



ENCRYPTER SES DONNÉES SENSIBLES

PRÉPARÉ PAR: PIERRE ROBILLARD

2 NOVEMBRE 2023



ENCRYPTER SES DONNÉES SENSIBLES

QU'EST-CE QU'ENCRYPTER?

L'APPLICATION VERACRIPT

- COMMENT CRÉER UN CONTAINER
- COMMENT ACCÉDER AUX DONNÉES DU CONTAINER

Encrypter ses données sensibles



Encrypter des données, c'est par définition, coder, chiffrer des données afin d'en garantir la confidentialité.

L'encryptage empêche un hacker ou une personne qui utilise votre portable ou votre ordinateur d'accéder et de lire vos données sensibles telles que:

1. Vos relevés bancaires, d'investissements et de cartes de crédit;
2. Votre testament;
3. Vos rapports d'impôts;
4. Vos photos, etc.

Encrypter ses données sensibles



Pour les encrypter, je vous propose l'application:
VeraCrypt.

VeraCrypt, une application « Open Source » permet de crypter des disques durs ou des clés USB, de créer des partitions chiffrées ou bien encore des containers protégés.

Un container, c'est un gros fichier, une sorte de clé USB virtuel puisque:

- 1) Brancher une clé USB à un ordinateur donne accès aux données de la clé comme décrypter un container donne accès aux données du container;
- 2) Débrancher une clé USB empêche l'accès aux données comme crypter un container empêche l'accès aux données.
- 3) Dans les deux cas, les fichiers apparaissent dans une arborescence sous une lettre

Création d'un container

Accéder au site: VeraCrypt.fr et cliquer sur Download.

Cliquer ensuite sur le lien approprié pour votre ordinateur pour télécharger l'application et cliquer de nouveau pour l'installer.



Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, v critical when security software is concerned. Thank you.

[Supported versions of operating systems](#)

For those seeking support for the TrueCrypt format, please visit [dedicated page for VeraCrypt version 1.25.9](#).

Latest Stable Release - 1.26.7 (Sunday October 1st, 2023)

-  **Windows:**
 - EXE Installer: [VeraCrypt Setup 1.26.7.exe](#) (PGP Signature)
 - MSI Installer (64 bit) for Windows 10 and later: [VeraCrypt_Setup_x64_1.26.7.msi](#) (PGP Signature)
 - Portable version: [VeraCrypt Portable 1.26.7.exe](#) (PGP Signature)
 - Debugging Symbols: [VeraCrypt_1.26.7_Windows_Symbols.zip](#) (PGP Signature)
-  **macOS:**
 - macOS Monterey 12 and later: [VeraCrypt_1.26.7.dmg](#) (PGP Signature)
 - [OSXFUSE](#) 4 or newer must be installed.
-  **Linux:**
 - Generic Installers: [veracrypt-1.26.7-setup.tar.bz2](#) (PGP Signature)
 - Linux Legacy installer for 32-bit CPU with no SSE2: [veracrypt-1.26.7-x86-legacy-setup.tar.bz2](#) (PGP Signature)

Création d'un container (suite)

The image shows a Windows desktop with several applications open: Corbeille, Microsoft Edge, Google Chrome, Firefox, and CCleaner. The VeraCrypt application is running, displaying the 'Assistant de création de volume VeraCrypt' window. The 'Créer un fichier conteneur chiffré' option is selected, and the 'Suivant >' button is circled in red. The 'Type de volume' window is also open, showing the 'Volume VeraCrypt standard' option selected, with the 'Suivant >' button circled in red. The 'Créer un volume' button in the main VeraCrypt window is also circled in red.

Assistant de création de volume VeraCrypt

Assistant de création de volume

- Créer un fichier conteneur chiffré**
Crée un disque virtuel chiffré dans un fichier. Recommandé pour les utilisateurs novices.
[Plus d'infos](#)
- Chiffrer une partition/un disque non système**
Chiffre une partition non système sur tout disque interne ou externe (ex : clé USB). Optionnellement, crée un volume caché.
- Chiffrer la partition ou l'intégralité du disque système**
Chiffre la partition/le disque où est installé Windows. Qui veut accéder au système, lire/écrire des fichiers, etc., devra entrer le bon mot de passe à chaque fois que Windows démarre. Crée un système caché (optionnel).
[Plus d'infos sur le système de chiffrement](#)

