will still not be able to connect. If I remember what I've read elsewhere correctly.

Here are some resources:

<https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/connecting-tor-vpn-for-window-s-users/>

Quote: Sometimes doing TOR -> VPN is necessary because of the spam filter reasons I mentioned above and other times having TOR as your last node to the internet is necessary like when

accessing the onion network.

That is found near the bottom of the page (the source of my confusion)

<https://trac.torproject.org/projects/tor/wiki/doc/TorPlusVPN#you-X-Tor>

They do not seem to like Tor > VPN much, despite what the previous page in this topic suggests :p

.vemla - July 18, 2015, 12:03 pm

Well done, OP.

Thank you for sharing all this and putting your time into making this, much appreciated.

HIGH PAID FELLA - July 18, 2015, 12:10 pm

(Jul 18, 2015 11:53 AM)???? Wrote: [\[CITE\]](#) I thought you were mentioning the part where I said to edit Tor's proxy settings to run it through something.

I have not tested it, but would the first setup in your post not connect to .onion websites? Because to access onion sites, while you are still connected to tor, you are using a VPN before the onion site, and you will still not be able to connect. If I remember what I've read elsewhere correctly.

Here are some resources:

<https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/connecting-tor-vpn-for-windows-users/>

That is found near the bottom of the page (the source of my confusion)

<https://trac.torproject.org/projects/tor/wiki/doc/TorPlusVPN#you-X-Tor>

They do not seem to like Tor > VPN much, despite what the previous page in this topic suggests :p
I would just stick to Tor and multiple relay's and a safe exit-node to visit .onion's and would dodge proxies to use Tor since they are not vey safe and stick to addon's that block Javascript, Flash etc. and use DuckDuckGo as search engine since Google is very annoying on Tor and not safe.

Goodies - July 18, 2015, 12:17 pm

(Jul 18, 2015 11:01 AM)PhantomElite Wrote: [\[CITE\]](#) With the issue of screen resolution, that's why you keep the TOR browser at its default size as they tell you.

I... actually did not know that about Tor. Good for them. Thanks for that factoid.

@Zer0

I honestly can't remember the name of the application, either.

???? - July 18, 2015, 12:24 pm

(Jul 18, 2015 12:10 PM)Asterea Wrote: [\[CITE\]](#) I would just stick to Tor and multiple relay's and a safe exit-node to visit .onion's and would dodge proxies to use Tor since they are not vey safe and stick to addon's that block Javascript, Flash etc. and use DuckDuckGo as search engine since Google is very annoying on Tor and not safe.

I like thinking about the most secure/private/anonymous setups possible :)

HIGH PAID FELLA - July 18, 2015, 12:36 pm

(Jul 18, 2015 12:24 PM)???? Wrote: [\[CITE\]](#) I like thinking about the most secure/private/anonymous setups possible :)

Most safe one would include Whonix/Tails, hacked wi-fi, tweaked browser, Tor, tunneling software,

proxies/VPN and your OPSec.

???? - July 18, 2015, 12:43 pm

What of having an old computer running linux firewall and another running whonix that you use as a gateway for tails and run unsafe browser in tails (with proper addons installed), along with what you've mentioned? At a point this kind of stuff gets tricky.

Goodies - July 18, 2015, 1:30 pm

(Jul 18, 2015 12:24 PM)???? Wrote: [\[CITE\]](#) I like thinking about the most secure/private/anonymous setups possible :)

Using acoustic couplers and a modem on a pay phone tunneled through Tor on a VPN with a virtual machine is the most secure setup you can reasonably have.

Hash G. - July 18, 2015, 1:32 pm

Bookmarking this, thank you for your HQ work !

Sam Winchester - July 18, 2015, 2:00 pm

One of the most detailed guides on Hackforums. Nice work.

?A?O - July 18, 2015, 2:07 pm

(Jul 18, 2015 02:00 PM)Sam Winchester Wrote: [\[CITE\]](#) One of the most detailed guides on Hackforums. Nice work.

Appreciate it. Lots of user input and things I still want to add and take out/change. Still working on this thread and will continue to update it.

Vector.A+ - July 18, 2015, 2:19 pm

Thank you it is an extremely helpful and descriptive guide

???? - July 18, 2015, 2:36 pm

This thread may be of interest:

<https://www.whonix.org/forum/index.php/topic,1383.0.html>

?A?O - July 18, 2015, 2:37 pm

(Jul 18, 2015 02:36 PM)???? Wrote: [\[CITE\]](#) This thread may be of interest:

<https://www.whonix.org/forum/index.php/topic,1383.0.html>

There's a few things I'll be looking at tomorrow, I'll add this to that list. Seems like it would be an interesting read. I'm up for any user input when it comes to this thread.

HIGH PAID FELLA - July 18, 2015, 3:08 pm

Also the usage of Tunnelier via a hacked RDP or VPS to tunnel your traffic through them can be very handy.

Aurora - July 18, 2015, 3:15 pm

This definitely deserves a sticky. Hopefully you'll always update this when needed zer0.

?A?O - July 18, 2015, 3:20 pm

(Jul 18, 2015 03:15 PM).Sinister Wrote: [\[CITE\]](#) This definitely deserves a sticky. Hopefully you'll always update this when needed zer0.

Yeah I am going to. As new security measures come into play and some die out, plan on adding and removing fairly frequently.

Goodies - July 18, 2015, 3:20 pm

(Jul 18, 2015 03:08 PM)Asterea Wrote: [\[CITE\]](#) Also the usage of Tunnelier via a hacked RDP or VPS to tunnel your traffic through them can be very handy.

Just to put some insight here, it's very easy for a Windows server admin to detect who is using the data. Even if you use an SSH tunnel, when it comes out the other side, the Windows server has full control. You're opening yourself up to a MITM attack without even knowing it.

Using your own VPS is much better, but a VPN is even better simply due to the nature of tunnels vs VPN connections. Tunnels just move data, but VPNs actually create a remote TCP/IP stack for you to use. Tunnels are similar, but not identical.

VPN through the tunnel (if possible) and that would be perfectly fine. It would look as if the VPN connection was initiated from the remote side of the tunnel.

HIGH PAID FELLA - July 18, 2015, 3:42 pm

(Jul 18, 2015 03:20 PM)Goodies Wrote: [\[CITE\]](#) Just to put some insight here, it's very easy for a Windows server admin to detect who is using the data. Even if you use an SSH tunnel, when it comes out the other side, the Windows server has full control. You're opening yourself up to a MITM attack without even knowing it.

Using your own VPS is much better, but a VPN is even better simply due to the nature of tunnels vs VPN connections. Tunnels just move data, but VPNs actually create a remote TCP/IP stack for you to use. Tunnels are similar, but not identical.

VPN through the tunnel (if possible) and that would be perfectly fine. It would look as if the VPN connection was initiated from the remote side of the tunnel.

I didn't ment to say to use a hacked VPS, but a bought one like an offshore one. Hacked RDP is an option but not very safe as you mentioned.

Also @OP, are you going to give credits in the thread to the people who helped with adding content? Would be very appreciated.

???? - July 18, 2015, 3:54 pm

(Jul 18, 2015 03:20 PM)Goodies Wrote: [\[CITE\]](#) Just to put some insight here, it's very easy for a Windows server admin to detect who is using the data. Even if you use an SSH tunnel, when it comes out the other side, the Windows server has full control. You're opening yourself up to a MITM attack without even knowing it.

