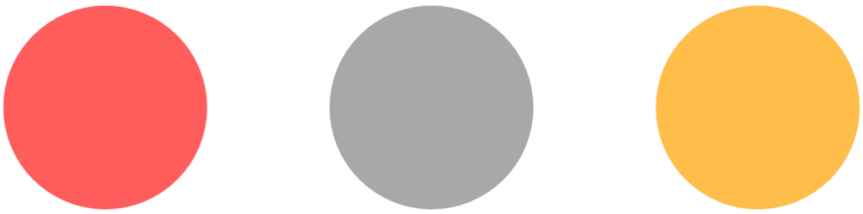

TAILS OS USB

BETRIEBSSYSTEM

EINFÜHRUNG, KURZANLEITUNG

& TIPPS

TAILSUSB.CH

Inhaltsverzeichnis

1. Was ist Tails?

Tails steht für „The Amnesic Incognito Live System“ und ist ein spezialisiertes Betriebssystem, das speziell entwickelt wurde, um deine Privatsphäre und Anonymität im digitalen Raum optimal zu schützen. In einer Zeit, in der Überwachung, Datensammlung und unerlaubtes Tracking zur alltäglichen Realität geworden sind, bietet Tails eine zuverlässige Möglichkeit, sich vor solchen Risiken effektiv zu schützen.

Das Betriebssystem basiert auf Debian Linux und ist so konzipiert, dass es vollständig vom USB-Stick oder einer DVD startet. Das bedeutet, du kannst Tails einfach und unkompliziert nutzen, ohne Veränderungen an deinem bestehenden System vorzunehmen. Das macht es ideal, wenn du etwa sensible Daten schützen oder sicherstellen möchtest, dass bei der Nutzung eines öffentlichen Computers keinerlei persönliche Informationen zurückbleiben.

Der Name „Amnesic“ (amnesisch) weist darauf hin, dass Tails keine Daten dauerhaft speichert oder Spuren hinterlässt. Sämtliche Aktionen, die du mit Tails durchführst, verschwinden spurlos, sobald du deinen Computer ausschaltest oder neu startest. Dateien, Verläufe oder persönliche Einstellungen bleiben niemals zurück, es sei denn, du entscheidest dich bewusst dafür, diese in einem speziell dafür vorgesehenen verschlüsselten Speicherbereich („Persistent Storage“) abzulegen.

Ein entscheidendes Merkmal von Tails ist die Integration des **Tor-Netzwerks**. Tor („The Onion Router“) sorgt für eine mehrfach verschlüsselte und anonymisierte Verbindung zum Internet. Diese Technologie leitet deine Daten über eine Reihe von weltweit verteilten Servern und verschleiert so effektiv deinen Standort sowie deine tatsächliche IP-Adresse. Dadurch wird es nahezu unmöglich, deine Identität zu verfolgen oder deine Online-Aktivitäten zu überwachen. Mit Tor kannst du anonym Webseiten besuchen, Dateien

teilen, E-Mails versenden oder anderweitig kommunizieren, ohne dass Dritte deine Aktivitäten nachvollziehen können.

Tails enthält von Haus aus eine sorgfältig zusammengestellte Auswahl an Programmen und Anwendungen, die auf grösstmögliche Privatsphäre ausgerichtet sind. Dazu gehören unter anderem ein speziell angepasster Webbrowser (basierend auf dem Tor Browser), E-Mail-Clients, Instant-Messenger für sichere Kommunikation, Office-Programme und Tools zur Verschlüsselung. Alle Anwendungen sind standardmässig so konfiguriert, dass sie keine personenbezogenen Daten speichern oder weitergeben.

Darüber hinaus bietet Tails zahlreiche Sicherheitsfunktionen wie einen "Gefährdungsreduzierten Modus" für das sichere Öffnen von Dokumenten und E-Mail-Anhängen, die eventuell gefährliche Inhalte enthalten könnten. Tails ist auch dafür bekannt, regelmässig aktualisiert zu werden, um stets auf aktuelle Bedrohungen und Sicherheitslücken reagieren zu können. Diese Updates sorgen dafür, dass du beim Surfen, Kommunizieren oder Arbeiten stets von den neuesten Schutzmechanismen profitierst.

Das Betriebssystem Tails richtet sich besonders an Nutzer, die aus beruflichen, politischen oder persönlichen Gründen auf umfassenden Datenschutz angewiesen sind. Dazu gehören Journalisten, Aktivisten, Whistleblower, Rechtsanwälte und politische Oppositionelle, die unter Umständen staatlicher Überwachung oder Zensur ausgesetzt sein könnten. Aber auch ganz gewöhnliche Internetnutzer profitieren stark von Tails, wenn es darum geht, ihre Privatsphäre vor unerwünschter Beobachtung oder gezielter Werbung zu schützen.