[Aide](#) < Précédent Suivant > Annuler

Assistant de création de volume VeraCrypt

Type de volume

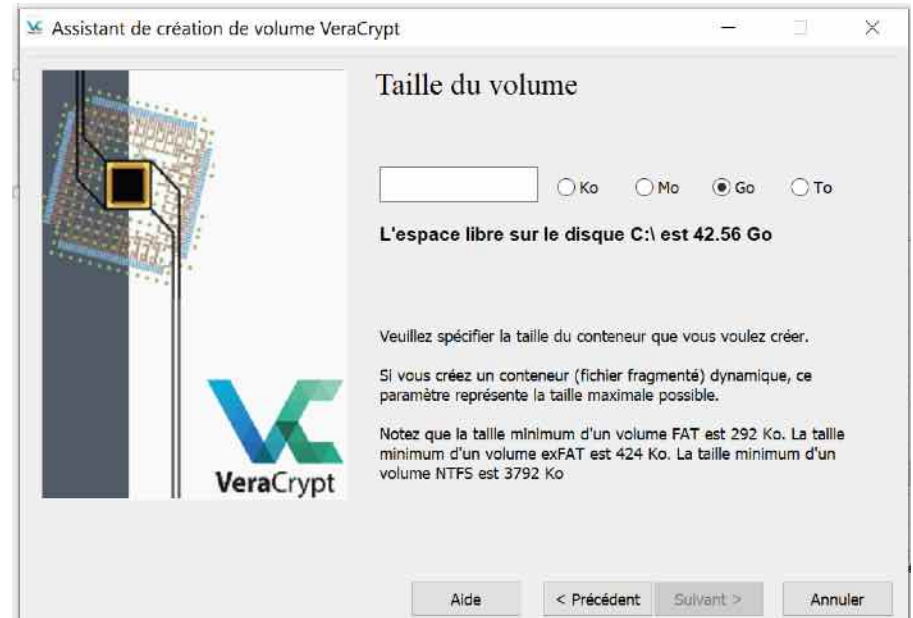
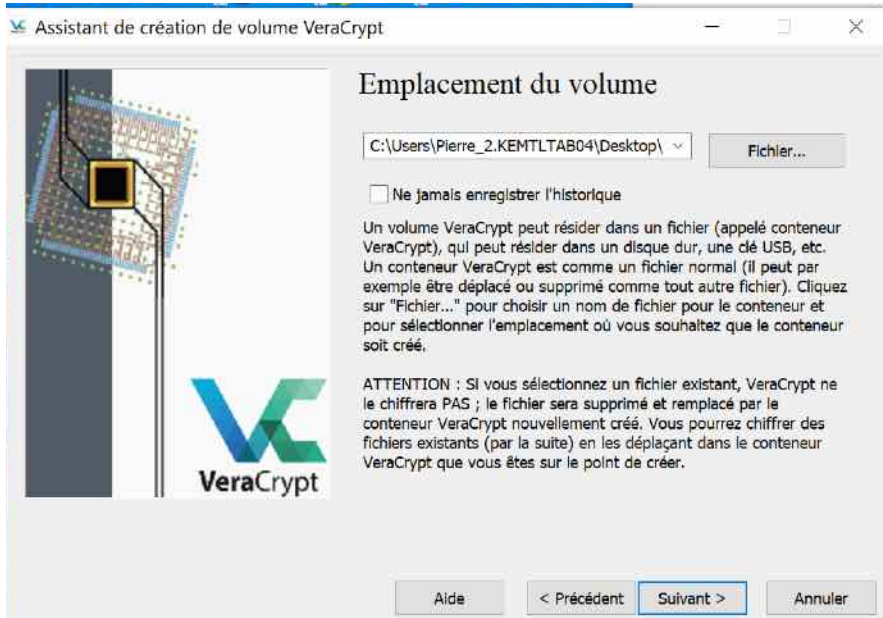
- Volume VeraCrypt standard**
Sélectionnez cette option si vous voulez créer un volume VeraCrypt normal.
- Volume VeraCrypt caché**
Il se peut que vous soyez forcé par quelqu'un de révéler votre mot de passe. Il y a des situations où vous ne pouvez pas refuser de divulguer le mot de passe (ex : par une extorsion). L'utilisation d'un volume caché vous permet de résoudre de telles situations sans donner le mot de passe de votre volume.
[Plus d'infos sur les volumes cachés](#)

[Aide](#) < Précédent **Suivant >** Annuler

Création d'un container (suite)

Choisissez l'emplacement du fichier du container et sa taille.

