

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

**Objectif :** Installer Tails sur une clé USB et l'utiliser pour naviguer sur Internet de manière totalement anonyme, sans laisser aucune trace sur l'ordinateur utilisé.

**Public visé :** Intermédiaire à Avancé (nécessite quelques notions d'informatique)

**Temps estimé :** 1 à 2 heures (téléchargement + installation)

**Niveau de difficulté :** ★★★☆☆ (Moyen)

### Prérequis :

- Un ordinateur récent (moins de 10 ans)
  - Une clé USB de **8 Go minimum** (deux clés recommandées)
  - Une connexion Internet
- 

### 1. Qu'est-ce que Tails ? (Le problème qu'il résout)

Tails est un système d'exploitation **amnesique** et **anonyme** qui se lance depuis une clé USB, sans rien installer sur l'ordinateur .

### Ce que Tails vous apporte

Problème	Solution Tails
Votre navigation est tracée (cookies, historique)	<b>Amnésie totale</b> : rien n'est enregistré après chaque session
Votre adresse IP vous identifie	Tout le trafic passe <b>obligatoirement par Tor</b> (réseau d'anonymisation)

---

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

Problème	Solution Tails
Votre fournisseur d'accès voit vos sites visités	Chiffrement des communications, impossible à espionner
Vous utilisez un ordinateur public/partagé	Aucune installation, aucune trace sur le disque dur
Vos fichiers personnels sont non chiffrés	<b>Stockage persistant chiffré</b> (optionnel) + VeraCrypt possible

### Pour qui est fait Tails ?

- **Journalistes** : pour communiquer avec des sources protégées
- **Activistes / Lanceurs d'alerte** : pour préserver leur anonymat
- **Citoyens sous régimes oppressifs** : pour contourner la censure
- **Tout utilisateur soucieux de sa vie privée** : pour une navigation véritablement anonyme

⚠ **Tails n'est pas une solution miracle** : il protège votre anonymat en ligne, mais ne vous rend pas invulnérable aux logiciels malveillants ou aux erreurs humaines.

## 2. Prérequis matériels

### Configuration minimale

Composant	Exigence
Processeur	64 bits x86-64 (Intel/AMD) – <b>les Mac M1/M2 ne sont PAS compatibles</b>
Mémoire vive (RAM)	2 Go minimum – <b>3 Go recommandés</b> pour un fonctionnement fluide

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

Composant	Exigence
Stockage	Clé USB de 8 Go minimum
Port	USB ou lecteur DVD

### Ordinateurs recommandés

Marque	Modèles qui fonctionnent bien
Lenovo ThinkPad	X250, X1 Carbon, T440, T480, T490
Dell	La plupart des modèles Latitude
HP	Série EliteBook

⚠ **À éviter** : Cartes graphiques Nvidia ou AMD Radeon (incompatibilités fréquentes) .

### Clés USB recommandées

Critère	Recommandation
Taille	8 Go minimum – <b>16 Go recommandé</b> si vous utilisez VeraCrypt en plus
Marques fiables	Kingston, Samsung, SanDisk
Version USB	3.0 ou supérieure (plus rapide – les ports USB 3.0 sont souvent bleus)
État	<b>Neuve de préférence</b> (les clés s'usent et ralentissent avec le temps)
💡 <b>Achetez en magasin physique</b> : Évitez les clés USB données ou achetées en ligne (risque de malware) .	

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### Combien de clés USB vous faut-il ?

Situation	Nombre de clés
Usage basique	1 clé (8 Go)
Avec stockage persistant Tails + VeraCrypt	<b>2 clés</b> (une pour Tails, une pour les données chiffrées)
Pour les mises à jour manuelles	3 clés (la 3e peut être plus petite)

### 3. Installation étape par étape

#### Étape 1 : Télécharger Tails

1. Rendez-vous sur le site officiel : <https://tails.net>
2. Cliquez sur **"Install Tails"** (en haut à droite ou sur la page d'accueil)
3. Sélectionnez votre système d'exploitation actuel :
  - Windows
  - macOS
  - Linux (dont Linux Mint)

#### Étape 2 : Télécharger et vérifier l'image Tails

##### Méthode recommandée (la plus simple) :

1. Téléchargez l'image USB de Tails (fichier .img)
2. Installez l'extension de navigateur **"Tails Verification"** (proposée automatiquement sur le site)
3. Une fois le téléchargement terminé, cliquez sur **"Verify Tails"**

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

4.Sélectionnez le fichier téléchargé

5.Attendez le message "**Verification successful!**" avant de continuer

⚠ **Ne sautez pas cette étape** : la vérification garantit que vous avez bien téléchargé la vraie version de Tails, sans modification malveillante.

