

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

Objectif : Chiffrer vos fichiers sensibles (documents administratifs, photos intimes, mots de passe, relevés bancaires) avec **Cryptomator** (cloud-friendly) ou **VeraCrypt** (conteneurs locaux) – pour que personne ne puisse y accéder sans votre mot de passe, même si votre ordinateur, téléphone ou disque dur externe est volé.

Public visé : Débutant à Intermédiaire (Cryptomator) à Avancé (VeraCrypt)

Temps estimé : 15 à 30 minutes

Niveau de difficulté : ★★☆☆☆ (Facile pour Cryptomator) à ★★★★★☆ (Moyen pour VeraCrypt)

Prérequis : Avoir des fichiers sensibles à protéger. Avoir un cloud (Nextcloud, Cryptpad, Google Drive, etc.) pour Cryptomator (optionnel).

1. Pourquoi chiffrer vos fichiers ? (Le problème)

Problème	Explication
Vol d'ordinateur ou de disque dur	Si votre ordinateur portable ou votre disque dur externe est volé, le voleur peut lire toutes vos données (documents, photos, mots de passe, etc.) en clair – aucun mot de passe requis.
Cloud non chiffré (Google Drive, iCloud, OneDrive)	Ces clouds stockent vos fichiers en clair sur leurs serveurs. L'entreprise peut les lire (et les analyse souvent). Si votre compte est piraté, vos fichiers sont exposés.
Clé USB perdue	Une clé USB perdue dans la rue donne accès à son contenu à n'importe qui.
Réquision légale (Cloud Act)	Les autorités américaines peuvent réquisitionner vos fichiers sur Google, iCloud ou OneDrive sans votre consentement.

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

Problème	Explication
Confiance envers un tiers	Même avec Nextcloud auto-hébergé (fiche N°7), le serveur peut être piraté. Le chiffrement côté client protège même dans ce cas.

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

2. Les deux grandes solutions

Solution	Type	Chiffrement	Cloud-friendly	Idéal pour
Cryptomator	Chiffrement côté client (chaque fichier individuellement)	AES-256	✓ Oui (travaille avec n'importe quel cloud)	Protéger des fichiers sur le cloud (Google Drive, Nextcloud, etc.)
VeraCrypt	Conteneur chiffré (un seul fichier "coffre")	AES-256, Serpent, Twofish, ou combinaisons	✗ Non (le conteneur se comporte comme un fichier, mais le cloud doit le synchroniser entièrement à chaque modification)	Protéger des fichiers localement (disque dur, clé USB)

Notre recommandation :

- **Vous utilisez un cloud** (Nextcloud, Google Drive, iCloud, OneDrive)
→ **Cryptomator** (chaque fichier est chiffré individuellement, le cloud ne voit que des blocs illisibles).
- **Vous stockez localement** (disque dur, clé USB) → **VeraCrypt** (conteneur très robuste, plus rapide pour les gros volumes).

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

•**Vous voulez le meilleur des deux mondes** → Utilisez **Cryptomator** pour le cloud, **VeraCrypt** pour les sauvegardes locales.

3. Cryptomator : le chiffrement pour le cloud

Pourquoi Cryptomator ?

- Open-source** (code auditable sur GitHub).
- Chiffrement de bout en bout** : vos fichiers sont chiffrés **avant** d'être envoyés dans le cloud. Le fournisseur de cloud ne voit que des blocs de données aléatoires.
- Fonctionne avec tous les clouds** : Nextcloud, Google Drive, iCloud, OneDrive, Dropbox, pCloud, etc.
- Transparent** : une fois déverrouillé, Cryptomator crée un disque virtuel (comme une clé USB). Vous travaillez normalement, Cryptomator chiffre en arrière-plan.
- Applications mobiles** (iOS, Android) : vous pouvez déchiffrer vos fichiers sur téléphone.
- Gratuit** sur ordinateur. Application mobile payante (5-10 €) ou gratuite via F-Droid (Android).

Comment faire ? (Pas à pas)

Étape 1 : Téléchargez et installez Cryptomator

Plateforme	Source
Windows / macOS / Linux	Site officiel : cryptomator.org → "Download" → Gratuit
Android	F-Droid (recommandé, gratuit) → recherchez "Cryptomator"
iOS	App Store (payant, environ 10 €)

Étape 2 : Créez un coffre (vault) dans votre cloud

1. Lancez Cryptomator.

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

2. Cliquez sur **"Ajouter un coffre"** (Add Vault).
3. Choisissez **"Créer un nouveau coffre"** .
4. Donnez un nom au coffre (ex: Documents sensibles).
5. **Emplacement** : sélectionnez le dossier de votre cloud synchronisé en local.