Using your own VPS is much better, but a VPN is even better simply due to the nature of tunnels vs VPN connections. Tunnels just move data, but VPNs actually create a remote TCP/IP stack for you to use. Tunnels are similar, but not identical.

VPN through the tunnel (if possible) and that would be perfectly fine. It would look as if the VPN connection was initiated from the remote side of the tunnel.

In the thread I posted earlier from the whonix forums, this paper was posted:

<https://www.usenix.org/system/files/conference/foci12/foci12-final8.pdf>

I haven't read it, but it shows that VPN's are unsafe to use, and user HulaHoop has some strong opinions about them.

Josch - July 18, 2015, 4:07 pm

Damn, why haven't I seen this thread before? Great work on this zer0! Guessing this means that

you're staying even though Null and some of it's members are leaving?

#Skyline - July 18, 2015, 4:19 pm

Holy sheit, this has a massive amount of content.
Very informational tutorial Zero.

?A?O - July 18, 2015, 4:20 pm

(Jul 18, 2015 03:42 PM)Asterea Wrote: [\[CITE\]](#) I didn't ment to say to use a hacked VPS, but a bought one like an offshore one. Hacked RDP is an option but not very safe as you mentioned.

Also @OP, are you going to give credits in the thread to the people who helped with adding content? Would be very appreciated.

Possibly, the main issue is I have to see how big the contribution is to the guide. If I make a section out of your suggestion, yes. If it's just a guide I add to the end, probably not. I plan on keeping this thread updated for a long time, you know how many users might give there input? But I think that's a pretty fair way of doing it. I might just add a spoiler at the end with users who added some sort of input. I just have to decide how I want it done.

HIGH PAID FELLA - July 18, 2015, 4:23 pm

(Jul 18, 2015 04:20 PM)zer0 ? Wrote: [\[CITE\]](#) Possibly, the main issue is I have to see how big the contribution is to the guide. If I make a section out of your suggestion, yes. If it's just a guide I add to the end, probably not. I plan on keeping this thread updated for a long time, you know how many users might give there input? But I think that's a pretty fair way of doing it. I might just add a spoiler at the end with users who added some sort of input. I just have to decide how I want it done.
Alright, great to hear you will give credits or mentions.

?A?O - July 18, 2015, 6:32 pm

(Jul 18, 2015 04:07 PM)JoScH Wrote: [\[CITE\]](#) Damn, why haven't I seen this thread before? Great work on this zer0! Guessing this means that you're staying even though Null and some of it's members are leaving?

I won't be on nearly as much once Null is gone. I'll be doing a lot of offsite computer things with members and friends but this thread is something I will continue to update regardless.

crazyycast13 - July 18, 2015, 6:53 pm

oo my thread got a shoutout at the bottom.

But in regards to encryption, do not decrypt volumes/drives/whatever in public. There are now little devices that can passively steal your encryption keys. In fact, when you do decide to sit down at some library, make sure that the table isn't bugged. There are a lot of ways nowadays that people can figure out what you are typing through tiny vibrations and stuff like that, so try to avoid using bluetooth keyboards. That's just a bad idea.

Now if only you went a little bit into more afk opsec...

?A?O - July 18, 2015, 7:02 pm

(Jul 18, 2015 06:53 PM)crazyycast13 Wrote: [\[CITE\]](#) oo my thread got a shoutout at the bottom.

But in regards to encryption, do not decrypt volumes/drives/whatever in public. There are now little devices that can passively steal your encryption keys. In fact, when you do decide to sit down at some library, make sure that the table isn't bugged. There are a lot of ways nowadays that people can figure out what you are typing through tiny vibrations and stuff like that, so try to avoid using bluetooth keyboards. That's just a bad idea.

Now if only you went a little bit into more afk opsec...

Oh I was going to PM you that I added your thread to this but forgot. Also, speaking of bluetooth keyboards, a while back I made my own KeySweeper ;)

crazyycast13 - July 18, 2015, 7:15 pm

(Jul 18, 2015 07:02 PM)zer0 ? Wrote: [\[CITE\]](#) Oh I was going to PM you that I added your thread to this but forgot. Also, speaking of bluetooth keyboards, a while back I made my own KeySweeper ;)

You should definitely mention that wireless keyboards are a no no, and also that it is possible to steal encryption keys with a device like this ->

<http://www.engadget.com/2015/06/23/pita-radio-wave-hack/>

Schatten - July 18, 2015, 8:15 pm

Let's all talk about Schatten's thread now. ?

<https://hackforums.net/showthread.php?tid=4912439>

No? Okay. ?

?A?O - July 18, 2015, 9:33 pm

(Jul 18, 2015 07:15 PM)crazyycast13 Wrote: [\[CITE\]](#) You should definitely mention that wireless keyboards are a no no, and also that it is possible to steal encryption keys with a device like this ->

<http://www.engadget.com/2015/06/23/pita-radio-wave-hack/>

Yeah I was possibly thinking of a hardware section but was still coming up with ideas on what exactly I'd have in it if I added that in.

Aurora - July 18, 2015, 9:58 pm

(Jul 18, 2015 09:33 PM)zer0 ? Wrote: [\[CITE\]](#) Yeah I was possibly thinking of a hardware section but was still coming up with ideas on what exactly I'd have in it if I added that in.

A hardware section would be nice. It would be quite useful for someone who's completely new like me.

???? - July 18, 2015, 10:06 pm

(Jul 18, 2015 09:58 PM).Sinister Wrote: [\[CITE\]](#) A hardware section would be nice. It would be quite useful for someone who's completely new like me.

You could run Pfsense on something like a RaspberryPi for a firewall maybe?

Edit: can't do that do to architecture. Some old computer or something would do.

Ghanem - July 19, 2015, 1:40 am

Feels good to see a thread like this.

I'll PM you something I wrote (but never finished) today.

Just in case you can extract some stuff from it and post it. ?

HIGH PAID FELLA - July 19, 2015, 4:42 am

A hardware section would be very nice to mention, such as tips, tricks and things to do and not-to-do. Such as burner phones, how to use them, how to get SIM's for them and such to start with.

sinmar - July 19, 2015, 5:40 am

(Jul 19, 2015 04:42 AM)Asterea Wrote: [\[CITE\]](#) A hardware section would be very nice to mention, such as tips, tricks and things to do and not-to-do. Such as burner phones, how to use them, how to get SIM's for them and such to start with.

Cell phones are pretty garbage security wise, if you need to call or text there are many online

services to do so.

HazrdN - July 19, 2015, 7:24 am

(Jul 18, 2015 12:10 PM)Asterea Wrote: [\[CITE\]](#) I would just stick to Tor and multiple relay's and a safe exit-node to visit .onion's and would dodge proxies to use Tor since they are not vey safe and stick to addon's that block Javascript, Flash etc. and use DuckDuckGo as search engine since Google is very annonying on Tor and not safe.

DDG? haha no, use startpage.

HIGH PAID FELLA - July 19, 2015, 7:26 am

(Jul 19, 2015 07:24 AM)HazrdN Wrote: [\[CITE\]](#) DDG? haha no, use startpage.

Startpage is good too considering it's set as the main s.e but why not DDG?

HazrdN - July 19, 2015, 7:28 am

(Jul 19, 2015 07:26 AM)Asterea Wrote: [\[CITE\]](#) Startpage is good too considering it's set as the main s.e but why not DDG?

DDG is bad, in the paste they used amazon servers and their was a pic how there TOS contradicted itself and the owner owned a data mining company before.

Also veracrypt is on a Microsoft owned website and there is no audit like TC.

