Tails

the**amnesic**incognito**live**system

Privacy for anyone anywhere

Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it to explicitly.

It is a complete operating system designed to be used from a DVD, USB stick, or SD card independently of the computer's original operating system. It is Free Software and based on Debian GNU/Linux.

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc.

use the Internet anonymously and circumvent censorship; all connections to the Internet are forced to go through the Tor network

leave no trace on the computer you are using unless you ask it explicitly

use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging

https://tails.boum.org

Tails sends its traffic through Tor.

Tails is built upon Debian

Online anonymity and censorship circumvention

Tor is an open and distributed network that helps defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Tor protects you by bouncing your communications around a network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Use anywhere but leave no trace

Using Tails on a computer doesn't alter or depend on the operating system installed on it. So you can use it in the same way on your computer, a friend's computer, or one at your local library. After shutting down Tails, the computer will start again with its usual operating system.

Tails is configured with special care to not use the computer's hard-disks, even if there is some swap space on them. The only storage space used by Tails is in RAM, which is automatically erased when the computer shuts down. So you won't leave any trace on the computer either of the Tails system itself or what you used it for. That's why we call Tails "amnesic".

This allows you to work with sensitive documents on any computer and protects you from data recovery after shutdown. Of course, you can still explicitly save specific documents to another USB stick or external hard-disk and take them away for future use.

State-of-the-art cryptographic tools

Tails also comes with a selection of tools to protect your data using strong encryption:

- Encrypt your USB sticks or external hard-disks using LUKS, the Linux standard for disk-encryption.
- Automatically use HTTPS to encrypt all your communications to a number of major websites using HTTPS Everywhere, a Firefox extension developed by the Electronic Frontier Foundation.
- Encrypt and sign your emails and documents using the de facto standard OpenPGP either from Tails email client, text editor or file browser.
- Protect your instant messaging conversations using OTR, a cryptographic tool that provides encryption, authentication and deniability.
- Securely delete your files and clean your diskspace using Nautilus Wipe.

Tails-OpenPGP • Signing Key

A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F