Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

7 nov, 2026 · @Gabriel

Objectif : *Chiffrer vos fichiers sensibles (documents administratifs, photos personnelles, relevés bancaires) avec* ***Cryptomator*** *(adapté au cloud) ou* ***VeraCrypt*** *(conteneurs et disques locaux), pour que personne ne puisse les lire sans votre mot de passe, même si votre ordinateur, votre téléphone ou votre disque externe est volé.*

- ***Public visé :*** *Débutant à intermédiaire (Cryptomator), intermédiaire à avancé (VeraCrypt)*
- ***Temps estimé :*** *15 à 30 minutes*
- ***Difficulté :*** *★★☆☆☆ (Facile pour Cryptomator) à ★★★☆☆ (Moyen pour VeraCrypt)*
- ***Prérequis :*** *des fichiers sensibles à protéger ; un cloud synchronisé sur l'ordinateur (Nextcloud, kDrive, Google Drive…) si vous utilisez Cryptomator*
- ***Fiches associées :*** *N°16 (gestionnaire de mots de passe), N°19 (sauvegardes), N°34 (Nextcloud), N°31 (NAS)*

1. Pourquoi chiffrer vos fichiers ? (Le problème)

Situation	Conséquence
Vol d'ordinateur ou de disque externe	Sans chiffrement, le voleur peut lire vos fichiers en branchant le disque sur un autre ordinateur, sans aucun mot de passe.
Cloud classique (Google Drive, iCloud, OneDrive)	Le fournisseur détient les clés de chiffrement : il peut techniquement accéder à vos fichiers. Si votre compte est piraté, tout est exposé.
Clé USB perdue	Quiconque la trouve lit son contenu.
Réquisitions (Cloud Act)	Les autorités américaines peuvent exiger d'un fournisseur américain qu'il livre vos données, où qu'elles soient stockées.
Serveur piraté	Même un Nextcloud auto-hébergé (fiche N°34) peut être compromis. Le chiffrement côté client protège aussi dans ce cas.

Le bénéfice : un fichier chiffré est illisible sans la clé (votre mot de passe). En cas de vol, de piratage ou de réquisition, vos données restent confidentielles.

2. Les deux grandes solutions

Solution	Principe	Chiffrement	Adapté au cloud	Idéal pour
Cryptomator	Coffre : chaque fichier est chiffré séparément, noms de fichiers compris	AES-256	✅ Seuls les fichiers modifiés sont resynchronisés	Fichiers stockés dans un cloud

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

Solution	Principe	Chiffrement	Adapté au cloud	Idéal pour
VeraCrypt	Conteneur (un gros fichier « coffre »), partition ou disque entier	AES, Serpent, Twofish, Camellia, Kuznyechik, ou combinaisons	⚠️ Peu adapté : le conteneur est un seul gros fichier	Disques externes, clés USB, disque système

Notre recommandation :

- **Vous utilisez un cloud** (Nextcloud, kDrive, Google Drive, iCloud, OneDrive) : **Cryptomator**. Le fournisseur ne voit que des fichiers illisibles aux noms aléatoires.
- **Vous stockez en local** (disque externe, clé USB) : **VeraCrypt**, très robuste et rapide pour les gros volumes.
- **Les deux :** Cryptomator pour le cloud, VeraCrypt pour les sauvegardes locales.

3. Cryptomator : le chiffrement pour le cloud

Pourquoi Cryptomator ?

- **Libre** (code publié sur GitHub), développé par une société allemande (Skymatic).
- **Chiffrement côté client :** vos fichiers sont chiffrés sur votre appareil **avant** d'être synchronisés. Le cloud ne stocke que des données illisibles.
- **Fonctionne avec la plupart des clouds :** tout service qui synchronise un dossier sur votre ordinateur (Nextcloud, kDrive, Google Drive, iCloud, OneDrive, Dropbox…).
- **Transparent :** une fois déverrouillé, le coffre apparaît comme un disque virtuel ; vous travaillez normalement.
- **Gratuit sur ordinateur** (Windows, macOS, Linux), sans limitation.
- **Mobile (Android, iOS) :** application gratuite en **lecture seule** ; l'écriture (ajouter, modifier des fichiers) demande un achat unique d'environ 30 € par plateforme. Sur Android, un essai complet de 30 jours est proposé.