- **Nextcloud** : C:\Users\...\Nextcloud\Cryptomator\
- **Google Drive** : C:\Users\...\Google Drive\Cryptomator\
- **iCloud** : C:\Users\...\iCloud Drive\Cryptomator\
- **Disque local** : D:\MesFichiers\

6. **Mot de passe** : choisissez un mot de passe **très fort** (20+ caractères, stockez-le dans Bitwarden – fiche N°16). **Ne le perdez pas** : sans lui, vos fichiers sont perdus définitivement (pas de récupération possible, pas de backdoor).
7. (Optionnel) Sauvegardez la **clé de récupération** (fichier .bkup) – stockez-la dans Bitwarden ou sur une clé USB hors ligne.
8. Cliquez sur **"Créer"** .

Étape 3 : Déverrouillez et utilisez votre coffre

1. Dans Cryptomator, cliquez sur le coffre → **"Déverrouiller"** (entrez votre mot de passe).
2. Le coffre apparaît comme un **disque virtuel** (sur Windows, une nouvelle lettre de lecteur ; sur Linux/macOS, un dossier monté).
3. **Déplacez ou copiez vos fichiers sensibles** dans ce disque virtuel.
4. Travaillez normalement (ouvrez, modifiez, sauvegardez). Cryptomator chiffre automatiquement.
5. Quand vous avez terminé : dans Cryptomator, cliquez sur **"Verrouiller"** (le disque virtuel disparaît).

Étape 4 : Synchronisez avec votre cloud

- Si votre cloud (Nextcloud, Google Drive) synchronise le dossier **Cryptomator**, les blocs chiffrés sont envoyés au serveur.
- Depuis un autre ordinateur (ex: votre ordinateur de travail) : installez Cryptomator, ouvrez le même cloud, déverrouillez le coffre avec votre mot de passe.

Étape 5 (optionnel) : Utilisez Cryptomator sur mobile

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

- Sur Android (F-Droid) : ouvrez Cryptomator → "Ajouter un coffre" → choisissez "Cloud" → sélectionnez Nextcloud (ou autre) → connectez-vous → déverrouillez avec le mot de passe.
- Sur iOS : même principe (application payante).

Exemple d'utilisation :

- Vous avez des photos de passeport, des contrats de travail, des relevés bancaires dans un dossier Documents/Sensible.
- Créez un coffre Cryptomator dans votre Nextcloud.
- Déplacez ces fichiers dans le coffre.
- Sur votre téléphone, installez Cryptomator, connectez-vous à Nextcloud, déverrouillez le coffre – vous accédez aux fichiers mais le cloud ne voit que du chiffré.

Limites de Cryptomator :

- Les noms de fichiers sont chiffrés (le cloud voit des noms aléatoires : aB3dF9xY.bin). Impossible de rechercher un fichier directement depuis le cloud (il faut déverrouiller le coffre).
- Les applications mobiles sont payantes sur iOS (mais gratuites sur Android via F-Droid).
- Léger ralentissement (chiffrement/déchiffrement en temps réel) – imperceptible sur un ordinateur moderne.

4. VeraCrypt : le conteneur chiffré pour stockage local

Pourquoi VeraCrypt ?

- **Successeur de TrueCrypt** (après son arrêt brutal), open-source, audité.
- **Conteneur chiffré** : un seul fichier (ex: moncoffre.hc) qui contient tous vos fichiers, comme une clé USB virtuelle.
- **Chiffrement très robuste** : AES-256, Serpent, Twofish, ou combinaisons (AES + Twofish + Serpent).
- **Chiffrement de disque entier** (optionnel) : vous pouvez chiffrer tout votre disque système.

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

- **Très rapide** (pas de surcharge réseau).
- **Portable** : vous pouvez transporter votre conteneur sur une clé USB.

Comment faire ? (Pas à pas)

Étape 1 : Téléchargez et installez VeraCrypt

- Site officiel : veracrypt.fr (ou veracrypt.eu).
- Téléchargez la version pour votre système (Windows, macOS, Linux).
- Installez (sur Windows, acceptez l'installation du driver).