Accepter les choix proposés par défaut.



Création d'un container (suite)

Entrer le mot de passe voulu



Assistant de création de volume VeraCrypt

Mot de passe du volume

Mot de passe :

Confirmer :

Utiliser fichiers clés

Afficher le mot de passe

Saisir un PIM

Il est très important que vous choisissiez un bon mot de passe. Vous devriez éviter d'utiliser un mot simple que l'on trouve dans un dictionnaire (ou une combinaison de plusieurs de ces mots). Il ne devrait pas contenir de noms ou de dates de naissance. Il ne devrait pas être facile à deviner. Un bon mot de passe est une combinaison de minuscules et de majuscules, de chiffres et de caractères spéciaux comme @ ^ = \$ * + etc. Il est recommandé de choisir un mot de passe d'au moins 20 caractères (le plus long, le mieux). La longueur maximale est de 64 caractères.

Aide < Précédent Suivant > Annuler

Création d'un container (suite)



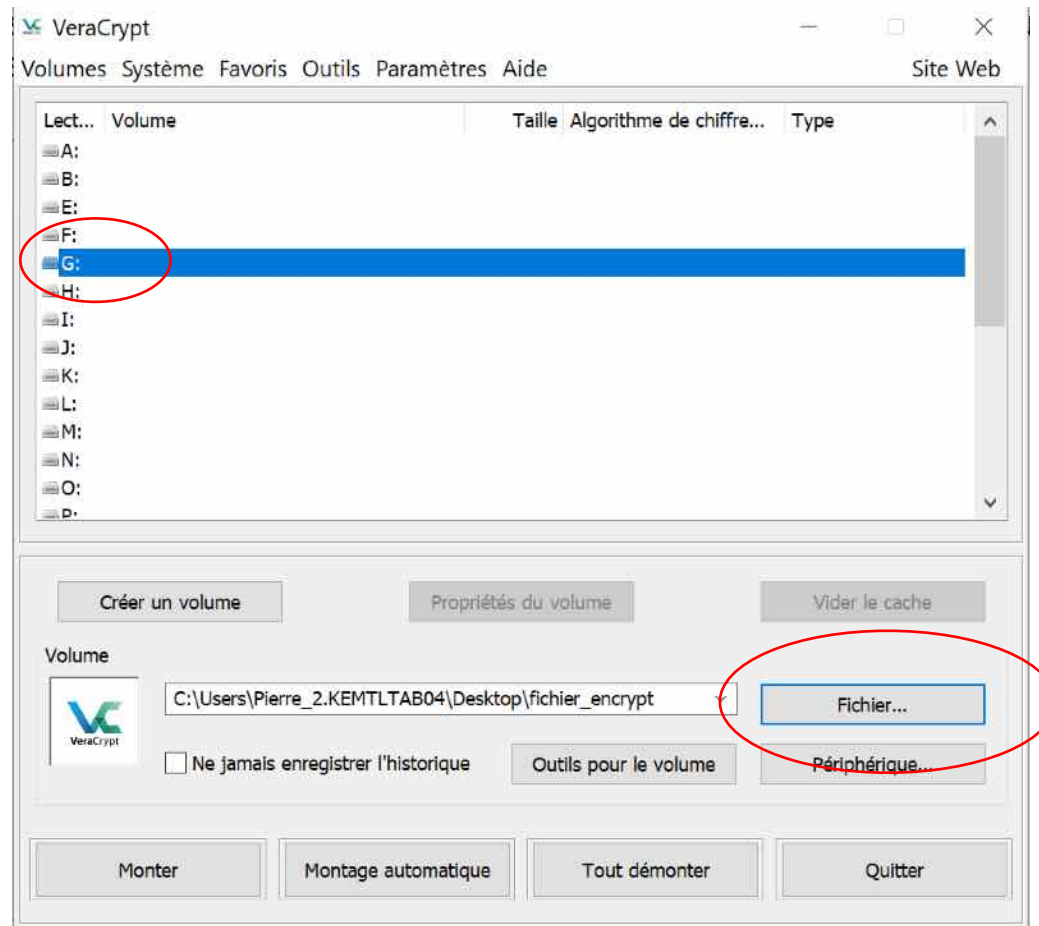
Comme le texte l'indique, déplacer la souris de manière aléatoire dans la fenêtre de gauche pour accroître la force cryptographique.

