DarkWeb User Guide

USB Device Manual

Privacy, Anonymity, and Security

Updated @ 7/12/21

Email: admin@juicypony.com
https://www.juicypony.com

Purchase Message

Congratulations on purchasing your device. In this device, there is no censorship to any information online. The custom made Tails disk software takes up about 8 GB of memory resulting in a 55GB, 23GB or a 7.2GB free memory space depending on your purchase. Please follow this guide to become familiar with the software interface and the basic darkweb practices. Please note that using a monitor alone will not make the USB drive work. You will need a computer with RAM, a CPU, and a network chip or WIFI adapter. This software will not work on a raspberry pi module.

For my safety, returns are only accepted 24 hours after the delivery time of the date if USB drive was unpackaged or 3 days after the delivery date if USB was packaged. Please use this link for the license agreement:

Table of Contents

Booting Up Software

1. On your Mac, Linux, or Windows computer, be sure to shut it down/power it off. If you have bluetooth on, turn it off. If you have your wifi network enabled, turn it off. Be sure to have a plug-in mouse and keyboard (No bluetooth connection for privacy and anonymity).
2. Insert your USB drive to any USB port available.
3. You want to go to your computer boot menu for this next step. Power on your computer and depending on the device you have, the key pressed to go to the boot menu is different. The table(next page)shows what key to press when your computer is starting up.
4. Select the disk that says ‘EPI Boot’ or ‘EPI USB Device’ or EFI USB Device’ or the option that contains the word ‘Generic’.
5. The software system will now load(If this is your first time running it, it may take a minute).
6. Confirm your language and select ‘start tails’.

Boot Menu Keys

Any Mac OS Computer	Alt or Option
Any Windows Computer	Shift-Restart
Acer	Esc or F12 or F9
Asus	Esc or F8
Dell	F12
HP	F9
Lenovo	F12 or F8 or F10
Samsung	ESC or F12 or F2
Sony	F11 or ESC or F10
Toshiba	F12
Others...	Esc or F12

Software Interface

Because you are using a seperate device (the USB), you are anonymous to any website. No one will know who you are since you have never put any personal information on your USB. The USB device has no tracking history and only uses the RAM on your computer instead of your SSD for data processing so that there is no evidence of you accessing any web services with the darkweb being one of them. The device IP is masked and a custom VPN is installed in the USB to ensure that no information is traceable. Any data packets sent in the web and in the software will be encrypted by our custom software.

A VPN stands for virtual private network. Generally, a VPN encrypts your wifi network and your connection to the internet. A VPN should not log your website activity which the custom made software and TOR does in a secure method. A VPN usually costs 5$/month, but on this software, it is free. Once a VPN is active, no one can see any contents that you are accessing on the internet.

Software Interface (Continued)

A custom antivirus program is also set on this USB. Any attempts that will reveal your identity on this USB or on the web will be useless to the hacker since everything on the USB will be encrypted by a private key, only accessible to you.

Your network settings is also only available for you to see as your configurations on the USB device is locked by the network itself. Any other applications will be blocked unless you personally allow or open them. Make sure Onion Circuits is also enabled on the device before opening up the web browser or any other online required applications. The use of pluggable transports will bypass ISP from their restrictions from the TOR Browser which is installed in this software.

This device is also mostly powered by TAILS. You can read the documentation online from the application.

Software Features

You may see that the date and time located on the top center of your screen is incorrect. The system settings are designed so that you appear in a different location than where you are at. You can safely connect to your network by hovering over the power logo on the top right, hovering over ‘Wi-Fi not connected’, and then clicking on ‘Select Network’. It is okay to select your own network since the system’s VPN is active. To confirm your anonymity and privacy, go to Applications ->Favorites->Tor Browser. Launch the Tor Browser and select Tor check. The IP address shown should be different than your actual IP address. To immediately exterminate any running processes/computer executions, remove the USB stick from the computer. This will still save the software, but not anything else. If there is any feature that asks you to download a file or to upgrade the system: Do not do it unless it is from the TAILS website. Downloaded files may try to disable security protocols in the system.