Étape 2 : Créez un conteneur chiffré

1. Lancez VeraCrypt.
2. Cliquez sur **"Créer un volume"** (Create Volume).
3. Choisissez **"Créer un conteneur de fichiers chiffrés"** → Suivant.
4. **Standard VeraCrypt** (par défaut) → Suivant.
5. **Emplacement** : choisissez où enregistrer votre conteneur (ex: D:\MonCoffre.hc). Le fichier peut porter n'importe quel nom (même monfichier.iso ou photo.jpg pour le cacher). Cliquez sur **"Sélectionner"**.
6. **Algorithme de chiffrement** : laissez **AES-256** (suffisant). Suivant.
7. **Taille** : choisissez la taille du conteneur (ex: 10 Go pour des documents, 100 Go pour des photos/vidéos). Suivant.
8. **Mot de passe** : choisissez un mot de passe **très fort** (stockez-le dans Bitwarden). **Ne le perdez pas**.
9. **Formatage** : laissez **FAT** (compatible) ou **NTFS** (Windows uniquement). Choisissez la taille de cluster par défaut.
10. **Formatage** : bougez la souris aléatoirement pendant quelques secondes (cela génère des données aléatoires). Cliquez sur **"Formatter"**.
11. La création prend quelques minutes selon la taille. Cliquez sur **"Terminer"**.

Étape 3 : Montez (ouvrez) votre conteneur

1. Dans VeraCrypt, sélectionnez une lettre de lecteur libre (ex: C: est déjà pris, choisissez M: ou N:).
2. Cliquez sur **"Sélectionner un fichier"** et choisissez votre conteneur (MonCoffre.hc).

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

3. Cliquez sur "**Monter**".
4. Entrez votre mot de passe.
5. Un nouveau disque apparaît dans l'explorateur (ex: MonCoffre (M:)).

Étape 4 : Utilisez votre conteneur comme un disque normal

- Glissez-déposez des fichiers dans le disque M:.
- Ouvrez, modifiez, sauvegardez normalement.
- Quand vous avez terminé : dans VeraCrypt, sélectionnez le disque et cliquez sur "**Démonter**".

Étape 5 (optionnel) : Chiffrement d'une clé USB entière

1. Branchez votre clé USB.
2. Dans VeraCrypt → "Créer un volume" → "Chiffrer une partition / disque non système" → Suivant.
3. Choisissez la clé USB → "Créer un volume VeraCrypt chiffré" → Suivant.
4. Le reste est similaire à la création d'un conteneur, mais la clé USB entière sera chiffrée (vous devrez la monter avec VeraCrypt à chaque utilisation).

Exemple d'utilisation :

- Vous avez une clé USB avec vos documents administratifs (contrats, impôts, etc.).
- Créez un conteneur VeraCrypt de 20 Go sur cette clé USB.
- Montez-le, déposez vos documents.
- Démontez-le. Si vous perdez la clé, personne ne peut lire les fichiers (pas de mot de passe).

Limites de VeraCrypt :

- **Pas compatible cloud** (le conteneur est un seul fichier ; si vous le mettez dans Nextcloud, chaque petite modification force la synchronisation du **conteneur entier**, ce qui est inefficace et peut consommer de la bande passante).
- **Pas de version mobile officielle** (il existe des forks, mais peu maintenus).
- **Moins intuitif** pour les débutants (plus technique que Cryptomator).

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

5. Cryptomator vs VeraCrypt : tableau comparatif

Critère	Cryptomator	VeraCrypt
Modèle	Chaque fichier est chiffré individuellement	Conteneur unique (fichier image)
Cloud-friendly	✓ Oui (les blocs sont synchronisés individuellement)	✗ Non (le conteneur entier est synchronisé à chaque modification)
Applications mobiles	✓ iOS (payant), Android (gratuit via F-Droid)	✗ Non (pas officielles)
Chiffrement	AES-256	AES-256, Serpent, Twofish, ou combinaisons
Open-source	✓	✓
Chiffrement de disque entier	✗ Non	✓ Oui
Facilité d'utilisation	★★★★☆	★★★★☆
Rapidité	★★★★☆ (léger ralentissement)	★★★★★ (très rapide)
Idéal pour	Cloud (Nextcloud, Drive, iCloud)	Stockage local (disque dur, clé USB)

6. Cas particuliers

Chiffrer un dossier entier (sans conteneur, avec Cryptomator)

Cryptomator ne peut chiffrer qu'un "coffre" (dossier spécifique). Il ne peut pas chiffrer un dossier arbitraire déjà existant sans le déplacer.

Solution : Créez un coffre Cryptomator dans votre cloud, puis déplacez votre dossier sensible à l'intérieur.

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

Chiffrer une clé USB pour l'échanger avec quelqu'un (sans logiciel)

Méthode : Créez un conteneur VeraCrypt sur la clé USB. La personne destinataire doit avoir VeraCrypt installé pour déchiffrer. Ce n'est pas idéal pour un échange grand public.

Alternative : Utilisez **Cryptomator** + un cloud (Nextcloud) + partage de lien (avec mot de passe). Mais le destinataire a besoin de Cryptomator.