Comment faire ? (Pas à pas)

Étape 1 : Téléchargez et installez Cryptomator

Plateforme	Source
Windows / macOS / Linux	cryptomator.org › **Downloads** (gratuit) ; sous Linux aussi via Flathub ou AppImage
Android	Google Play, ou F-Droid (dépôt principal : « Cryptomator Lite », ou le dépôt F-Droid de Cryptomator)
iOS	App Store (gratuit en lecture seule, achat intégré pour l'écriture)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

Étape 2 : Créez un coffre dans votre cloud

1. Lancez Cryptomator.
2. Cliquez sur **Ajouter** › **Nouveau coffre**.
3. Donnez un nom au coffre (exemple : Documents sensibles).
4. **Emplacement :** choisissez le dossier de votre cloud synchronisé sur l'ordinateur, par exemple :
    - Nextcloud : `C:\Users\<vous>\Nextcloud\` ;
    - Google Drive : le dossier « Mon Drive » du lecteur Google Drive ;
    - iCloud : le dossier iCloud Drive ;
    - disque local : `D:\MesFichiers\`.
5. **Mot de passe :** choisissez un mot de passe **très fort** (phrase de passe de 5 mots ou plus), enregistrez-le dans votre gestionnaire de mots de passe (fiche N°16).
6. Acceptez de **créer une clé de récupération** : c'est une **suite de mots** qui permet de réinitialiser le mot de passe oublié. Copiez-la dans votre gestionnaire de mots de passe ou imprimez-la et rangez-la en lieu sûr.
7. Cliquez sur **Créer le coffre**.

Vous devez voir :

- le nouveau coffre dans la liste de Cryptomator, et dans votre cloud un dossier qui contient `vault.cryptomator` et un dossier `d`.

⚠️ Sans le mot de passe **et** sans la clé de récupération, vos fichiers sont perdus définitivement : il n'existe aucune porte dérobée.

Étape 3 : Déverrouillez et utilisez votre coffre

1. Dans Cryptomator, sélectionnez le coffre › **Déverrouiller**, puis saisissez le mot de passe.
2. Le coffre apparaît comme un **disque virtuel** (nouvelle lettre de lecteur sous Windows, volume monté sous macOS et Linux).
3. Copiez ou déplacez vos fichiers sensibles dans ce disque virtuel.
4. Travaillez normalement : Cryptomator chiffre en arrière-plan.
5. Quand vous avez terminé : **Verrouiller**. Le disque virtuel disparaît.

Vous devez voir :

- dans le dossier du cloud, uniquement des fichiers aux noms illisibles (terminés par `.c9r`).

Étape 4 : Synchronisez avec votre cloud

- Votre client cloud envoie automatiquement les fichiers chiffrés au serveur.
- Depuis un autre ordinateur : installez Cryptomator, ouvrez le même dossier synchronisé avec **Ajouter** › **Coffre existant** (fichier `vault.cryptomator`), puis déverrouillez-le.

Étape 5 (facultatif) : Utilisez Cryptomator sur mobile

1. Ouvrez Cryptomator › **Ajouter un coffre** › **Coffre existant**.

gabriel.ananda@mailo.com
CC BY SA

2. Choisissez votre service (Nextcloud via WebDAV, Google Drive, OneDrive, Dropbox…), connectez-vous, puis sélectionnez le fichier `vault.cryptomator`.
3. Déverrouillez avec le mot de passe.

Vous devez voir :

- vos fichiers en clair dans l'application (en lecture seule sans achat).

Limites de Cryptomator :

- Les noms de fichiers sont chiffrés : impossible de chercher un fichier depuis l'interface web du cloud (il faut déverrouiller le coffre).
- L'écriture sur mobile est payante (achat unique par plateforme).
- Léger surcoût de calcul, imperceptible sur un ordinateur récent.
- La taille des fichiers et leur nombre approximatif restent visibles pour le fournisseur.

4. VeraCrypt : le conteneur chiffré pour le stockage local

Pourquoi VeraCrypt ?

- **Successeur de TrueCrypt** (abandonné en 2014), libre, audité (audit Quarkslab de 2016).
- **Conteneur chiffré :** un seul fichier (exemple : `MonCoffre.hc`) qui se monte comme un disque.
- **Chiffrement robuste :** AES, Serpent, Twofish, Camellia ou combinaisons en cascade.
- **Chiffrement d'une partition, d'un disque externe ou du disque système** (Windows).
- **Rapide** et **portable** : un conteneur se transporte sur une clé USB.
- **Maintenu activement :** version 1.26.31 du 2 novembre 2026.