Cliquer ensuite sur formater et ensuite sur terminer.



Accéder aux données du container

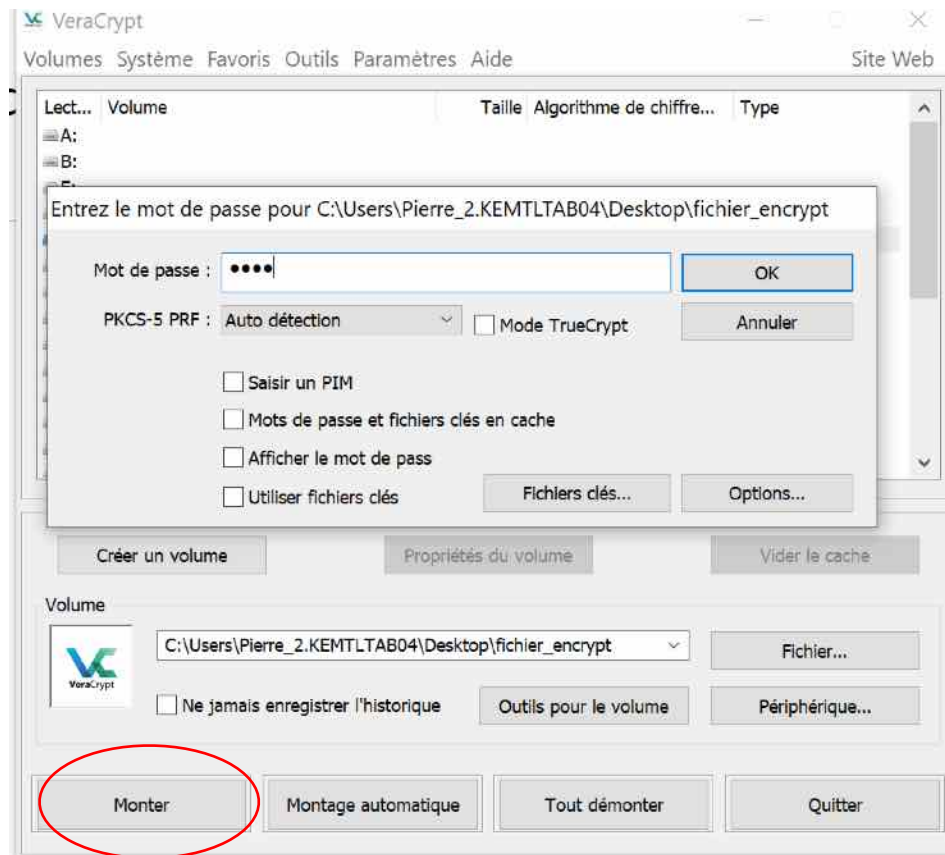
Cliquer sur l'icône VeraCrypt, choisissez une lettre, et cliquer sur fichier pour accéder au fichier du container lequel va apparaître dans la fenêtre.



Accéder aux données du container (suite)

