# Tails

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

## Privatsphäre für alle, überall

Tails ist ein Live-Betriebssystem, das darauf ausgerichtet ist Ihre Privatsphäre und Anonymität zu bewahren. Es hilft Ihnen dabei, das Internet so gut wie überall und von jedem Computer aus anonym zu nutzen, ohne dabei Spuren zu hinterlassen, sofern Sie dies nicht ausdrücklich wünschen.

Tails ist ein vollständiges Betriebssystem, das direkt von einer DVD, einem USB-Stick oder einer SD-Karte aus genutzt wird, unabhängig von dem auf dem Computer installierten Betriebssystem. Tails ist Freie Software und basiert auf Debian GNU/Linux.

Tails beinhaltet verschiedene Programme, die im Hinblick auf die Sicherheit vorkonfiguriert wurden: einen Webbrowser, einen Instant-Messaging-Client, ein E-Mail-Programm, ein Office-Paket, einen Bild- und Audioeditor etc.

das Internet anonym nutzen und Zensur umgehen; alle Verbindungen zum Internet werden zwingend durch das Tor Netzwerk geleitet;

auf dem verwendeten Computer keine Spuren hinterlassen, sofern Sie es nicht ausdrücklich wünschen

kryptographische Werkzeuge auf dem aktuellen Stand der Technik benutzen, um Ihre Dateien, E-Mails und Instant-Messaging-Nachrichten zu verschlüsseln

Tails sendet Daten über Tor

Tails basiert auf Debian.

**https://tails.boum.org**

## Onlineanonymität und Zensurumgehung

Tor ist ein offenes und verteiltes Netzwerk, das Ihnen dabei hilft, sich gegen eine Form der Netzwerküberwachung zu wehren, die persönliche Freiheit und Privatsphäre, vertrauliche Geschäftsbeziehungen, und die Sicherheit von Ländern gefährdet: die sogenannte »Verkehrsdatenanalyse«.

Tor schützt Sie, indem es Ihre Kommunikation durch ein verteiltes Netzwerk von Relais springen lässt, das von Freiwilligen aus aller Welt betrieben wird. Es verhindert, dass jemand der Ihre Internetverbindung beobachtet, nachvollziehen kann, welche Seiten Sie besuchen, und sorgt dafür, dass die von Ihnen besuchten Seiten Ihren tatsächlichen Standort nicht ausfindig machen können.

## Überall nutzen, ohne Spuren zu hinterlassen

Die Benutzung von Tails auf einem Computer verändert weder das installierte Betriebssystem, noch ist es von diesem abhängig. Es kann also gleichermaßen auf dem eigenen Computer, dem eines Freundes, oder einem Computer Ihrer örtlichen Bibliothek verwenden werden. Nachdem Sie Tails heruntergefahren haben, kann der Computer wie gehabt mit seinem üblichen Betriebssystem starten.

Tails ist mit großer Sorgfalt konfiguriert, nicht die Festplatten des Computers zu benutzen, auch dann nicht, wenn Auslagerungsspeicher (swap space) zur Verfügung steht. Der einzige von Tails genutzte Speicher ist der Arbeitsspeicher (RAM), der automatisch gelöscht wird, sobald der Computer herunterfährt. So hinterlassen Sie weder Spuren des Tails-Systems, noch dessen, was Sie auf dem Computer getan haben. Deshalb nennen wir Tails "amnestisch" (engl.: amnesic).

Dies erlaubt Ihnen auf jedem Computer an sensiblen Dokumenten zu arbeiten, und schützt Sie vor Datenwiederherstellung nach dem Herunterfahren. Natürlich können Sie weiterhin ausgewählte Dokumente und Dateien auf einem anderen USB-Stick oder einer externen Festplatte speichern, und für die zukünftige Nutzung mit sich nehmen.

## Kryptographische Werkzeuge auf dem aktuellen Stand der Technik

Tails beinhaltet eine Auswahl an Werkzeugen, um Ihre Daten mit starker Verschlüsselung zu schützen:

- Verschlüsseln Sie Ihren USB-Stick oder externe Festplatten mit LUKS, dem Linux-Standardprogramm zur Festplattenverschlüsselung.
- Verschlüsseln Sie mit HTTPS Everywhere Ihre Kommunikation mit einer Vielzahl großer Webseiten automatisch durch HTTPS. HTTPS Everywhere ist ein Firefox-Plugin, welches von der Electronic Frontier Foundation entwickelt wird.
- Verschlüsseln und signieren Sie Dokumente und E-Mails mit dem de facto Standard OpenPGP, entweder im Tails E-Mail-Client, im Text-Editor oder aus dem Datei-Browser heraus.
- Schützen Sie Ihre Unterhaltungen über Instant Messaging (IM) mit OTR - ein kryptographisches Protokoll, welches Verschlüsselung und Authentifizierung bietet, sowie dem Prinzip der glaubhaften Abstreitbarkeit (plausible deniability) folgt.
- Löschen Sie Ihre Dateien auf sichere Art und Weise und überschreiben Sie Ihre Festplatte mit Nautilus Wipe.

**Tails-OpenPGP • Signatur Schlüssel**

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