Comment protéger vos données avec 4 actions simples

30 Octobre 2019

CLUSIR Tahiti

Agenda

Intro - Comprendre les enjeux et les menaces

1. Gérer ses mots de passe avec lastpass ou keepass
2. Chiffrer vos données avec Veracrypt
3. Mettre en place des sauvegardes avec nexcloud
4. Utiliser une messagerie instantanée sécurisée avec signal

Comprendre les enjeux et les menaces

De bonnes sauvegardes peuvent sauver votre entreprise

https://www.g-echo.fr/videos/2015-CGPME-Cloture.mp4

1) Gérer ses mots de passe

La taille c’est important

- Un simple ordinateur peut calculer 100 000 000 mots de passe à la seconde
- Un mot de passe de **8 caractères** sera deviné par un ordinateur en quelques minutes.

Un mot de passe doit faire 10 caractères minimum pour résister aux attaques par force brute.

Pour les mots de passe importants, une longueur de 12 caractères est fortement conseillé.

Mais un mot de passe long, est-ce suffisant ?

Malheureusement non. ☹

Popularity – Top 20

Password	Number of Users with Password (absolute)
123456	290731
12345	79078
123456789	76790
Password	61958
iloveyou	51622
princess	35231
rockyou	22588
1234567	21726
12345678	20553
abc123	17542

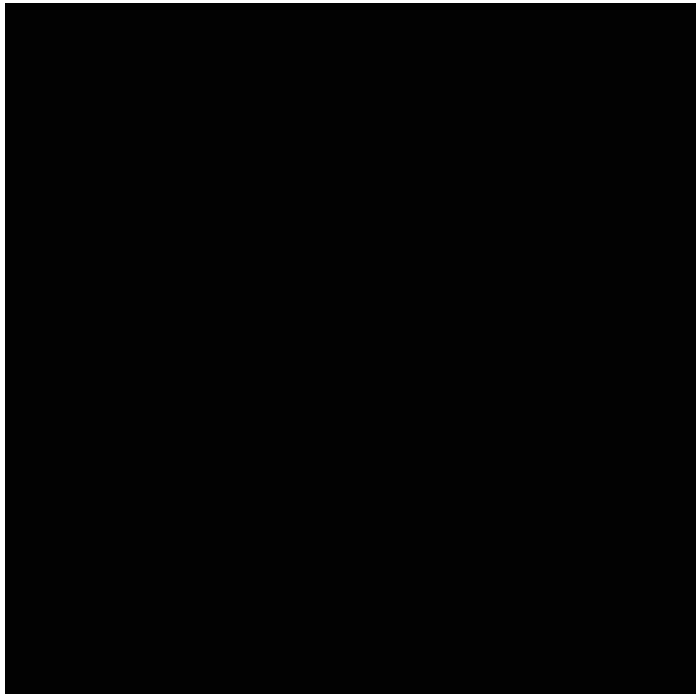
N'utilisez pas des mots de passe triviaux. Les attaquants testent en premier les mots de passe les plus utilisés à l'aide de dictionnaire. Ils sont cassés en quelques secondes.

Eviter les motifs qui affaiblissent votre mot de passe :

- Votre prénom ou celui de vos proches
- Le nom de l'application

Utiliser un mot de passe long en évitant les mots de passe et les motifs

Utilisez la méthode de la phrase



Avec la méthode de la phrase vu dans la vidéo ci dessus, vous obtenez un mot de passe long, complexe mais facile à retenir.

Un mot de passe unique pour chaque service sensible

J'ai un mot de passe long et complexe. Je l'utilise depuis des années. Suis-je à l'abri ?

Non car de très grosses bases de mots de passe circulent sur internet provenant de sites connus qui se sont faits pirater ces dernières années (Linkedin, gmail, icloud …)

Votre mot de passe associé à votre adresse mail personnelle circule probablement sur internet.

Pour vous en assurer, aller sur https://haveibeenpwned.com/ (*) et taper votre mail personnel. Vous aurez la réponse.

- **Ne surtout pas réutiliser un mot de passe** déjà utilisé pour un service personnel (ex: mon compte Gmail).
- **Définissez un mot de passe unique pour chaque service sensible** notamment pour accéder à votre messagerie personnelle ou professionnelle

D’où l’utilité d’un coffre de mot de pass

- Si vous avez **plus de 5 mots de passe** à retenir, utilisez un **coffre de mot de passe.**
- Un coffre vous permet de stocker vos mots de passe de façon sécurisé et de n'utiliser qu'un seul mot de passe maitre pour verrouiller les autres.