Ein weiterer grosser Vorteil von Tails ist seine Einfachheit und Benutzerfreundlichkeit. Du benötigst kein tiefgehendes technisches Wissen, um von den Vorteilen zu profitieren. Nach einer kurzen Eingewöhnungszeit kannst du problemlos von allen Sicherheitsfunktionen profitieren und dich darauf verlassen, dass deine Aktivitäten anonym bleiben.

Zusammenfassend bietet Tails eine vollständige, einfach nutzbare und sichere Umgebung für digitale Kommunikation und Aktivitäten im Netz. Egal, ob du Nachrichten liest, E-Mails versendest, Dokumente bearbeitest oder sensible Daten austauschst – mit Tails hast du stets die Kontrolle darüber, wer Zugriff auf deine Daten bekommt und wer nicht. Dieses Betriebssystem steht nicht nur für Sicherheit und Anonymität, sondern gibt dir auch die Freiheit zurück, dich ohne Angst vor unerwünschter Überwachung im digitalen Raum zu bewegen.

2. Tails OS vom USB Stick starten

Um Tails von einem USB-Stick zu starten, führe die folgenden Schritte aus:

1. Schalte deinen Computer vollständig aus.
2. Stecke den USB-Stick mit Tails in einen freien USB-Port.
3. Starte den Computer und öffne das Boot-Menü. Je nach Hersteller deines Computers erfolgt dies meist durch Drücken von Tasten wie F12, ESC, F10 oder Del während des Startvorgangs.
4. Wähle im Boot-Menü den USB-Stick als Startlaufwerk aus.
5. Bestätige deine Auswahl und warte, bis Tails geladen ist.

Nachdem Tails gestartet ist, kannst du mit der Nutzung beginnen und profitierst sofort von den Sicherheits- und Datenschutzfunktionen des Betriebssystems.

3. Erste Schritte nach dem Start

Nachdem Tails erfolgreich gestartet wurde, sind folgende erste Schritte wichtig:

1. Wähle deine bevorzugte Sprache und dein Tastaturlayout aus.
2. Richte bei Bedarf eine Internetverbindung ein. Tails unterstützt sowohl kabelgebundene (Ethernet) als auch drahtlose (WLAN) Netzwerke.
3. Überprüfe und bestätige die Tails-Einstellungen im Begrüßungsfenster.
4. Wenn du den verschlüsselten Speicher („Persistent Storage“) verwenden möchtest, kannst du ihn hier aktivieren oder einrichten.
5. Beginne mit der Nutzung der vorinstallierten Anwendungen, beispielsweise dem Tor Browser für anonymes Surfen oder Thunderbird für verschlüsselte E-Mail-Kommunikation.

4. Tipps nach dem Start

Die Nutzung von Tails bietet bereits eine erhebliche Erhöhung deiner digitalen Sicherheit und Privatsphäre. Dennoch gibt es einige wichtige Tipps und Praktiken, die du befolgen solltest, um deine Sicherheit weiter zu maximieren und Risiken effektiv zu minimieren.

4.1 Anonymität bewahren

Ein zentraler Vorteil von Tails ist die Nutzung des Tor-Netzwerks zur Wahrung deiner Anonymität. Dennoch ist es entscheidend, bestimmte Gewohnheiten zu entwickeln, um nicht versehentlich Informationen preiszugeben:

- **Vermeide persönliche Informationen:** Gib niemals persönliche Informationen wie Name, Adresse, Telefonnummer oder andere Details preis, die auf deine Identität schliessen lassen könnten.
- **Vorsicht bei Logins:** Verwende keine Websites, die ein Login erfordern und deine persönliche Identität preisgeben könnten, wenn du maximale Anonymität wahren willst. Wenn Logins unumgänglich sind, nutze separate, anonyme Konten.
- **Verhalten im Internet:** Bleibe achtsam und bewusst bei der Nutzung von Foren, sozialen Netzwerken oder Kommentarsektionen, da dein Schreibstil oder spezielle Informationen dich identifizierbar machen könnten.

4.2 Umgang mit Dateien und Anhängen

Dateien und Anhänge stellen ein mögliches Sicherheitsrisiko dar. Daher solltest du Folgendes beachten:

- **Dateien nur aus vertrauenswürdigen Quellen öffnen:** Öffne niemals Dateien oder Anhänge von unbekannten oder verdächtigen Quellen. Nutze den in Tails integrierten gefährdungsreduzierten Modus, um Anhänge sicher zu öffnen.
- **Vorsicht mit Dokumentenformaten:** Einige Dateitypen, insbesondere PDF- und Office-Dateien, können Malware enthalten. Nutze die in Tails enthaltenen Programme, um diese Dateien sicher zu öffnen und zu überprüfen.