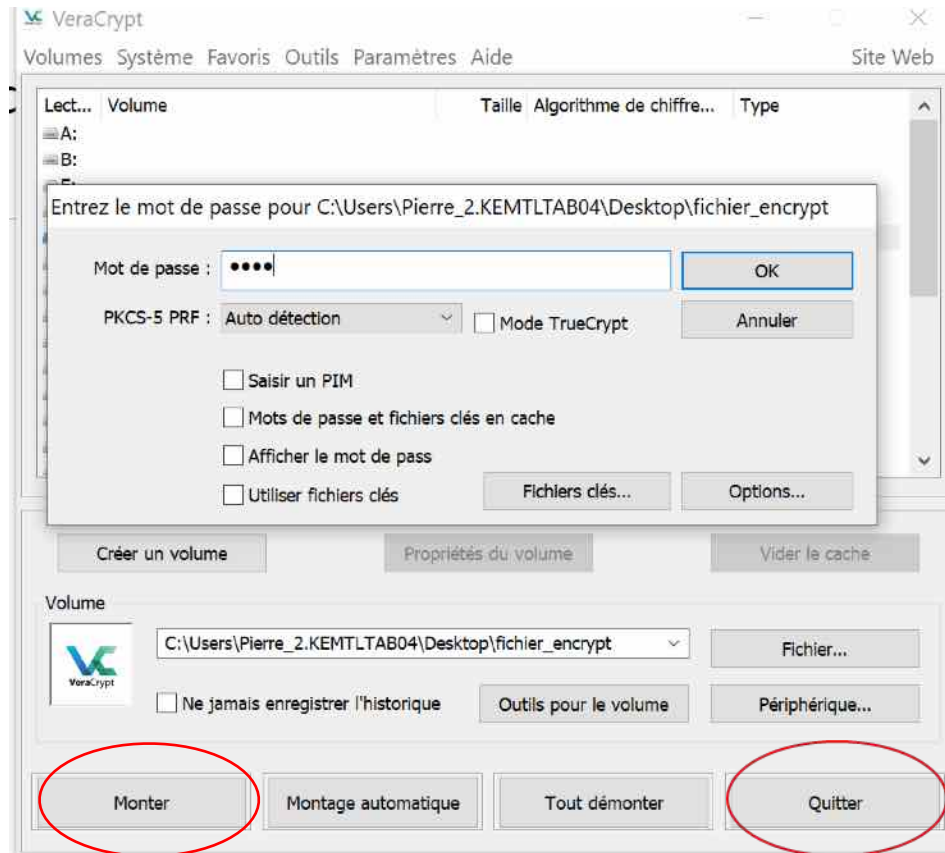


Cliquer sur 'Monter', entrer le mot de passe



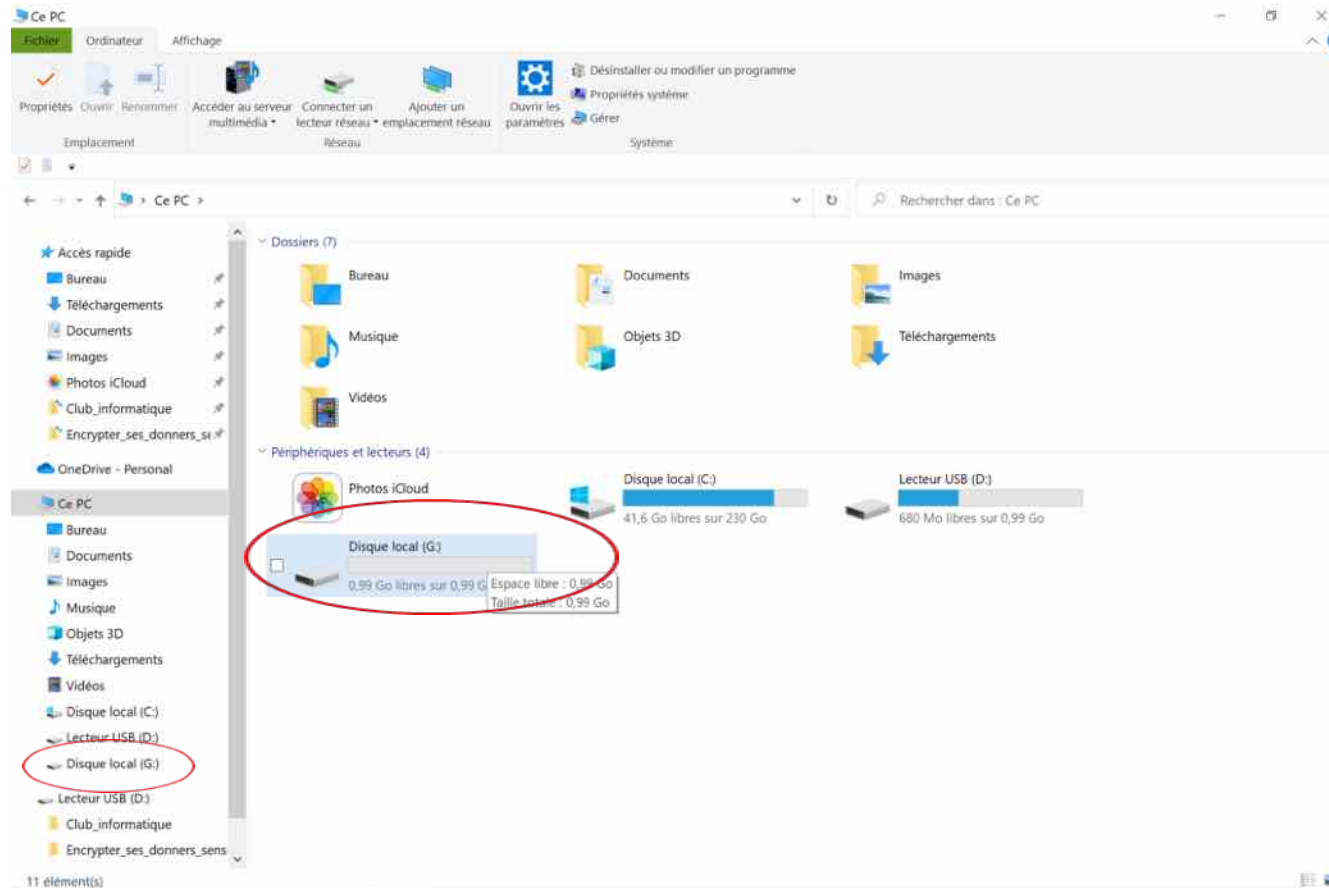
Accéder aux données du container (suite)