Particuliers / TPE

Keepass

Dashlane

Entreprise

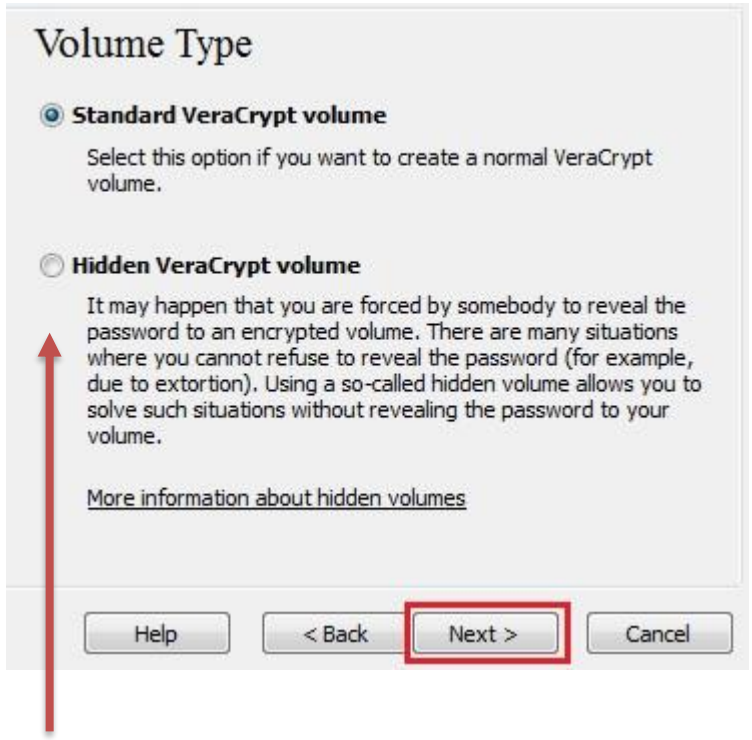
lockself

PRODUITS CERTIFIÉS CSPN

CLUSIR TAHITI

2) Chiffrer vos données avec Veracrypt

VeraCrypt



VeraCrypt est un logiciel utilitaire sous licence libre utilisé pour le chiffrement à la volée. Il est développé par la société française IDRIX et permet de créer un disque virtuel chiffré dans un fichier ou une partition. [Wikipédia]

https://www.veracrypt.fr/en/Downloads.html

2) Mettre en place des sauvegardes avec nexcloud

NextCloud

Nextcloud est un logiciel libre, de site d'hébergement de fichiers, et un fork du logiciel ownCloud. À l'origine accessible via WebDAV, n'importe quel navigateur web, ou des clients spécialisés, son architecture ouverte a permis de voir ses fonctionnalités s'étendre depuis ses origines. Wikipédia

4) Utiliser une messagerie instantanée sécurisée avec signal

lesquels choisir ?

- Premiers critères utilisateur :
  - la taille du réseau social joignable,
  - la facilité d'utilisation,
  - l'accessibilité de la solution,
  - liste des services annexes

- Qu'en est il du critère sécurité ?
  - Chiffrement des messages de bout en bout
  - qualité des algorithmes cryptographiques
  - confidentialité persistante (Perfect Forward Secrecy ou PFS)
  - limitation de l'exposition des métadonnées

CLUSIR TAHITI

lesquels choisir ?

- Chiffrement bout en bout ?

Slack

wechat

Signal

WhatsApp

Telegram

lesquels choisir ?

- qualité des algorithmes cryptographiques ?

code source
est librement
consultable

Signal

WhatsApp

Telegram

?

?

Code n’est pas libre

lesquels choisir ?

- Confidentialité persistante (Perfect Forward Secrecy ou PFS)

Signal

WhatsApp

La confidentialité persistante, est une propriété en cryptographie qui garantit que la découverte par un adversaire de la clé privée d'un correspondant ne compromet pas **la confidentialité des communications passées**. Wikipédia

lesquels choisir ?

- limitation de l'exposition des métadonnées

développée
depuis 2014 par
une organisation à
but non lucratif

Signal

WhatsApp

Edward Snowden il like

?

- La collecte de données c'est le business model de facebook.
- Brian Acton, le cofondateur de WhatsApp. Il a démissionné de la start-up en 2017. Il fait désormais partie de l'équipe de développement de Signal

Signal, une application qui ne nécessite pas la création de compte

- Installer signal
- Utiliser signal pour les communications sensibles

Signal

Merci

www.clusir-tahiti.org

CLUSIR TAHITI