Comment faire ? (Pas à pas)

Étape 1 : Téléchargez et installez VeraCrypt

1. Téléchargez VeraCrypt depuis le site officiel **veracrypt.io** › **Downloads** (Windows, macOS, Linux).
2. Vérifiez si possible la signature PGP ou l'empreinte SHA256 publiées sur la page de téléchargement.
3. Installez :
    - **Windows :** acceptez l'installation du pilote ;
    - **macOS :** installez d'abord **FUSE-T** (recommandé sur les Mac à puce Apple) ou macFUSE, puis la version correspondante de VeraCrypt ;
    - **Linux :** paquet .deb ou .rpm, AppImage ou installateur générique.

⚠️ Méfiez-vous des sites de téléchargement tiers.

Étape 2 : Créez un conteneur chiffré

1. Lancez VeraCrypt.
2. Cliquez sur **Créer un volume**.
3. Choisissez **Créer un fichier conteneur chiffré** › **Suivant**.

gabriel.ananda@mailo.com
CC BY SA

4. Choisissez **Volume VeraCrypt standard** › **Suivant**.
5. **Emplacement du volume :** cliquez sur **Fichier…**, choisissez un dossier et un nom (exemple : `D:\MonCoffre.hc`) › **Suivant**.
6. **Options de chiffrement :** laissez **AES** et **SHA-512** › **Suivant**.
7. **Taille du volume :** par exemple 10 Go pour des documents › **Suivant**.
8. **Mot de passe :** phrase de passe très forte (20 caractères ou plus), enregistrée dans votre gestionnaire › **Suivant**.
9. **Formatage :**
    - système de fichiers **exFAT** pour un conteneur utilisable sous Windows, macOS et Linux (NTFS si vous restez sous Windows) ;
    - déplacez la souris au hasard dans la fenêtre jusqu'à ce que la jauge soit pleine (cela renforce l'aléa des clés) ;
    - cliquez sur **Formater**.
10. À la fin, cliquez sur **Quitter**.

Vous devez voir :

- le fichier `MonCoffre.hc` à l'emplacement choisi, de la taille prévue.

Étape 3 : Montez (ouvrez) votre conteneur

1. Dans la fenêtre principale de VeraCrypt, sélectionnez une lettre de lecteur libre (exemple : M:).
2. Cliquez sur **Fichier…** et choisissez `MonCoffre.hc`.
3. Cliquez sur **Monter** et saisissez le mot de passe.

Vous devez voir :

- un nouveau disque (M:) dans l'explorateur de fichiers.

Étape 4 : Utilisez le conteneur comme un disque normal

- Glissez-déposez vos fichiers dans le disque M:.
- Ouvrez et modifiez-les normalement.
- Quand vous avez terminé : sélectionnez le disque dans VeraCrypt › **Démonter**.

Étape 5 (facultatif) : Chiffrez une clé USB ou un disque externe entier

1. Branchez la clé USB et **copiez ailleurs son contenu** (le chiffrement d'un périphérique vide l'efface).
2. VeraCrypt › **Créer un volume** › **Chiffrer une partition/un disque non système** › **Suivant**.
3. Sélectionnez la clé USB, puis **Créer un volume chiffré et le formater**.
4. Suivez les mêmes étapes que pour un conteneur.

À chaque utilisation, la clé devra être montée avec VeraCrypt (**Montage automatique**).

Exemple d'utilisation :

- Créez un conteneur de 20 Go sur un disque externe pour vos documents administratifs.

gabriel.ananda@mailo.com
CC BY SA

- Montez-le, déposez les documents, démontez-le.
- Si vous perdez le disque, personne ne peut lire le conteneur sans le mot de passe.

Limites de VeraCrypt :

- **Peu adapté au cloud :** le conteneur est un seul gros fichier ; à chaque modification, le client cloud doit le resynchroniser (souvent en entier), avec un risque de conflit si deux appareils l'ouvrent.
- **Pas d'application mobile officielle :** la documentation de VeraCrypt cite des applications tierces compatibles, non développées par l'équipe.
- **Moins intuitif** que Cryptomator.

5. Cryptomator ou VeraCrypt : tableau comparatif

Critère	Cryptomator	VeraCrypt
Principe	Chaque fichier est chiffré séparément	Conteneur unique, partition ou disque
Adapté au cloud	✅	⚠️ Peu adapté
Applications mobiles	✅ Android et iOS (lecture gratuite, écriture payante)	❌ Pas d'application officielle
Algorithmes	AES-256	AES, Serpent, Twofish, Camellia, Kuznyechik, cascades
Libre	✅	✅
Chiffrement du disque système	❌	✅ (Windows)
Facilité d'utilisation	★★★★☆	★★★☆☆
Rapidité	★★★★☆	★★★★★
Idéal pour	Cloud	Disque externe, clé USB, disque système