Cliquer sur 'Monter', entrer le mot de passe et cliquer sur 'Quitter'.
Attention: Quitter ne fait que fermer la fenêtre de VeraCrypt. Les fichiers restent accessibles.



Accéder aux données du container (suite)

Les données sont maintenant accessibles sous la lettre choisie.



Accéder aux données du container (suite)



Pour refermer le container, c'est-à-dire réencrypter les fichiers pour les rendre inaccessibles, vous devez ouvrir VeraCrypt et cliquer sur « démonter » ou « tout démonter ».

Dans le gestionnaire de fichier, assurez-vous que vous ne voyez plus la lettre que vous aviez associée au container. Cela vous confirmera que vos données sensibles ne seront plus accessibles.

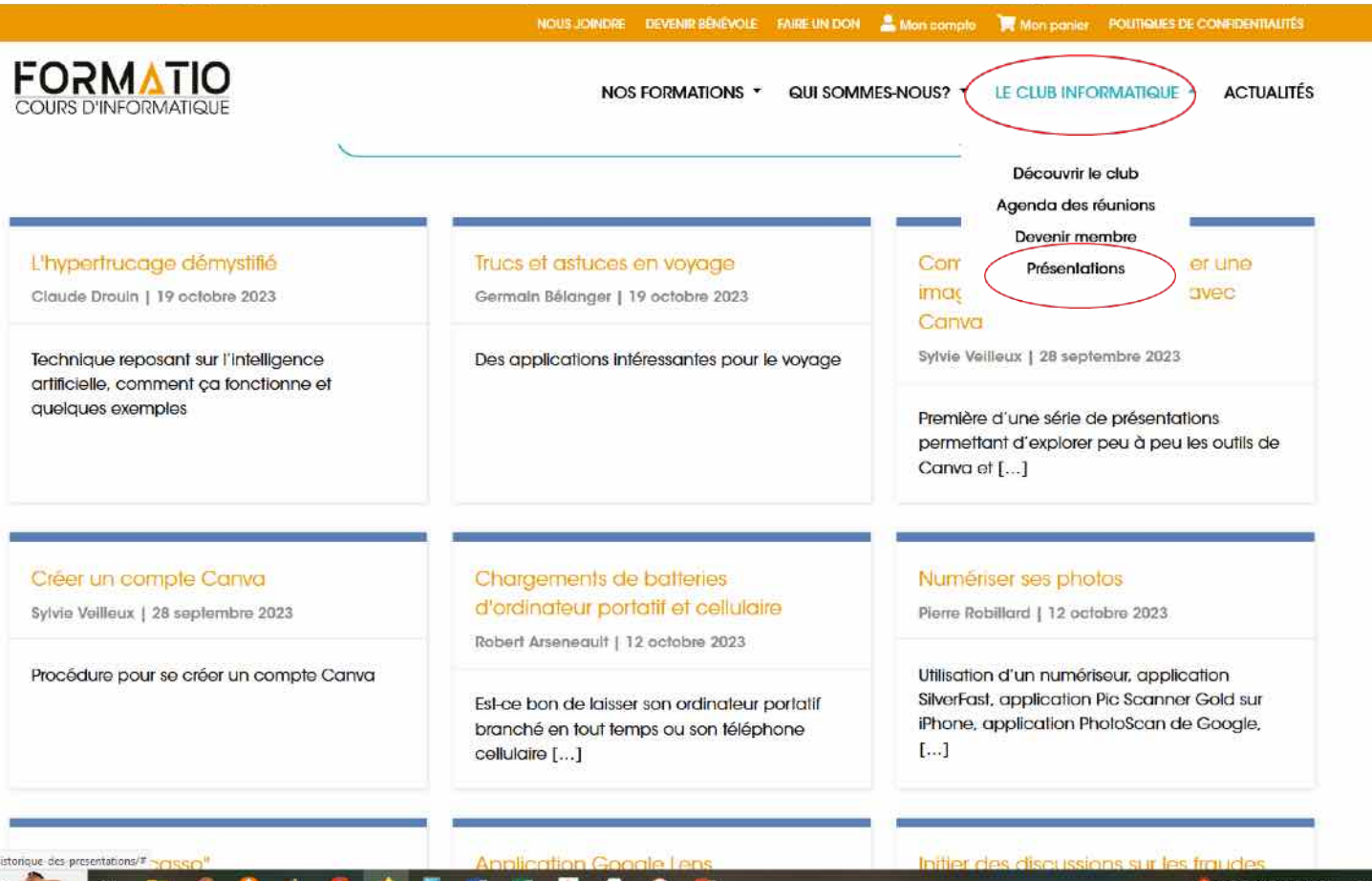
Fermer l'ordinateur ou le portable sans que vous aillez fermé le container ne cause pas de problème. Le container sera quand même refermé et son contenu inaccessible.