Save as Persistent

Everytime that you shutdown, restart, or pull the USB stick out of the computer, everything except for the custom software will be erased. This includes files that you saved and your saved network connection. To put this software system on save mode, go to: Applications->Tails->Configure persistent volume. Remember your passphrase that you set down. This will save any system changes that you make and any files in the ‘Tor Browser(persistent)’ folder. Beware that your security and anonymity may lower if you use this feature. The next time that you start tails, you can log-in using the persistent feature using the passphrase you set. This will open the last saved event on the software system. Files, configurations, bookmarks, and passwords will be saved with Persistent.

DuckDuckGo Browser

The Tor Browser that is installed on this software has some functionalities of the DuckDuckGo Browser. They do not log or track your information unless you enable the browser to do so in settings. The two most important features of the Browser is the shield icon and the broom icon. Use the broom icon once every day to select a new bridge and a new identity to the web. This will make identifying you impossible. The shield icon gives you security against cookies and tracking bots depending on the security level. Safest is recommended with safer on only if you want to watch videos. This will give another level of encryption to personal information.

DarkWeb Search Engines and Onion Links

Search Engines:
duckduckgo.com - https://3g2upl4pq6kufc4m.onion/
NotEvil - hss3uro2hsxfogfq.onion/
Torch - xmh57jrzrnw6insl.onion/
Ahmia - msydqstlz2kzerdg.onion
Hidden wiki - http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

Others:
Hidden answers - answerstedhctbek.onion
Dread - http://dreadditevelidot.onion/
Fake Identity -http://elfq2qefxx6dv3vy.onion/fakeid.php

Temporary Mail:
http://grrmailb3fxpjbwm.onion/
https://www.guerrillamail.com/
https://tempmailaddress.com
http://grrmailb3fxpjbwm.onion/

DarkWeb Search Engines and Onion Links Cont.

Full Mailbox:
Proton Mail - https://protonmail.com/ OR https://protonirockerxow.onion/login
torbox - http://torbox3uiot6wchz.onion/
elude - http://eludemaillhqfkh5.onion/
Riseup - http://nzh3fv6jc6jskki3.onion
mail2tor - http://mail2tor2zyjdctd.onion/

Anonymous Bitcoins

Go to Applications ->Internet ->Electrum Bitcoin Wallet. Name your wallet and click next. By default, select Standard wallet and click next. If you need a new wallet, select ‘Create a new seed’. Select Segwit and click next. Write down and store safely the wallet generation seed word codes. Create a password for your wallet. Your wallet is now ready to send and receive bitcoins. You can use bitcoin mixers/tumblers if the bitcoins need to be fully anonymous and untraceable.

Beware of Scams! Any websites that ask you to pay cryptocurrency is most likely a scam. Take caution if a web page asks you to do something on your end. If an onion web page asks you for your personal information, do not give it to them.

Data Encryption

Click on the clipboard icon on the top right of your screen or go to Applications -> Utilities -> Passwords and Keys. Go to GnuPG Keys. Click on File -> New -> PGP Key. Name your Key, use a fake name and email address. You can create a fake email address by going to a email link on page 11. Set your password to create your key. Private keys are in silver color and public keys are in gold color. Share your public key with people who you talk to so that they can encrypt and decrypt their messages towards your device. Export your public key by going to File -> Share -> Select the Tor Browser Folder. You should get an .asc file, that is your public key available for sharing. You can read the key by opening it on text editor.

For saving public keys from other people, download the .asc file to the Tor Browser Folder. Open up Passwords and Keys. Go to File -> Import -> Select the downloaded key -> Import.

Data Encryption (Continued)

Right click on files and select ‘encrypt’. Select the public keys of people who will be seeing those files. Sign the file using your public key. Enter your password. The file is now encrypted. To decrypt the file, download the file and right click to select ‘Open with Decrypt File’. You can also sign the file by right clicking the file and signing it by clicking ‘Sign’. Send the .sig file along with the encrypted files so that the second party can check whether the files has been tampered. To check if the signature is valid, right click the .sig file and select ‘Open with Verify Signature‘. If the notification says the signature is valid, then the files did not get touched by third parties.

Secure Data Deletion on USB

For removing files:

Right click on the file and select ‘wipe’.

For Full Data Deletion:

The USB device will have its contents unreadable and then deleted and also its software exterminated. Go to Applications -> Utilities -> Disks. Select the USB that you want to erase. Select the gears icon and then select ‘Overwrite existing data with zeroes’.