4.3 Sicher Umgang mit Kommunikation

Tails bietet spezielle Tools für sichere Kommunikation. Nutze diese gezielt, um deine Privatsphäre zu schützen:

- **Verschlüsselte E-Mails nutzen:** Verwende Thunderbird mit OpenPGP-Verschlüsselung für E-Mails, um sicherzustellen, dass nur der Empfänger die Inhalte lesen kann.
- **Sichere Instant-Messenger:** Nutze Instant-Messenger wie den in Tails integrierten Messenger, der Verschlüsselung bietet. Vermeide Messenger, die nicht auf Verschlüsselung setzen.

4.4 Persistant Storage sicher nutzen

Tails erlaubt die Einrichtung eines verschlüsselten Persistent Storage, in dem Daten dauerhaft gespeichert werden können. Beachte dazu folgende Empfehlungen:

- **Verschlüsselten Speicher gezielt verwenden:** Speichere nur solche Daten dauerhaft, die du wirklich benötigst, und stelle sicher, dass sie sensible Informationen enthalten, die vor unbefugtem Zugriff geschützt werden müssen.
- **Starkes Passwort verwenden:** Richte ein komplexes, einzigartiges Passwort für deinen Persistent Storage ein und bewahre es sicher auf.
- **Daten regelmässig prüfen:** Überprüfe regelmässig die gespeicherten Daten und lösche Inhalte, die nicht länger benötigt werden.

4.5 Aktualisiserungen regelmässig durchführen

Tails veröffentlicht regelmässig Updates, um Sicherheitslücken zu schliessen und die Privatsphäre zu verbessern:

- **Regelmässige Updates durchführen:** Stelle sicher, dass du immer die neueste Version von Tails verwendest. Aktualisiere das System jedes Mal, wenn du dazu aufgefordert wirst.

- **Updates nur von offizieller Quelle beziehen:** Lade Updates ausschließlich von der offiziellen Tails-Website herunter, um Manipulationen vorzubeugen.

4.6 Umgang mit fremden und öffentlichen Computern

Tails ist ideal für die Nutzung an öffentlichen oder fremden Computern geeignet:

- **USB-Stick nie unbeaufsichtigt lassen:** Lass deinen Tails USB-Stick niemals unbeaufsichtigt, um Manipulation oder Diebstahl zu verhindern.
- **Geräte regelmässig wechseln:** Wechsle regelmässig das Gerät, von dem aus du Tails nutzt, um die Verfolgung zu erschweren.
- **Hardware-Sicherheit überprüfen:** Nutze möglichst Computer, deren Sicherheit dir bekannt ist, oder führe zumindest grundlegende Prüfungen der Hardware auf Auffälligkeiten durch.

4.7 Umgang mit Passwörtern

Ein sicherer Umgang mit Passwörtern ist essenziell:

- **Passwortmanager verwenden:** Nutze sichere Passwortmanager, um starke, einzigartige Passwörter für verschiedene Dienste zu erstellen und sicher zu verwalten.
- **Passwörter regelmässig ändern:** Ändere regelmässig deine Passwörter, insbesondere wenn du vermutest, dass eines kompromittiert sein könnte.

4.8 Sicherheitsbewusstsein entwickeln

Ein wichtiger Teil der digitalen Sicherheit ist das Bewusstsein für Risiken und Bedrohungen:

- **Informiere dich regelmässig:** Bleibe auf dem neuesten Stand über aktuelle Sicherheitsbedrohungen, um dich entsprechend schützen zu können.

- **Schulungen und Tutorials nutzen:** Nutze Schulungen, Workshops und Tutorials, die von Datenschutzexperten angeboten werden, um dein Wissen kontinuierlich zu erweitern.

4.91 Risiken durch Externe reduzieren

Externe Geräte wie USB-Sticks oder externe Festplatten können Sicherheitsrisiken bergen:

- **Externe Geräte nur aus vertrauenswürdigen Quellen nutzen:** Verwende nur externe Datenträger, deren Herkunft bekannt und vertrauenswürdig ist.
- **Verschlüsselung externer Datenträger:** Verschlüssele externe Datenträger, die sensible Daten enthalten, um sie vor unberechtigtem Zugriff zu schützen.

4.92 Netzwerke

Beim Verbinden mit Netzwerken sind folgende Sicherheitsmassnahmen wichtig:

- **Öffentliche Netzwerke meiden:** Nutze möglichst keine ungesicherten öffentlichen WLAN-Netzwerke. Falls unvermeidbar, stelle sicher, dass du über Tails eine sichere Verbindung aufbaust.
- **Verbindung prüfen:** Prüfe immer sorgfältig, mit welchem Netzwerk du dich verbindest, und bevorzuge vertrauenswürdige Netzwerke.

5. Copyright

Dieses Dokument wurde erstellt, um Nutzer bei der sicheren Verwendung von Tails OS zu unterstützen.

Tails ist ein unabhängiges Open-Source-Projekt unter tails.boum.org.

Diese Publikation steht in keiner offiziellen Verbindung zum Tails-Projekt.