Secure Operating Systems

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)

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

Proxy.sh

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

Private Internet Access

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

ZorroVPN

ZorroVPN Link: https://zorrovpn.com/

Other Notable VPNs (for additional levels of security)
CryptoStorm Link: https://cryptostorm.is/

Protection from DNS Leaking
IPLeak Link: https://ipleak.net/
LeakTest Link: https://www.dnsleaktest.com/

Or I can use 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
Tor is an open source browser project

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 - js blocker

Ghostery - Ghostery is a privacy based browser extension used to block specific tracking cookies along various sites.

RefControl - RefControl is an extention 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.

HTTPS Everywhere - Every link will be encrypted with https

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 - Google shows a lack of care for users privacy in general.we can use these instead
DuckDuckGo.com
Ixquick.com
Etools.ch
WebRTC Fix - This fixes a big security hole that can reveal you 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.

Invisible Internet Project (I2P)
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/

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.

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.

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/...s-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.
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-...op-of-tor/

Encryption

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. They 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-pgp/
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 is placed and is a very useful encryption tool.
VeraCrypt Link: https://veracrypt.codeplex.com/

Another good piece of encryption software is DiskCryptor which has similiar 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 encrypted an individual file or a whole folder. File encryption is a much simpler process that 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?...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 files 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 contains 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 files 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.fileshredder.org/
CCleaner: https://www.piriform.com/ccleaner

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 type, 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 of 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...x?id=11533
MD5/SHA-1 Hash Verification Software: https://www.raymond.cc/blog/7-tools-veri...a1-hashes/

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

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 # infront 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 that 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

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

Now finally you can be secure from nasty people.