HIGH PAID FELLA - July 19, 2015, 7:29 am

(Jul 19, 2015 07:28 AM)HazrdN Wrote: [\[CITE\]](#) DDG is bad, in the paste they used amazon servers and their was a pic how there TOS contradicted itself and the owner owned a data mining company before.

Also veracrypt is on a Microsoft owned website and there is no audit like TC.

Alright, good to know. Will change back to Startpage then.

HazrdN - July 19, 2015, 7:33 am

Cryptostorm is a good reputable VPN.

sinmar - July 19, 2015, 7:51 am

(Jul 19, 2015 07:24 AM)HazrdN Wrote: [\[CITE\]](#) DDG? haha no, use startpage.

imo I prefer ixquick over startpage, they're owned by the same company.

Billie Joe Armstrong - July 19, 2015, 8:17 am

Cant bookmarked but will read them later.

HazrdN - July 19, 2015, 8:35 am

(Jul 19, 2015 07:51 AM)sinmar Wrote: [\[CITE\]](#) imo I prefer ixquick over startpage, they're owned by the same company.

Yeah it doesn't really matter which one you use but don't use ddg.

?A?O - July 19, 2015, 8:56 am

Finishing up some C/ASM work then I'm going to be going through all comments individually and make a list of what people think should be added in and removed. Will take a little bit of time to go through everyone's opinions.

Joaquín Guzmán Loera - July 19, 2015, 11:04 am

Great guide. These are one of the rare guide on this sub-forum that aren't completely fucking stupid.

Thatmobguy - July 19, 2015, 4:15 pm

Hell of a nice guide. Very Detailed and a good read.

?A?O - July 20, 2015, 7:20 am

If anyone has a lot of experience with OSX or has suggestions on the same level as this thread for OSX security to add at the end, feel free to PM me.

Xmlrpc - July 20, 2015, 7:50 am

Very nice, high-quality guide! Thank you for posting!

?A?O - July 21, 2015, 5:04 am

(Jul 20, 2015 07:50 AM)Xmlrpc Wrote: [\[CITE\]](#) Very nice, high-quality guide! Thank you for posting! Thanks, please if anyone has any feedback please PM or post, still looking for more suggestions before I update this week.

Cf Bypass - July 21, 2015, 7:39 am

Great guide, took a while to read all the way through, but valuable information gained.

?A?O - July 22, 2015, 5:32 am

(Jul 21, 2015 07:39 AM)Cf Bypass Wrote: [\[CITE\]](#) Great guide, took a while to read all the way through, but valuable information gained. Thanks, always nice to get good feedback.

indicud - July 22, 2015, 5:36 am

Bump so I can get out of bed later and read this haha

vpaka26 - July 22, 2015, 8:56 am

Really good tutorial :) this will help me a lot. Thanks!

James Burnham - July 23, 2015, 1:40 am

I tried IPLeak.net while under PROXY.SH and it showed my real IP along the VPN IP. What can I do about this?

Schatten - July 23, 2015, 1:43 am

(Jul 23, 2015 01:40 AM)Darth Burnham Wrote: [\[CITE\]](#) I tried IPLeak.net while under PROXY.SH and it showed my real IP along the VPN IP. What can I do about this?

Do you have WebRTC disabled in your browser? If you're in Firefox, make sure media.peerconnection.enabled is disabled.

James Burnham - July 23, 2015, 1:55 am

(Jul 23, 2015 01:43 AM)Schatten Wrote: [\[CITE\]](#) Do you have WebRTC disabled in your browser? If you're in Firefox, make sure media.peerconnection.enabled is disabled.

That worked. Thank you very much.

Regarding Deleting Files/Information Correctly.

I have some files that I deleted the regular way.

Now I would like to shred anything that may be left behind.

How will I do this?

?A?O - July 23, 2015, 6:59 pm

(Jul 23, 2015 01:55 AM)Darth Burnham Wrote: [\[CITE\]](#) That worked. Thank you very much.

Regarding Deleting Files/Information Correctly.

I have some files that I deleted the regular way.

Now I would like to shred anything that may be left behind.

How will I do this?

I'm getting off right now for the night but tomorrow I'll help you out with this. Mainly, just PM me whether you're on a Linux or Windows.

Enzio - July 23, 2015, 11:15 pm

Nice tutorial. Bookmarked.

Otis??????????????? - July 24, 2015, 1:33 am

Posting to keep this up so I can read later on when I'm fully awake.

Schatten - July 24, 2015, 6:27 am

(Jul 24, 2015 01:33 AM).Sytech Wrote: [\[CITE\]](#) Posting to keep this up so I can read later on when I'm fully awake.

Alright bud - thanks for updating us on your current status of whether you're fully awake or not.

Uriel - July 24, 2015, 3:57 pm

What is the best way to go about securely removing the contents of an SSD seeing as DBAN does not support the wiping of an SSD? I know that the service they feature on their page supports SSD's but it is not free. I was wondering if there are currently any good free solutions.

Thank you.

RaidenHF - July 24, 2015, 6:51 pm

Thank you! This was very helpful.

?A?O - July 26, 2015, 6:30 am

(Jul 24, 2015 06:51 PM)dillon4419 Wrote: [\[CITE\]](#) Thank you! This was very helpful.

Glad to hear it helps people out.

Arise - July 26, 2015, 7:49 am

Bookmarked this for future reference, this is a great tutorial, I love how indepth it goes! Its very helpful thanks.

Red It - July 26, 2015, 11:35 am

(Jul 24, 2015 03:57 PM)Madness Wrote: [\[CITE\]](#) What is the best way to go about securely removing the contents of an SSD seeing as DBAN does not support the wiping of an SSD? I know that the service they feature on their page supports SSD's but it is not free. I was wondering if there are currently any good free solutions.

Thank you.

As far as I know you got about 3 options to erase a SSD drive.

1. Try using the manufacturer's SSD management software to wipe the drive. I know Samsung Magician and Intel SSD toolbox have a secure erase feature.

2. Encrypt the drive and then forget the password. No password no data.

3. Use HDparm Secure erase, Its a linux only program and in order to work correctly the SSD drive most NOT be connected via usb. You can find more information about it [here](#)

mr_boss - July 26, 2015, 2:06 pm

Very helpful information :D

Good for beginners and more advanced people too.

Thank you ?

Lysergide - July 27, 2015, 5:38 am

I think this is one of the best guides about something I have ever read.

And it gives exactly the information I was looking for, especially the social related section, which you do not find easily around.

Again, a big thank you.

SteCache - July 27, 2015, 3:18 pm

Awesome tutorial, thank's mate :)

?A?O - July 27, 2015, 10:37 pm

(Jul 27, 2015 05:38 AM)Lysergide Wrote: [\[CITE\]](#) I think this is one of the best guides about something I have ever read.

And it gives exactly the information I was looking for, especially the social related section, which you do not find easily around.

Again, a big thank you.

Keep checking it from time to time. Going to be editing it as things change.

???? - July 28, 2015, 9:02 am

(Jul 27, 2015 10:37 PM)zer0 ? Wrote: [\[CITE\]](#) Keep checking it from time to time. Going to be editing it as things change.

Any change logs with the updates? :)

Aurora - July 28, 2015, 9:03 am

(Jul 28, 2015 09:02 AM)???? Wrote: [\[CITE\]](#) Any change logs with the updates? :)

An update log would be nice actually.