---

### 4. Installation sur Linux Mint (méthodes recommandées)

🌀 **Linux Mint** propose plusieurs outils intégrés pour créer une clé USB bootable.

#### Méthode A – USB Image Writer (mintstick) – RECOMMANDÉE

**C'est la solution officielle de Linux Mint, préinstallée et sans surprise.**

#### Étapes :

- 1.Insérez votre clé USB (8 Go minimum)
- 2.Cliquez sur le **Menu** (en bas à gauche) et tapez "**USB Image Writer**"
- 3.Lancez l'application
- 4.Cliquez sur le bouton pour sélectionner l'image Tails (fichier .img)
- 5.Sélectionnez votre clé USB dans la liste (vérifiez bien le nom pour ne pas effacer un autre disque)
- 6.Cliquez sur "**Write**" (ou "Écrire")
- 7.Confirmerez l'effacement des données
- 8.Attendez la fin du processus (environ 10 minutes)

**Avantages** : Déjà installé, simple, zéro collecte de données.

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### Méthode B – Disques (GNOME Disks) – Alternative

#### Étapes :

1. Insérez votre clé USB
  2. Lancez l'application "**Disques**" (depuis le Menu)
  3. Sélectionnez votre clé USB dans la liste de gauche
  4. Cliquez sur les **trois points verticaux** → "**Restaurer l'image disque**"
  5. Choisissez le fichier image Tails téléchargé (.img)
  6. Sélectionnez votre clé USB comme destination (⚠ vérifiez bien)
  7. Cliquez sur "**Démarrer la restauration...**"
- 

### 5. Le stockage persistant Tails (par défaut)

#### À quoi ça sert ?

Par défaut, Tails est **amnesique** : tout ce que vous faites disparaît au redémarrage. Le **stockage persistant** intégré permet de conserver chiffrés certains fichiers et configurations d'une session à l'autre.

#### Ce que vous pouvez stocker de façon persistante

Élément	Utilité
Dossier Persistant	Vos fichiers personnels
Marque-pages Tor Browser	Vos sites favoris
Logiciels supplémentaires	Programmes que vous ajoutez

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

Élément	Utilité
Configuration réseau	Paramètres Wi-Fi, VPN
Clés PGP / SSH	Pour communications chiffrées

### Création du stockage persistant

1. Allez dans **Applications → Tails → Configure persistent volume**
2. Cliquez sur **"Continue"**
3. Choisissez une **phrase de passe** (longue et sécurisée – au moins 5-7 mots aléatoires)
4. **Notez-la sur papier** et conservez-la dans votre portefeuille
5. Cliquez sur **"Create"**
6. Choisissez les fonctionnalités à rendre persistantes
7. Redémarrez Tails

### 6. Ajout de VeraCrypt sur la clé Tails

#### Pourquoi utiliser VeraCrypt en plus du stockage persistant ?

Situation	Pourquoi VeraCrypt ?
Partage de fichiers avec Windows/macOS	Le stockage persistant Tails n'est lisible que sous Linux. VeraCrypt est compatible avec les 3 systèmes.
Déni plausible (volume caché)	Vous pouvez révéler un mot de passe "factice" tout en cachant vos vraies données.
Séparation des usages	Une partition chiffrée distincte pour les documents sensibles, indépendante de Tails.

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### Situation

### Pourquoi VeraCrypt ?

#### Confiance dans VeraCrypt

Certains utilisateurs préfèrent un outil qu'ils connaissent déjà.

### Prérequis importants

Avant de vous lancer, comprenez bien ceci :







**VeraCrypt sur la même clé USB que Tails est techniquement complexe et risque de casser Tails lors des mises à jour.**

**La méthode recommandée par la documentation officielle : utilisez deux clés USB distinctes :**

- **Clé n°1** : Tails (sans modification)
- **Clé n°2** : vos données chiffrées avec VeraCrypt, à brancher en complément

C'est plus simple, plus fiable, et tout aussi sécurisé.