Le container est présent sur le disque dur de l'ordinateur sous la forme d'un fichier de la taille que vous avez choisie, qu'il soit vide ou rempli de fichiers.

Vous pouvez faire une sauvegarde en copiant le fichier du container sur une clé USB ou un autre média.

Encrypter ses données sensibles

La présentation sera disponible sur Formatio.info sous l'onglet 'Le club informatique' et 'Présentations'



The screenshot shows the Formatio website interface. At the top, there is a navigation bar with links: NOUS JOINDRE, DEVENIR BÉNÉVOLE, FAIRE UN DON, Mon compte, Mon panier, and POLITIQUES DE CONFIDENTIALITÉS. Below this is the main navigation menu with links: NOS FORMATIONS, QUI SOMMES-NOUS?, LE CLUB INFORMATIQUE (highlighted with a red circle), and ACTUALITÉS. The 'LE CLUB INFORMATIQUE' dropdown menu is open, showing options: Découvrir le club, Agenda des réunions, Devenir membre, and Présentations (highlighted with a red circle). The main content area displays a grid of articles. The first article is 'L'hypertrucage démystifié' by Claude Drouin, dated 19 octobre 2023, with a description: 'Technique reposant sur l'intelligence artificielle, comment ça fonctionne et quelques exemples'. The second article is 'Trucs et astuces en voyage' by Germain Bélanger, dated 19 octobre 2023, with a description: 'Des applications intéressantes pour le voyage'. The third article is 'Corriger une image avec Canva' by Sylvie Veilleux, dated 28 septembre 2023, with a description: 'Première d'une série de présentations permettant d'explorer peu à peu les outils de Canva et [...]'. The fourth article is 'Créer un compte Canva' by Sylvie Veilleux, dated 28 septembre 2023, with a description: 'Procédure pour se créer un compte Canva'. The fifth article is 'Chargements de batteries d'ordinateur portable et cellulaire' by Robert Arseneault, dated 12 octobre 2023, with a description: 'Est-ce bon de laisser son ordinateur portable branché en tout temps ou son téléphone cellulaire [...]'. The sixth article is 'Numériser ses photos' by Pierre Robillard, dated 12 octobre 2023, with a description: 'Utilisation d'un numériseur, application SilverFast, application Pic Scanner Gold sur iPhone, application PhotoScan de Google, [...]'. The seventh article is 'Application Google Lens' and the eighth is 'Initier des discussions sur les fraudes'.