6. Cas particuliers

Chiffrer un dossier existant avec Cryptomator

Cryptomator ne chiffre que le contenu d'un **coffre**. Pour protéger un dossier existant : créez un coffre, déplacez le dossier à l'intérieur, puis supprimez l'original non chiffré (et videz la corbeille).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

Échanger une clé USB chiffrée avec quelqu'un

- **VeraCrypt :** créez un conteneur sur la clé ; le destinataire doit installer VeraCrypt et connaître le mot de passe (transmis par un autre canal).
- **7-Zip :** une archive .7z protégée par mot de passe utilise AES-256 et chiffre aussi les noms de fichiers si vous cochez **Chiffrer les noms de fichiers**. C'est une solution simple et solide pour un envoi ponctuel. ⚠️ Évitez le format ZIP avec « ZipCrypto », facilement cassable.

Chiffrer tout le disque de l'ordinateur

Système	Solution
Windows	**BitLocker** (Windows Pro) ou **chiffrement de l'appareil** (Windows Famille sur matériel compatible), intégrés mais propriétaires ; ou **VeraCrypt** (chiffrement du système)
macOS	**FileVault** (intégré)
Linux	**LUKS**, proposé à l'installation de la plupart des distributions

Notre recommandation :

- **Windows :** activez au minimum BitLocker ou le chiffrement de l'appareil. ⚠️ Avec un compte Microsoft, la clé de récupération est sauvegardée par défaut sur votre compte en ligne : notez-la aussi hors ligne, et sachez que Microsoft peut y accéder. Pour un logiciel libre, préférez VeraCrypt (plus technique).
- **macOS :** activez FileVault (**Réglages Système** › **Confidentialité et sécurité** › **FileVault**).
- **Linux :** utilisez LUKS dès l'installation.

7. À savoir avant de se lancer

Crainte fréquente	La réalité
« Je perds tout si j'oublie mon mot de passe. »	Oui : c'est le principe. Enregistrez le mot de passe dans votre gestionnaire (fiche N°16) et, pour Cryptomator, gardez la clé de récupération en lieu sûr (papier dans un coffre, par exemple).
« Cryptomator ralentit-il mes fichiers ? »	Très peu : sur un ordinateur récent, c'est imperceptible, sauf pour de très gros fichiers.
« Cryptomator marche avec n'importe quel cloud ? »	Avec tout cloud qui synchronise un dossier sur l'ordinateur, et sur mobile avec les services pris en charge par l'application (WebDAV, Google Drive, OneDrive, Dropbox…).
« VeraCrypt fonctionne sur macOS et Linux ? »	Oui. Sur macOS, il faut d'abord installer FUSE-T ou macFUSE.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

Crainte fréquente	La réalité
« Comment partager un fichier chiffré sans cloud ? »	Un petit conteneur VeraCrypt ou une archive 7-Zip chiffrée ; le mot de passe se transmet par un autre canal.
« Le chiffrement protège-t-il contre les rançongiciels ? »	Non. Pendant que le coffre est déverrouillé, un logiciel malveillant peut le lire ou le chiffrer. Verrouillez-le après usage et gardez des sauvegardes (fiche N°19).

8. Plan d'action : par où commencer ?

Étape	Action	Outil	Temps
1	Repérez vos fichiers les plus sensibles (papiers d'identité, impôts, relevés bancaires).	–	10 min
2	Si vous avez un cloud : installez Cryptomator et créez un coffre.	Cryptomator	15 min
3	Si vous avez un disque externe ou une clé USB : installez VeraCrypt et créez un conteneur.	VeraCrypt	20 min
4	Déplacez vos fichiers sensibles dans le coffre ou le conteneur, puis supprimez les originaux.	–	10 min
5	Enregistrez mots de passe et clé de récupération dans votre gestionnaire (fiche N°16).	Gestionnaire	2 min
6	Vérifiez que vos sauvegardes contiennent bien le coffre ou le conteneur (fiche N°19).	–	5 min

9. Challenge 7 jours

Challenge : pendant 7 jours, protégez au moins 10 fichiers sensibles avec Cryptomator ou VeraCrypt.

- **Jour 1 :** installez Cryptomator et créez un coffre dans votre cloud.
- **Jour 2 :** déplacez 5 fichiers sensibles dans le coffre ; dans l'interface web du cloud, vérifiez qu'ils sont illisibles.
- **Jour 3 :** ouvrez le coffre depuis un autre ordinateur ou votre téléphone.
- **Jour 4 :** créez un conteneur VeraCrypt de 1 Go sur une clé USB ou un disque externe.
- **Jour 5 :** déplacez 5 autres fichiers dans le conteneur.

gabriel.ananda@mailo.com
CC BY SA

- **Jour 6 :** verrouillez le coffre et démontez le conteneur ; vérifiez que les fichiers ne sont plus accessibles.
- **Jour 7 :** supprimez les versions non chiffrées (et videz la corbeille) ; vérifiez que mots de passe et clé de récupération sont bien enregistrés.