?A?O - July 28, 2015, 2:38 pm

(Jul 28, 2015 09:02 AM)???? Wrote: [\[CITE\]](#) Any change logs with the updates? :)

Hmm I didn't think about this but I'll probably add one in sometime as a spoiler at the end of the thread.

???? - July 29, 2015, 8:52 am

Is there any guide that lists and covers most attack vectors?

777ethods - July 29, 2015, 10:04 am

Really high quality post. Definitely bookmarking this, thanks!

?A?O - July 29, 2015, 12:49 pm

(Jul 29, 2015 08:52 AM)???? Wrote: [\[CITE\]](#) Is there any guide that lists and covers most attack vectors?

Link:

https://www.owasp.org/images/6/6c/Encoded_Attacks_Threats_Countermeasures_9_30_08.pdf

Is something like that what you are looking for? Need a bit more specifics on your question but this has some useful information.

lenaos - July 29, 2015, 6:20 pm

This is a great thread, bookmarked.

???? - July 29, 2015, 7:01 pm

(Jul 29, 2015 12:49 PM)zer0 ? Wrote: [\[CITE\]](#) Link:

https://www.owasp.org/images/6/6c/Encoded_Attacks_Threats_Countermeasures_9_30_08.pdf

Is something like that what you are looking for? Need a bit more specifics on your question but this has some useful information.

Basically, every single attack vector vs. you when you log online and don't want your IP to be compromised, like the webrtc fix is one attack vector, tor is another, exit nodes, etc etc. Just going through every possible attack vector to be completely secure/anonymous/private.

HIGH PAID FELLA - July 30, 2015, 9:05 am

(Jul 29, 2015 07:01 PM)???? Wrote: [\[CITE\]](#) Basically, every single attack vector vs. you when you log online and don't want your IP to be compromised, like the webrtc fix is one attack vector, tor is another, exit nodes, etc etc. Just going through every possible attack vector to be completely secure/anonymous/private.

You should watch out for the third party applications you use with Tor such as Javascript, Flash, and such. Recently they showed how they can disable all your addons by just visiting a HTML page.

ras4sc - July 30, 2015, 9:14 am

(Jul 30, 2015 09:05 AM)Asterea Wrote: [\[CITE\]](#) You should watch out for the third party applications you use with Tor such as Javascript, Flash, and such. Recently they showed how they can disable all your addons by just visiting a HTML page. That was with Chrome, and it's already fixed.

HIGH PAID FELLA - July 30, 2015, 9:27 am

(Jul 30, 2015 09:14 AM)ras4sc Wrote: [\[CITE\]](#) That was with Chrome, and it's already fixed. Oh, only with Chrome. I thought it was also with Firefox. My bad x)

?A?O - August 3, 2015, 2:39 pm

It's good hearing the feedback for this thread.
Feel free to tell me things you want added in.

Aurora - August 3, 2015, 5:52 pm

(Aug 3, 2015 02:39 PM)zer0 ? Wrote: [\[CITE\]](#) It's good hearing the feedback for this thread.
Feel free to tell me things you want added in.
Will you be making this thread into a PDF anytime soon?

Leeway - August 3, 2015, 5:53 pm

This is a really nice guide thank you for this.

unchat - August 4, 2015, 4:17 pm

Very nice, high-quality guide! Thank you for posting!

?A?O - August 5, 2015, 11:03 am

(Aug 3, 2015 05:52 PM).Sinister Wrote: [\[CITE\]](#) Will you be making this thread into a PDF anytime soon?

I'm going on a six day trip starting tomorrow. When I get back I'll try to make it a priority.

CCHrambo - August 5, 2015, 11:05 am

Pretty good start of an awesome opsec guide :) If you need any help for more advanced additions PM me!

FDE (hardware and software) 2 layers
Anti-evil made methods

Anti- cold boot methods
Blue Proximity (nice application) Google it

Not going to go into more detail but there are a few additions you could add having to do with proxification, host OS hardening, etc.

sinmar - August 5, 2015, 11:26 am

(Aug 5, 2015 11:05 AM)CCHrambo Wrote: [\[CITE\]](#) Pretty good start of an awesome opsec guide :) If you need any help for more advanced additions PM me!

FDE (hardware and software) 2 layers
Anti-evil made methods
Anti- cold boot methods
Blue Proximity (nice application) Google it

Not going to go into more detail but there are a few additions you could add having to do with proxification, host OS hardening, etc.

so basically the basics of antifoensics so that when ur computer gets taken by the mean men in blue their forensics team can't get ur stuff

Aurora - August 5, 2015, 6:56 pm

(Aug 5, 2015 11:03 AM)zer0 ? Wrote: [\[CITE\]](#) I'm going on a six day trip starting tomorrow. When I get back I'll try to make it a priority.

That's good to hear. Looking forward to seeing that PDF.

renoik - August 5, 2015, 11:31 pm

Good guide, really useful.

Thanks you!

?A?O - August 6, 2015, 12:41 am

Going on my six day trip where I won't be online the whole time. When I get back I'm going to be updating parts of the thread and going to be creating a PDF as well for people to download.

Aeurraa - August 8, 2015, 10:48 am

Great guide, extremely detailed! Helped me to improve my physical security a lot!

?A?O - August 10, 2015, 11:53 am

Just getting back from my trip so tomorrow or next day I'll make a PDF and get back to updating this

Aurora - August 10, 2015, 5:57 pm

(Aug 10, 2015 11:53 AM)zer0 ? Wrote: [\[CITE\]](#) Just getting back from my trip so tomorrow or next day I'll make a PDF and get back to updating this

Again, I'm looking forward to that PDF. Thanks for all your hard work!

?A?O - August 14, 2015, 11:54 am

Okay starting work on the PDF today, also updating a few things within the thread.

hexcypher - August 14, 2015, 2:06 pm

This information is absolutely appreciated. What a wealth of guide.

Y?ung Thug - August 15, 2015, 7:34 pm

Effor is commendable, nice share m8 :)

Aurora - August 16, 2015, 8:09 am

(Aug 14, 2015 11:54 AM)zer0 ? Wrote: [\[CITE\]](#) Okay starting work on the PDF today, also updating a few things within the thread.

That's good to hear. ?

Do you have an estimated time frame for when it will be completed?

?A?O - August 16, 2015, 1:37 pm

(Aug 16, 2015 08:09 AM).Sinister Wrote: [\[CITE\]](#) That's good to hear. ?

Do you have an estimated time frame for when it will be completed?

Not really, school coming up and everything else I have going on. All I can say right now is it will get done soonish.

Strayta - August 16, 2015, 1:44 pm

Awesome guide man! Very well done

HIGH PAID FELLA - August 16, 2015, 4:45 pm

I have a new "Jabber server"-suggestion, find more information about it [here](#).

D4T4B4S3 - August 16, 2015, 4:54 pm

Congratz man. Great post with full details. This is what putting an effort to a thread should look like.

FFY00 - August 17, 2015, 3:26 am

Very HQ post. Congratulations

-zERaIT - August 17, 2015, 3:45 am

I admire your hard work on this, zer0. Good job.

Incendiary. - August 17, 2015, 6:39 am

Holy fuck thats HQ.

You just earned my respect good sir, i will be referring to this thread alot in the near future.

sinmar - August 17, 2015, 11:49 am

if you have captio.ch under the XMPP servers list you should put thedark.army - new server ran by the same sysadmins: <https://hackforums.net/showthread.php?tid=4950712>

?A?O - August 18, 2015, 2:01 am

(Aug 17, 2015 11:49 AM)sinmar Wrote: [\[CITE\]](#) if you have captio.ch under the XMPP servers list you should put thedark.army - new server ran by the same sysadmins:

<https://hackforums.net/showthread.php?tid=4950712>

He already told me over XMPP. I have added it in. I'll keep them up so long as they stay at an A rating.