Alternative plus simple (moins sécurisée) : Utilisez un archive ZIP avec mot de passe (mais le chiffrement ZIP est faible). Préférez **7-Zip** avec chiffrement AES-256 (mais moins robuste que VeraCrypt).

Chiffrer son disque dur entier (ordinateur)

Système	Solution
---------	----------

Windows	BitLocker (intégré, mais propriétaire) ou VeraCrypt (disque système)
---------	--

macOS	FileVault (intégré, propriétaire) – plus simple que VeraCrypt
-------	--

Linux	LUKS (intégré, open-source, recommandé) ou VeraCrypt
-------	--

Notre recommandation :

- Windows : préférez **VeraCrypt** (open-source) à BitLocker (propriétaire, potentielle backdoor).
- macOS : utilisez **FileVault** (intégré, suffisant, mais propriétaire). Si vous êtes exigeant, VeraCrypt (mais plus complexe).
- Linux : utilisez **LUKS** (intégré à l'installation, open-source, fiable).

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

7. À savoir avant de se lancer

Crainte fréquente	La réalité
"Je vais perdre mes fichiers si j'oublie mon mot de passe."	Oui. C'est le principe : sans le mot de passe, personne (même vous) ne peut déchiffrer les fichiers. Stockez votre mot de passe dans Bitwarden (fiche N°16) et sur un papier dans un coffre.
"Cryptomator ralentit-il l'accès à mes fichiers ?"	Un tout petit peu (l'ordinateur chiffre/déchiffre en temps réel). Sur un ordinateur moderne, c'est imperceptible sauf pour les très gros fichiers (> 1 Go).
"Puis-je utiliser Cryptomator avec n'importe quel cloud ?"	Oui, y compris Nextcloud auto-hébergé, Google Drive, iCloud, OneDrive, Dropbox, pCloud, etc.
"VeraCrypt est-il compatible avec macOS / Linux ?"	Oui, VeraCrypt est multiplateforme. Sous Linux, nécessite veracrypt (dans les dépôts) ou installation manuelle.
"Et si je veux partager un fichier chiffré avec quelqu'un (sans cloud) ?"	Utilisez VeraCrypt avec un petit conteneur (ex: 50 Mo) que vous envoyez par email ou clé USB. L'autre personne a besoin de VeraCrypt (ou de la version portable) et du mot de passe.
"Le chiffrement protège-t-il contre les virus / ransomwares ?"	Non. Si votre ordinateur est infecté, le ransomware peut chiffrer vos fichiers pendant que le coffre est déverrouillé. Déverrouillez votre coffre uniquement quand vous en avez besoin, et verrouillez-le après.

8. Plan d'action : par où commencer ?

Étape	Action	Outil	Temps
1	Identifiez vos fichiers les plus sensibles (documents administratifs, photos intimes, mots de passe, relevés bancaires).	—	10 min

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

Étape	Action	Outil	Temps
2	Si vous avez un cloud (Nextcloud, Google Drive) : installez Cryptomator et créez un coffre.	Cryptomator	15 min
3	Si vous avez un disque dur externe ou une clé USB : installez VeraCrypt et créez un conteneur.	VeraCrypt	20 min
4	Déplacez vos fichiers sensibles dans le coffre/le conteneur.	—	10 min
5	Stockez le mot de passe dans Bitwarden (fiche N°16).	Bitwarden	2 min
6	(Optionnel) Sauvegardez la clé de récupération Cryptomator (ou le conteneur VeraCrypt) sur un second disque.	—	5 min

9. Challenge 7 jours

Challenge : Pendant 7 jours, utilisez Cryptomator (ou VeraCrypt) pour protéger au moins **10 fichiers sensibles** (documents administratifs, photos, etc.).

Jour 1 : Installez Cryptomator. Créez un coffre dans votre cloud Nextcloud (ou Google Drive).

Jour 2 : Déplacez 5 fichiers sensibles dans le coffre. Vérifiez que le cloud (interface web) affiche des fichiers illisibles.

Jour 3 : Déverrouillez le coffre depuis un autre ordinateur (ou votre téléphone). Accédez aux fichiers.

Jour 4 : Créez un conteneur VeraCrypt de 1 Go sur votre clé USB (ou disque dur externe).

Jour 5 : Déplacez 5 autres fichiers dans le conteneur VeraCrypt.

Jour 6 : Démontez le coffre Cryptomator et le conteneur VeraCrypt. Vérifiez que les fichiers ne sont plus accessibles (disparus du disque virtuel).