## 7. Tableau comparatif : stockage persistant Tails vs VeraCrypt

Critère	Stockage persistant Tails (LUKS)	VeraCrypt (clé séparée)
Compatibilité Windows/macOS	 Non (Linux uniquement)	 Oui
Intégration avec Tails	 Automatique (déverrouillage au démarrage)	 Automatique également (VeraCrypt installé)
Déni plausible (volume)	 Non	 Oui

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

Critère	Stockage persistant Tails (LUKS)	VeraCrypt (clé séparée)
caché)		
<b>Facilité de création</b>	✓ Très facile (intégré)	⚠ Moyenne (nécessite un autre ordinateur)
<b>Risque de casser Tails</b>	✗ Aucun	⚠ Oui si sur la même clé
<b>Mises à jour Tails</b>	✓ Transparentes	⚠ Compliquées si VeraCrypt sur la même clé
<b>Vitesse</b>	✓ Rapide	⚠ Plus lent

### 8. Avantages et inconvénients de VeraCrypt sur la clé Tails

#### ✓ Avantages


Avantage	Explication
<b>Interopérabilité</b>	Vous pouvez lire/écrire sur votre partition chiffrée depuis Windows, macOS ou Linux
<b>Déni plausible</b>	VeraCrypt permet de créer un volume "caché" – un deuxième mot de passe dévoile un contenu factice, le vrai reste masqué
<b>Indépendance</b>	Vos données chiffrées ne dépendent pas du bon fonctionnement du stockage persistant Tails
<b>Confiance établie</b>	VeraCrypt est un standard depuis des années, audité régulièrement

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### ✗ Inconvénients

Inconvénient	Explication
<b>Complexité technique</b>	Créer une partition VeraCrypt sur la clé Tails demande de modifier la table de partition – risqué
<b>Risque de casser Tails</b>	Une mauvaise manipulation peut rendre Tails non bootable
<b>Mises à jour problématiques</b>	Tails se met à jour automatiquement. Une partition modifiée peut bloquer le processus
<b>Lenteur</b>	VeraCrypt est plus lent que LUKS (chiffrement natif Linux)
<b>Nécessite un autre ordinateur</b>	Vous ne pouvez PAS créer un volume VeraCrypt depuis Tails (l'outil n'est pas inclus pour la création)

### Verdict

Vous utilisez Tails...	Utilisez...
<b>uniquement sur votre ordinateur personnel</b>	Stockage persistant Tails (LUKS) – plus simple
<b>sur des ordinateurs publics variés (cybercafé, etc.)</b>	Stockage persistant Tails – plus fiable
<b>et devez partager des fichiers avec Windows/macOS</b>	VeraCrypt sur une <b>seconde clé USB séparée</b>
<b>et avez besoin de déni plausible</b>	VeraCrypt sur une <b>seconde clé USB séparée</b>
<b>et voulez absolument une seule clé</b>	 Possible mais déconseillé – faites une sauvegarde avant toute manipulation

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### 9. Comment créer une clé VeraCrypt séparée pour Tails (méthode recommandée)

#### Ce qu'il vous faut :

- Une **seconde clé USB** (8 Go minimum, peut être plus petite que la clé Tails)
- Un ordinateur avec **Windows, macOS ou Linux** (pas Tails)

#### Étapes (sous Windows ou Linux standard) :

1. Téléchargez VeraCrypt sur <https://www.veracrypt.fr>
2. Insérez votre seconde clé USB
3. Lancez VeraCrypt
4. Cliquez sur **"Create Volume"**
5. Choisissez **"Create a file container"** OU **"Create a volume within a partition/drive"**
  - Pour une clé USB, choisissez **"Create a volume within a partition/drive"**
6. Sélectionnez **"Standard VeraCrypt volume"** (ou "Hidden" si vous voulez le déni plausible)
7. Sélectionnez votre clé USB comme emplacement
8. Choisissez l'algorithme de chiffrement : **AES** (recommandé, rapide et sécurisé)
9. Choisissez une **phrase de passe forte** (différente de celle de Tails)
10. Formatez la partition en **FAT32** (pour compatibilité maximale)
11. Cliquez sur **"Format"** (cela efface toutes les données sur la clé)
12. Une fois créé, vous pouvez copier vos fichiers sensibles dans ce volume (il apparaît comme un disque normal après déverrouillage)

#### Utilisation dans Tails :

1. Démarrez Tails normalement
2. Branchez votre seconde clé USB (celle avec VeraCrypt)

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

3. Allez dans **Applications** → **Utilities** → **VeraCrypt**

4. Cliquez sur **"Select Device"** et choisissez votre clé USB

5. Cliquez sur **"Mount"**

6. Entrez votre phrase de passe

7. Le volume apparaît comme un disque normal dans le gestionnaire de fichiers



**Astuce** : Vous pouvez rendre ce processus plus rapide en ajoutant VeraCrypt à vos favoris persistants Tails.

## 10. Dépannage

### Tails ne démarre pas après avoir modifié la clé USB

Problème	Solution
J'ai créé une partition VeraCrypt	Re-téléchargez Tails et réinstallez-le sur une clé vierge.
sur la clé Tails	Considérez que cette clé est perdue.
La clé n'apparaît plus dans le Boot Menu	La table de partition a été corrompue. Réinstallez Tails.