TeddyMedina - August 18, 2015, 5:52 am

Thanks Bro, must be pinned.

Bayani - August 18, 2015, 11:13 am

I definitely bookmarked this. Learning a lot!

Thanks.

farux - August 18, 2015, 11:58 pm

Wow so good. Thanks a ton, Bookmarking

Raymond Reddington - August 19, 2015, 12:23 am

Wow, what a great detailed thread it is. Read it fully sad I have already given out enough of my personal data online. I will have to begin off somewhere now.

?A?O - August 19, 2015, 1:20 pm

(Aug 19, 2015 12:23 AM)Raymond Reddington Wrote: [\[CITE\]](#) Wow, what a great detailed thread it is. Read it fully sad I have already given out enough of my personal data online. I will have to begin off somewhere now.

Not the end of the world if your information is out there already. These are just steps/precautions to take when traversing the web regardless.

Marquall - August 19, 2015, 1:21 pm

Great post, implementing some of your advice now

?A?O - August 20, 2015, 1:07 pm

(Aug 19, 2015 01:21 PM)Marquall Wrote: [\[CITE\]](#) Great post, implementing some of your advice now Always good to hear ?

kush3d - August 20, 2015, 4:46 pm

Thank you very much for taking the time to put this together zer0 It is very thorough and detailed.

?A?O - August 21, 2015, 7:37 pm

(Aug 20, 2015 04:46 PM)kush3d Wrote: [\[CITE\]](#) Thank you very much for taking the time to put this together zer0 It is very thorough and detailed.

Within the next few days I'll be updating it a bit. School start Monday so I'll see when I can do it.

Zigggy - August 21, 2015, 7:40 pm

BUMP cause this is important

Aurora - August 21, 2015, 7:58 pm

I like the updates, Zero. Keep it up.

markeloff - August 22, 2015, 1:23 am

Great guide, man.

Good job.

TeddyMedina - August 22, 2015, 1:40 am

Hi zer0,

Are you going to make a pdf ?

faiz4uster - August 22, 2015, 3:13 am

Great Post very Informative for someone like me implemented your methods now thank you very much

Kraith - August 22, 2015, 5:18 am

Amazing and detailed work you've done on this guide. Good job.

?A?O - August 22, 2015, 2:19 pm

(Aug 22, 2015 01:40 AM)TeddyMedina Wrote: [\[CITE\]](#) Hi zer0, Are you going to make a pdf ?

Yeah, I promise I'll be turning it into one, just school starts Monday and I'm moving back to my apartment so there is just a lot going on right now, but it will be done when I'm settled down.

TeddyMedina - August 22, 2015, 4:11 pm

Thanks friend, your post is great and sorry if I disturb you.

I put it in a word document to print it, but as you are planning to make a pdf, I'll wait.

Thanks again.

?A?O - August 24, 2015, 5:30 pm

(Aug 22, 2015 04:11 PM)TeddyMedina Wrote: [\[CITE\]](#) Thanks friend, your post is great and sorry if I disturb you.

I put it in a word document to print it, but as you are planning to make a pdf, I'll wait.

Thanks again.

I'll do it this upcoming weekend. I have a three day weekend so it's perfect

.GonZ0. - August 25, 2015, 2:56 pm

This is Huge! Thank you very much for posting this. This will give a help to many people here, including me. I will bookmark this for sure. Thanks again!

bushmine - August 25, 2015, 9:01 pm

I commend you! Thanks zer0!

Machiavellian101 - August 27, 2015, 3:22 pm

I have just skim read this and plan to read it prop later. I also have to say that this does look like a decent thread in this section; a thread that is hard to come by these days. Congratz.

?A?O - August 28, 2015, 7:39 pm

Worked on the PDF a bit today, hopefully done by Sunday night.

Washington George - August 29, 2015, 7:49 am

Thank you for this! Great tutorial! <3

sademo - August 30, 2015, 4:06 pm

this is a great tutorial, thank you!

Aurora - August 30, 2015, 5:01 pm

(Aug 28, 2015 07:39 PM)zer0 ? Wrote: [\[CITE\]](#) Worked on the PDF a bit today, hopefully done by Sunday night.

Thanks for dedicating your time to it.

?A?O - August 31, 2015, 11:34 am

(Aug 30, 2015 05:01 PM).Sinister Wrote: [\[CITE\]](#) Thanks for dedicating your time to it.

Yeah it's getting done, just school right now is cutting a lot of time into my personal time.

voldemort725 - September 1, 2015, 8:42 am

Fantastic guide. Really well written. Really appreciate the amount of effort that you put into this, it really shows and hopefully will protect some of the newbies out there!

CrypteMyJar - September 2, 2015, 1:42 pm

Amazing thread and Very useful tutorial , Thanks.

?A?O - September 4, 2015, 1:48 am

Appreciate all good feedback. Continuing to find and figure out things I want and don't want added to

this.

HIGH PAID FELLA - September 6, 2015, 6:00 am

Bumping this amazing mega-guide.

Sorrowful - September 6, 2015, 10:49 am

Solid guide from this man, but pretty sure insight takes the cake with their tutorial on how to install a VPN!

Still a great guide nonetheless.

?A?O - September 6, 2015, 11:57 am

(Sep 6, 2015 10:49 AM)Sorrowful Wrote: [\[CITE\]](#) Solid guide from this man, but pretty sure insight takes the cake with their tutorial on how to install a VPN!

Still a great guide nonetheless.

I explained the VPNs people should use, that's all. It's too simple to install a VPN to write about installing one in this guide.

Sorrowful - September 6, 2015, 2:24 pm

(Sep 6, 2015 11:57 AM)zer0 ? Wrote: [\[CITE\]](#) I explained the VPNs people should use, that's all. It's too simple to install a VPN to write about installing one in this guide.

Well keep up the work, atleast you don't create a group just to spam sections with cancerous tutorials on how build a dirt house in minecraft!

luckyns - September 7, 2015, 3:50 pm

Incredibly detailed, bravo it is ! Thank you !! :)

#Skyline - September 8, 2015, 7:32 pm

This should be a sticky Zer0, why you no sticky ?

?A?O - September 8, 2015, 7:59 pm

(Sep 8, 2015 07:32 PM)#Skyline? Wrote: [\[CITE\]](#) This should be a sticky Zer0, why you no sticky ?
Hah, not up to me bud ?

#Skyline - September 8, 2015, 8:47 pm

(Sep 8, 2015 07:59 PM)zer0 ? Wrote: [\[CITE\]](#) Hah, not up to me bud ?

You put so much work into this, you could print this out as a book and sell it to a university.

Anyways dude, as I've said before, this is a great tutorial if you want to learn about Anonymity. GJ zer0 ?

?A?O - September 11, 2015, 8:22 pm

Going to be updating a few things tomorrow or the next day. A few things I will change as things are starting to be used less frequently.

?eezy - September 11, 2015, 11:51 pm

Thanks for this. You obviously spent heaps of time on this and it looks great.
Bookmarked :)

Jaguar. - September 12, 2015, 6:08 am

Great guide thanks for this

Handiquacks - September 13, 2015, 4:43 pm

Solid guide, keep adding on to it looks very good.

Synapse. - September 14, 2015, 5:15 am

Great guide, man.

Good job.