Jour 7 : (Optionnel) Supprimez les versions non chiffrées de ces fichiers (corbeille, dossiers d'origine). Stockez le mot de passe dans Bitwarden.

À la fin :

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

- Vos fichiers sensibles sont protégés même en cas de vol ou de piratage.
- Vous maîtrisez deux outils de chiffrement (cloud et local).

10. Alternatives et approfondissements

Si vous avez besoin de...	Essayez plutôt...
Chiffrer un disque dur entier (système)	VeraCrypt (disque système), LUKS (Linux), FileVault (macOS) – ou BitLocker (Windows, mais propriétaire)
Chiffrer un dossier local (sans conteneur)	Utilisez Cryptomator (stockez le coffre en local, pas dans le cloud) – ce n'est pas l'usage prévu mais ça fonctionne
Chiffrer un email (pièce jointe)	Utilisez PGP (GnuPG) – fiche dédiée à venir
Chiffrer un fichier en ligne (partage rapide)	Utilisez Send (Firefox Send-like, auto-destruction) – ou CryptPad (fiche N°7) qui chiffre déjà les fichiers
Chiffrer un disque dur externe (multi-systèmes)	VeraCrypt (compatible Windows/macOS/Linux)

11. En résumé (ce que vous gagnez)

Action	Bénéfice
Utiliser Cryptomator	Protéger vos fichiers dans le cloud (Nextcloud, Google Drive, iCloud) – le fournisseur ne voit que du bruit aléatoire
Utiliser VeraCrypt (conteneur)	Protéger vos fichiers sur disque dur local ou clé USB – coffre-fort numérique
Utiliser VeraCrypt (disque entier)	Protéger tout l'ordinateur – même en cas de vol, le voleur ne peut pas démarrer sur votre disque sans le mot de passe

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

Action	Bénéfice
Stocker le mot de passe dans Bitwarden	Ne pas perdre l'accès à vos fichiers chiffrés
Quitter le stockage en clair (cloud ou disque)	Plus de risque de lecture par des tiers (Google, Microsoft, Apple, voleur)

Conclusion générale

Si vous êtes...	Choisissez...
Utilisateur de cloud (Nextcloud, Google Drive, iCloud)	Cryptomator (cloud-friendly, chaque fichier chiffré individuellement)
Utilisateur de stockage local (disque dur externe, clé USB)	VeraCrypt (conteneur ou disque entier)
Débutant / non technique	Cryptomator (interface plus simple, application mobile, compatible cloud)
Exigeant / paranoïde	VeraCrypt (plus robuste, plus d'algorithmes, chiffrement de disque entier)
Vous avez besoin des deux (cloud + local)	Cryptomator pour le cloud + VeraCrypt pour la clé USB (les deux sont gratuits)

À retenir absolument :

- **Le chiffrement ne protège pas contre la perte de mot de passe.**
Stockez-le dans Bitwarden **et** sur un papier (coffre).
- **Cryptomator = cloud. VeraCrypt = local.** Choisissez l'outil adapté à votre usage.
- **Commencez petit** : cryptez un seul dossier (vos relevés bancaires ou photos de passeport). Une fois le réflexe pris, étendez à tous vos fichiers sensibles.
- **Le chiffrement est une couche de protection supplémentaire.** Il ne remplace pas la sauvegarde (fiche N°19) ni l'antivirus.

Fiche Pratique N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol V1.0

Test final (Cryptomator) :

- 1.Installez Cryptomator. Créez un coffre dans votre dossier Nextcloud (ou Google Drive).
- 2.Déposez un fichier test.txt contenant "mot de passe secret" dans le coffre.
- 3.Synchronisez votre cloud. Connectez-vous à l'interface web du cloud.
- 4.Cherchez le fichier test.txt (il n'apparaît pas – à la place, des blocs illisibles).
- 5.Déverrouillez le coffre sur un autre ordinateur (ou votre téléphone). Ouvrez test.txt.
- 6.Si le texte est lisible : **Cryptomator fonctionne** ✓

Test final (VeraCrypt) :

- 1.Installez VeraCrypt. Créez un conteneur de 100 Mo sur votre bureau.
- 2.Montez le conteneur (disque M:). Copiez test.txt dedans.
- 3.Démontez le conteneur. Essayez d'ouvrir le fichier MonCoffre.hc (il ne s'ouvre pas – c'est un conteneur binaire).
- 4.Remontez le conteneur, vérifiez que test.txt est toujours là.
- 5.Démontez, supprimez le fichier MonCoffre.hc (ou rangez-le dans un dossier sécurisé).
- 6.Si tout fonctionne : **VeraCrypt fonctionne** ✓