### VeraCrypt ne voit pas ma clé USB dans Tails

Problème	Solution
La clé USB n'est pas montée	Vérifiez que la clé est bien reconnue dans le gestionnaire de fichiers (elle doit apparaître).
Le volume n'est pas détecté	Assurez-vous d'avoir bien sélectionné <b>"Select Device"</b> et non un fichier conteneur.

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### Je n'arrive pas à écrire sur mon volume VeraCrypt depuis Tails

Problème	Solution
Le volume a été formaté Tails n'a pas de problème en écriture sur FAT32	Tails n'a pas de problème en écriture sur FAT32. Vérifiez que vous avez bien déverrouillé le volume.
Le volume est en lecture seule	Démontez et remontez le volume. Si le problème persiste, reformatez le volume depuis un autre ordinateur.

## 11. Challenge 7 jours

**Objectif :** Maîtriser les bases de Tails et du chiffrement additionnel en 7 jours.

### Jour    Objectif

**Jour 1** Télécharger et installer Tails sur une clé USB

**Jour 2** Démarrage réussi – explorer le bureau, tester la navigation avec Tor Browser

**Jour 3** Créer le stockage persistant (phrase de passe)

**Jour 4** Créer une clé VeraCrypt séparée (sur un autre ordinateur)

**Jour 5** Dans Tails, déverrouiller la clé VeraCrypt et copier des fichiers

**Jour 6** Tester le "Wipe" (suppression sécurisée) d'un fichier sur la clé Tails

**Jour 7** Redémarrer sans ouvrir le stockage persistant – vérifier l'absence de traces

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### 12. En résumé – ce que vous gagnez

Action	Bénéfice
Installer Tails	Système anonyme et amnesique sur clé USB
Créer un stockage persistant	Conserver fichiers et réglages de façon chiffrée (simple, intégré)
Ajouter une clé VeraCrypt séparée	Compatibilité Windows/macOS + déni plausible possible
Utiliser Wipe	Supprimer définitivement un fichier (irrécupérable)
Faire une clé de secours	Protection contre la perte de données

### 13. Conclusion finale

Si vous êtes...	Choisissez...
Utilisateur occasionnel de Tails	Stockage persistant uniquement (plus simple)
Utilisateur régulier, sur votre ordinateur	Stockage persistant
Utilisateur qui partage des fichiers avec Windows/macOS	Stockage persistant + <b>clé VeraCrypt séparée</b>
Utilisateur qui a besoin de déni plausible	<b>Clé VeraCrypt séparée</b> (volume caché)
Débutant total	Commencez sans VeraCrypt – ajoutez-le plus tard si besoin

## Fiche Pratique N°32 – Installation et utilisation de Tails (The Amnesic Incognito Live System) - Naviguez anonymement sans laisser de traces V1.0

### Ce qu'il faut retenir :

⚠ **Ne tentez pas de mettre VeraCrypt sur la même clé USB que Tails** à moins d'être un utilisateur très avancé. Les risques de casser Tails (notamment lors des mises à jour) sont élevés.

✅ **La méthode recommandée** : deux clés USB distinctes

- Clé n°1 : Tails avec stockage persistant intégré
- Clé n°2 : VeraCrypt pour les données partagées ou à déni plausible

🔒 **Rappel final** :

- Tails **ne laisse aucune trace** sur l'ordinateur utilisé
  - Tout le trafic passe **obligatoirement par Tor** (anonymat)
  - Le **stockage persistant** intégré suffit pour 95% des usages
  - **VeraCrypt** est utile pour la compatibilité Windows et le déni plausible
- 

### Ressources officielles :

- Site officiel : <https://tails.net>
- Documentation complète : <https://tails.net/doc/index.fr.html>
- VeraCrypt : <https://www.veracrypt.fr>
- Support Tails : <https://tails.net/support>