Live5 - September 14, 2015, 3:02 pm

really good detailed post thx

Diamond09 - September 14, 2015, 4:45 pm

What a great guide OP!

But I have a concern. It mentions that your ISP does not have a clue that you are using Tor? How is this so? What about search terms on tor (providing tor is configured correctly with more security) I'm sorry if this has been discussed before...thanks

darkdexter - September 15, 2015, 12:04 am

thanks for sharing this great method

Irriducibili - September 15, 2015, 1:02 am

very cool guides

thank you bro :)

Kareov - September 15, 2015, 10:48 am

Thank you so much sir, that's a lot of new stuff I have learnt today.

Bigbroxy - September 15, 2015, 9:02 pm

Great information. Appreciate it all. Will definitely be using some of it. Very good job here. Thanks.

Zer0Degree5 - September 16, 2015, 3:32 am

Wow!! Top post here IMO. Very nice and high quality tutorial!

FRANKIE - September 16, 2015, 3:40 am

To be honest I had no idea about the metadata in a picture. Learning something new every day

Rottweiler. - September 16, 2015, 8:59 am

Thanks for this dude , its really helpfull :)

Kronicz - September 16, 2015, 7:50 pm

Great tutorial! Keep up the good shit m8

?MIN?M - September 17, 2015, 12:11 am

What I particularly found interesting was lynis. I am definately going to use it and see how I come up. I appreciate the helpful tutorial.bravo.

?A?O - September 17, 2015, 1:39 am

I'm currently working on subjects relating to cold boot attacks and prevent someone from dumping memory to get encryption keys but it's a lot of research since there is no surefire way of preventing it.

SwindlerBob - September 17, 2015, 7:58 am

Quick question in regards to some of this information. Is TOR still as secure as some people say or is there something new to replace TOR?

?A?O - September 19, 2015, 1:33 pm

(Sep 17, 2015 07:58 AM)SwindlerBob Wrote: [\[CITE\]](#) Quick question in regards to some of this information. Is TOR still as secure as some people say or is there something new to replace TOR? Nothing really new to replace TOR yet although there are a lot of security researchers currently looking into other options. Here's a PDF on something called HORNET: High-speed Onion Routing at the Network Layer that a team has been researching for a while.

<http://arxiv.org/pdf/1507.05724v1.pdf>

Also, TOR is not secure like it used to be. You can still use it for many things, but I wouldn't say its super secure by any means.

redasurC - September 19, 2015, 1:35 pm

Great information. Appreciate it all. Will definitely be using some of it. Very good job here. Thanks.

Verifying - September 20, 2015, 4:26 pm

Really nice and high quality tutorial, thanks!

Puppeteer - September 21, 2015, 1:35 am

This is a nice tut but didn't read everything. Posting so I can read it later

?A?O - September 23, 2015, 1:23 am

Been working a lot more directly with cryptography lately so hoping to add more information soon.

Money Talks. - September 23, 2015, 2:44 am

Bookmarked very nice and hq thread

Incendiary. - September 23, 2015, 7:26 am

(Sep 23, 2015 01:23 AM)zer0 ? Wrote: [\[CITE\]](#) Been working a lot more directly with cryptography lately so hoping to add more information soon.

Looking forward to the update. This is a insanely HQ thread, more people need to see it

SwindlerBob - September 24, 2015, 11:38 am

zer0 another question for you regarding tails. I have currently starting to set up my VM and want to load one with tails. What else other than the pre loaded package that comes with tails will I need? Also how to I load my PGP keys over to tails? I haven't seen a way how or tutorial online.

tommy44 - September 26, 2015, 9:04 am

Thanks for this tut, bookmarked so I can come back later :)

?A?O - September 28, 2015, 12:43 pm

(Sep 24, 2015 11:38 AM)SwindlerBob Wrote: [\[CITE\]](#) zer0 another question for you regarding tails. I have currently starting to set up my VM and want to load one with tails. What else other than the pre loaded package that comes with tails will I need? Also how to I load my PGP keys over to tails? I haven't seen a way how or tutorial online.

Sorry been away for the weekend, I'll try to send you a PM tonight regarding this.

novrina - September 28, 2015, 9:11 pm

fucking kontrol tutorial....!!!!

nice info

GL for u dude

PageMaster - September 29, 2015, 1:23 am

My only issue with this guide is that it perpetuates the Use of proxies for Staying anonymous. Proxies DO NOT WORK. Proxies ARE USELESS. And anyone who recommends them needs to stop. And anyone who insists that proxies are safe are either idiots, trolls, or trying to infect you. (AND HERE IS WHY: <https://www.youtube.com/watch?t=7&v=0QT4YJn7oVI>)
Watch the video LEARN and think twice. One of my top 10 favorite Defcon Talks delivered by Chema Alonso in Defcon 20 about How to own people using Javascript Botnets created by a Rogue "Anonymous" Proxy Server

?A?O - September 29, 2015, 12:40 pm

(Sep 29, 2015 01:23 AM)PageMaster Wrote: [\[CITE\]](#) My only issue with this guide is that it perpetuates the Use of proxies for Staying anonymous. Proxies DO NOT WORK. Proxies ARE USELESS. And anyone who recommends them needs to stop. And anyone who insists that proxies are safe are either idiots, trolls, or trying to infect you. (AND HERE IS WHY: <https://www.youtube.com/watch?t=7&v=0QT4YJn7oVI>)

Watch the video LEARN and think twice. One of my top 10 favorite Defcon Talks delivered by Chema Alonso in Defcon 20 about How to own people using Javascript Botnets created by a Rogue "Anonymous" Proxy Server

Nothing makes you 100% safe but SOCKS5 sure can help if used correctly alongside other methods. Maybe you should do some reading yourself because in my thread I state that nothing keeps you 100% safe, it just helps you. Also, people who tell someone to you a proxies are trying to infect someone? Might want to take some more time to read instead of preaching nonsense.

Also, in the context of my thread, no where do I say to use a proxy alone. It is always to be used within a chain or with other security measures being taken at the same time.

scruie - September 29, 2015, 12:49 pm

wow great post to get started, thanks!

PageMaster - September 29, 2015, 2:11 pm

(Sep 29, 2015 12:40 PM)zer0 ? Wrote: [\[CITE\]](#) Nothing makes you 100% safe but SOCKS5 sure can help if used correctly alongside other methods. Maybe you should do some reading yourself because in my thread I state that nothing keeps you 100% safe, it just helps you. Also, people who tell someone to you a proxies are trying to infect someone? Might want to take some more time to read instead of preaching nonsense.

Also, in the context of my thread, no where do I say to use a proxy alone. It is always to be used within a chain or with other security measures being taken at the same time.

Watch the video. all proxies are a risk EVEN SOCKS5. Even in a Chain. The proxie itself is the risk. That video demonstrates that.

?A?O - October 4, 2015, 3:11 am

Hopefully something new will be coming out in the relative future because TOR and that side of the web isn't what it used to be.

Crocs - October 4, 2015, 3:19 am

Good tutorial for starters, thanks.

?A?O - October 9, 2015, 1:30 pm

(Oct 4, 2015 03:19 AM)Tigris Wrote: [\[CITE\]](#) Good tutorial for starters, thanks.

Thanka, appriciate all feedback.

inkredibleandy1 - October 10, 2015, 8:34 pm

Thanks for sharing very important and useful post. Bless up man!