Vous allez constater :

- vos fichiers sensibles restent protégés en cas de vol ou de piratage ;
- vous maîtrisez deux outils de chiffrement, pour le cloud et pour le local.

10. Alternatives et approfondissements

Si vous avez besoin de…	Essayez plutôt…
Chiffrer tout le disque de l'ordinateur	LUKS (Linux), FileVault (macOS), BitLocker ou VeraCrypt (Windows)
Chiffrer un dossier local sans conteneur	Un coffre Cryptomator stocké sur le disque local (fonctionne très bien)
Chiffrer un email	OpenPGP (GnuPG, Thunderbird) ou un service chiffré comme Proton Mail ou Tuta (fiche N°10)
Envoyer un fichier chiffré via un lien	Send (send.vis.ee, successeur libre de Firefox Send, liens qui expirent) ou CryptPad (fiche N°7)
Chiffrer un disque externe partagé entre Windows, macOS et Linux	VeraCrypt (volume en exFAT)

11. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Utiliser **Cryptomator**	Vos fichiers dans le cloud deviennent illisibles pour le fournisseur	Section 3
Utiliser un **conteneur VeraCrypt**	Coffre-fort numérique sur disque externe ou clé USB	Section 4
Chiffrer le **disque entier**	Un ordinateur volé ne livre pas vos données	Section 6
Ranger mots de passe et clé de récupération	Vous ne perdez pas l'accès à vos fichiers	Fiche N°16
Quitter le **stockage en clair**	Fin de la lecture par des tiers (fournisseur, voleur)	–

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

12. Conclusion générale

Si vous êtes…	Choisissez…
Utilisateur de cloud	Cryptomator
Utilisateur de stockage local (disque externe, clé USB)	VeraCrypt (conteneur ou disque entier)
Débutant	Cryptomator (interface simple, applications mobiles)
Très exigeant	VeraCrypt (plus d'options, chiffrement du disque système)
Les deux usages	Cryptomator pour le cloud + VeraCrypt pour la clé USB

À retenir absolument

- **Le chiffrement ne pardonne pas la perte du mot de passe :** gardez-le dans votre gestionnaire et conservez la clé de récupération Cryptomator en lieu sûr.
- **Cryptomator pour le cloud, VeraCrypt pour le local.**
- **Commencez petit :** un seul dossier (papiers d'identité, relevés bancaires), puis étendez.
- **Le chiffrement ne remplace pas la sauvegarde** (fiche N°19) ni les mises à jour.

Test final (Cryptomator) :

1. Créez un coffre Cryptomator dans votre dossier Nextcloud (ou autre cloud).
2. Déposez dans le coffre un fichier `test.txt` contenant « mot de passe secret ».
3. Laissez le cloud se synchroniser, puis ouvrez son interface web.
4. Cherchez `test.txt` : il n'apparaît pas, seulement des fichiers aux noms illisibles.
5. Ouvrez le coffre sur un autre ordinateur ou sur votre téléphone, puis ouvrez `test.txt`.
6. Si le texte est lisible : Cryptomator fonctionne ✅

Test final (VeraCrypt) :

1. Créez un conteneur VeraCrypt de 100 Mo sur votre bureau.
2. Montez-le (disque M:) et copiez `test.txt` dedans.
3. Démontez-le, puis essayez d'ouvrir `MonCoffre.hc` avec un éditeur : le contenu est illisible.
4. Remontez le conteneur et vérifiez que `test.txt` est toujours là.
5. Démontez-le.
6. Si tout fonctionne : VeraCrypt fonctionne ✅

Références

- Cryptomator – Tarifs et fonctionnalités (bureau gratuit ; mobile : lecture seule gratuite, écriture 29,99 €)
- Cryptomator – Android passe au modèle freemium (juillet 2026)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.1

- Cryptomator – Documentation : mot de passe et clé de récupération
- Cryptomator – Téléchargements
- VeraCrypt – Téléchargements (version 1.26.31 du 2 novembre 2026, FUSE-T sur macOS)
- VeraCrypt – Accueil et historique des versions
- VeraCrypt – Tutoriel pour débutants (création d'un conteneur)
- Privacy Guides – Changement de domaine du site de VeraCrypt (2025)

gabriel.ananda@mailo.com
CC BY SA