Vireo - October 11, 2015, 3:40 pm

(Oct 4, 2015 03:11 AM)zer0 ? Wrote: [\[CITE\]](#) Hopefully something new will be coming out in the relative future because TOR and that side of the web isn't what it used to be.

The problem isn't on the technical end, so I don't see how that would change anything. Maybe you don't frequent the right forums?

farux - October 11, 2015, 9:28 pm

Awesome guide! Bookmarking this so that I can reference back when needed. Thanks for taking the time to put this together!

astr0 - October 13, 2015, 7:58 pm

Wonderful thread zer0. Just curious as to what you might be planning on adding on? Also, it's nice to see another Crunchbang user ;)

blackmuggle - October 14, 2015, 11:35 am

thank you so much
you are a good man
i wish you good luck

Hypnotist - October 15, 2015, 6:39 am

Damn you covered a lot here... Nice share man!

435267 - October 16, 2015, 11:20 am

bookmarked also here.very good work.

?A?O - October 16, 2015, 12:39 pm

This weekend I'll be adding a section for QubeOS and possibly one other thing.

Mr_Brightside - October 21, 2015, 5:13 am

This is a excellent guide and helped me tons! ? thanks

MAHATMA_GHANDI - October 23, 2015, 12:55 pm

awsome guide man, bookmarked

GitBit - October 29, 2015, 6:26 am

Just wanted to say thanks for this, much of valuable resources there.
It will take some time to read it all.

Documentary - October 29, 2015, 8:04 pm

This is a very nice tutorial

doomkit - October 31, 2015, 1:22 am

thank you, for this usefull info and help contributing for this forum.

HFTetramorph - October 31, 2015, 12:35 pm

Nice guide, I would recommend adding BitLocker (Prebuilt into any server or pro+ version of Windows) to your list of Whole Drive Encryption. This is a nice little program because it also takes advantage of your TPM (if you have one) and has the ability to require a flash drive + PIN to decrypt your computer.

FrenchDoxx - November 5, 2015, 12:16 pm

Hello,

Javascript is dangerous ? It's break my anonymity ?

Stark-astic - November 7, 2015, 8:52 am

too good to be true shit. hahaha but everything is genuine and totally works (only if the person is cautious and flawless). :) good going dude. the way you have explained it all is just amazing. if some user still doesnt get it, he should retreat back to reading nursery rhymes.

Vu47K - November 12, 2015, 11:07 am

very Informative And Superior Tut

Thank You so much For this Amazing effort

?A?O - November 25, 2015, 4:52 pm

(Nov 12, 2015 12:07 PM)Vu47K Wrote: [\[CITE\]](#) very Informative And Superior Tut

Thank You so much For this Amazing effort

Thanks for the feedback.

SparkMasterTape - November 26, 2015, 11:03 am

Bookmarked for when I get home ;)

Can you access hf when using for? I'm thinking about swapping to tor.

Caliban - November 26, 2015, 12:50 pm

(Nov 26, 2015 12:03 PM)dignitasyo Wrote: [\[CITE\]](#) Bookmarked for when I get home ;)

Can you access hf when using for? I'm thinking about swapping to tor.

No. HF cant be accessed through proxies,vpn, tor. I think only socks4/5 may work on HF but when u get caught RIP in pepperoney lmao.

?A?O - December 2, 2015, 2:25 pm

(Nov 26, 2015 01:50 PM)AlbertWesker Wrote: [\[CITE\]](#) No. HF cant be accessed through proxies,vpn, tor. I think only socks4/5 may work on HF but when u get caught RIP in pepperoney lmao.

Socks proxies usually do the trick or using an RDP of sorts.

I'd suggest doing so personally but that's just me.

eandrew - December 2, 2015, 5:25 pm

This is a great guide! I learned new things from it!

EL BB - December 3, 2015, 1:48 am

Very comprehensive guide, thanks for writing it. Lots of resources. I know many of the ideas can be applied to mobile devices, perhaps a thread on mobile security would be good?

Landchester_Turtle - December 3, 2015, 4:27 pm

What are some of the best vpns out there?

?A?O - December 3, 2015, 11:56 pm

(Dec 3, 2015 05:27 PM)Landchester_Turtle Wrote: [\[CITE\]](#) What are some of the best vpns out there?

I'm going to sleep now but I'll send a pretty detailed PM tomorrow at some point.

Landchester_Turtle - December 4, 2015, 4:13 am

Really helpful thanks for making this guide

thefoxtroll - December 7, 2015, 4:12 am

Cool stuff in here, in the bookmarks it goes, until it gets to see the light of day when I have some

free time. Thanks :D

th3ThUnD3r - December 7, 2015, 7:25 am

wow,guide very useful and well done :)

1337Orb - December 7, 2015, 9:30 am

Nice bro this is a good tut but there are better tuts out there

__Joel - December 11, 2015, 8:08 am

By adding add ons to Tor you're reducing your anonymity. According to the owners of Tor it's best to not stand out from the rest of the Tor users and leave it as it is...

dimara - December 12, 2015, 10:40 am

Good luck Sir this is awesome!

Wezeen - December 13, 2015, 2:31 am

great guide... thanks ;)

Insane Developer - December 13, 2015, 2:50 am

This is HQ! Thanks a lot mate

Mataram - December 14, 2015, 7:31 am

Everything you wrote here is actually kind of interesting, since all of this could actually help.

Aluna - December 14, 2015, 9:51 am

Will be using nearly everything you've provided but with a bit more security just for my paranoia.

Ov3rFl0w_ - December 14, 2015, 10:45 am

I Recommend: ESET Nod32 Smart Security

In my opinion as ITC student ESET is the best Anti Virus in 2015

.

Btw Good HQ post , Keep it up

Maxiim - December 19, 2015, 5:33 pm

This thread so good that it deserves a bump

Miniature - December 19, 2015, 6:07 pm

Very nice thread. Good job, OP! :)

Fleckens - December 19, 2015, 6:08 pm

posting to save this for later.

Wealth. - December 20, 2015, 5:13 am

Wow

great thread

thanks

tcoX21 - December 21, 2015, 4:23 pm

Awesomeeee!! Thank you very much!!!

HiddenEyE - December 22, 2015, 10:15 pm

gush i love this thread, i kind of learnt a lot from it

Axios - December 23, 2015, 2:08 am

Thanks for the work done.

shortcode - December 23, 2015, 3:55 am

I would like to translate some parts of your article in Italian to use them for my website. I can?

?A?O - December 23, 2015, 5:03 pm

(Dec 23, 2015 04:55 AM)shortcode Wrote: [\[CITE\]](#) I would like to translate some parts of your article in Italian to use them for my website. I can?

Yeah that's fine.

Arbitrage - December 24, 2015, 5:50 am

This is a really excellent guide, thank you for sharing!

Cimex - December 24, 2015, 7:14 am

Very nice tutorial.

Rise up got rooted a few weeks ago though, so wouldn't trust it again just yet

Duke Da Beast - January 2, 2016, 2:26 am

what vpn's will work on tails os? i dont want to use win to run a .exe

arnity - January 2, 2016, 10:48 am

thanks for this guide, very nice detailed

xADHDx - January 2, 2016, 3:10 pm

Detailed post. I learned a little from this too. I wish we had more of this on hack forums.

cl@usi - January 3, 2016, 7:19 pm

Great guide, maybe you could mention freenet? It's a darknet similar to i2p

?A?O - January 10, 2016, 9:28 am

(Jan 3, 2016 08:19 PM)cl@usi Wrote: [\[CITE\]](#) Great guide, maybe you could mention freenet? It's a darknet similar to i2p

Honestly, I may just redo an updated thread with more of how I personally do my setup now. Would be less information but better software and tools.

bryan1 - January 11, 2016, 8:23 pm

nice tutorial great stuff

?MIN?M - February 2, 2016, 3:37 am

This is quite helpful for anyone looking, so i'mma bump it

estriquinina - February 2, 2016, 6:40 am

This is an amazing guide, thanks!

tacos912 - February 3, 2016, 8:40 am

This guide is absolutely fantastic. Thank you very much for taking the time. I had several questions I was going to post a thread about but no longer need to since you covered so much in here!

anOnlulz - February 4, 2016, 4:13 am

This thread is very detailed thanks :)

Caliban - February 4, 2016, 8:32 am

This is indeed a great guide, i remember when i read it for the first time and i was just like "what the fuck?" and now i actually comprehend it.

Coresus28 - February 4, 2016, 4:45 pm

I have only really skimmed this but it seems like a great guide. I'm just wondering if there is anything that can work specifically on windows since it was mentioned to never use windows and also just to ask why windows is dangerous.

Caliban - February 4, 2016, 6:25 pm

(Feb 4, 2016 05:45 PM)Coresus28 Wrote: [\[CITE\]](#) I have only really skimmed this but it seems like a great guide. I'm just wondering if there is anything that can work specifically on windows since it was mentioned to never use windows and also just to ask why windows is dangerous.

windows is full of spyware and most malware is designed for windows, also it isnt secure like tails/whonix

?Xe - February 5, 2016, 1:42 am

Extremely detailed and helpful, was very interested the VPN & TOR connection paths and gave me a bit more to think about :D

sHAY - February 5, 2016, 1:46 am

Awesome thread, This will be really usefull.

TurdFerguson - March 5, 2016, 8:05 am

Great tutorial. Just wish I could see the thread about packet stenography :(

HIGH PAID FELLA - March 5, 2016, 8:24 am

Please consider adding the following points:Cold Blood Attacks (yep, shutting down your encrypted box is not enough in some cases)

The specific dangers of TOR, such as a correlation attack, or other mistakes which can be found [here](#) and [here](#).

The new & TOR-based IM: Ricochet(.IM)

EDIT: and adding this source would be nice, it's a really interesting concept (<https://www.deepdotweb.com/2015/04/15/so-you-want-to-be-a-darknet-drug-lord/>)

libc - March 5, 2016, 11:26 am

(Mar 5, 2016 09:24 AM)astr Wrote: [\[CITE\]](#) Please consider adding the following points:Cold Blood Attacks (yep, shutting down your encrypted box is not enough in some cases)

The specific dangers of TOR, such as a correlation attack, or other mistakes which can be found [here](#) and [here](#).

The new & TOR-based IM: Ricochet(.IM)

EDIT: and adding this source would be nice, it's a really interesting concept (<https://www.deepdotweb.com/2015/04/15/so-you-want-to-be-a-darknet-drug-lord/>)

What makes you think "Ricochet" is any better than XMPP? The only obvious advantage I see is third parties (in theory) can't deduct who you're communicating with.

The fact that the client and the protocol itself are in their early stages and haven't been thoroughly audited yet is a major negative.

HIGH PAID FELLA - March 5, 2016, 11:27 am

(Mar 5, 2016 12:26 PM)libc Wrote: [\[CITE\]](#) What makes you think "Ricochet" is any better than XMPP? The only obvious advantage I see is third parties (in theory) can't deduct who you're

communicating with.

The fact that the client and the protocol itself are in their early stages and haven't been thoroughly audited yet is a major negative.

I agree 100%, just give it some time would be my 2 cents.

dotcomsuper - June 8, 2016, 9:26 pm

vpn72 most recommended russian products

tyga1z - June 10, 2016, 6:15 am

well done bro, but summarize it in a video form...

Ghostzapper - June 19, 2016, 5:06 pm

Very Good Information. Bookmarked. Thanks

Silly Putty - June 23, 2016, 4:06 am

Nice hide, sure it helped some users

camlto - July 22, 2016, 5:45 pm

High Quality stuff right here! Will come in very handy! Thanks a million times OP!

Dave from the lawyer firm - July 23, 2016, 7:44 am

thanks for the awesome share man <3

Denizen - July 24, 2016, 11:07 am

Great guide. Having known little, I feel like I know a tad more ^^

Question about Tor through VPN and vice versa:

Tor through VPN is straight forward (if I understood correctly). Turn on your PC => turn on VPN => open Tor => internet.

But for the VPN through Tor, the guide says: PC => encrypt with VPN => Tor => specific type of VPNs => internet. The step "encrypt with VPN," does this mean you would use 2 VPNs? ie. You first open Proxy.sh => Tor => AirVPN => internet ?

N0xeus - July 26, 2016, 2:35 am

Very good post. You answer a lot of questions, thanks !

Dave from the lawyer firm - July 26, 2016, 8:30 am

thanks for the awesome share man <3

cipherfly - August 18, 2016, 2:47 pm

Wow, i think i've never seen such an complex yet simple tutorial before. Great work man, helped me alot!

Nickname. - September 30, 2016, 2:50 am

Very nice and detailed guide!!

Posting this so I can find it back.

Once again,

thanks

NapoleonicCode - September 30, 2016, 3:55 am

Looks like a high quality guide that I will try out, thank you :) Which OS would you recommend for staying anonymous?

neb535 - October 5, 2016, 8:53 am

thanks for the share dude

Max P™ - October 5, 2016, 3:49 pm

RIP, when did this dude get closed??

22gotya - October 7, 2016, 3:29 pm

Thanks for the share buddy

I'm just trying to learn everything i possibly can

Mr.DoomHead - October 9, 2016, 6:54 am

Nice read thats for sure.

Thank you for putting this together, I grabbed a few bits of new info from it.

user088 - November 18, 2016, 11:48 am

Why isn't this guide encrypted?

Clubababa - November 20, 2016, 4:46 pm

Thanks you for the sharing this :)

m4Virus - November 21, 2016, 11:22 am

Perfect method (y) i will follow this method Step by Step , thanks a Lot

Xandolia - November 21, 2016, 12:13 pm

Thank you so much for this guide, Very detailed.

MrJohnCena - November 21, 2016, 3:29 pm

WOW ? Page Bookmarked. thanks for sharing this awesome anonimity guide. ill for sure use it. thanks once again.

Raph777 - November 23, 2016, 7:49 am

This guide is amazing and really useful, thank you so much!

NiceTutorialsDude - November 24, 2016, 5:48 am

Defenitly Bookmarked :p Thankssssssssssssssssssssssssss

Toxic Impact - November 24, 2016, 5:07 pm

Nice Thanks Will Try This soon

xanity - January 10, 2017, 1:54 pm

Bookmarked very nice and thread. Actually learned something.

dean094 - January 10, 2017, 8:29 pm

thank you man, nice tutorial)

meatyklackers - November 21, 2017, 5:17 pm

Amazing! Love the level of detail and effort that you put into this. Much appreciated.

Quanzo - August 14, 2018, 7:41 am

Bump this shit, really nice. I'll be back.

bird_1000 - *September 5, 2018, 8:12 am*

Still useful for everyday usage of the web in 2018. Thank you.

highboy - *July 1, 2023, 12:41 pm*

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

sesasafe - *September 28, 2023, 12:09 pm*

Would love to see a 2023 updated version!

denekzah - *September 3, 2026, 4:08 am*

WOW this is so usefull. Thank you.