Sécurisation des Fichiers & Données

Formation pour journalistes et professionnels des médias

Jour 3 - Protection de vos informations sensibles

Agenda du jour

01

Chiffrement de fichiers

Protéger vos preuves sensibles

02

Partage sécurisé

Transmettre sans laisser de traces

03

Suppression sécurisée

Effacer définitivement vos données

04

Sauvegardes chiffrées

Préserver sans compromettre

05

Cas pratique

Gérer une fuite de documents

Rappel : La communication sécurisée

Principes clés abordés hier :

1. Chiffrement de bout en bout
2. Métadonnées et leur importance
3. Applications recommandées

Questions sur ces éléments avant de continuer ?

Chiffrement de fichiers

Pourquoi chiffrer vos documents sensibles ?

Protection contre les saisies

Matériel confisqué mais données inaccessibles

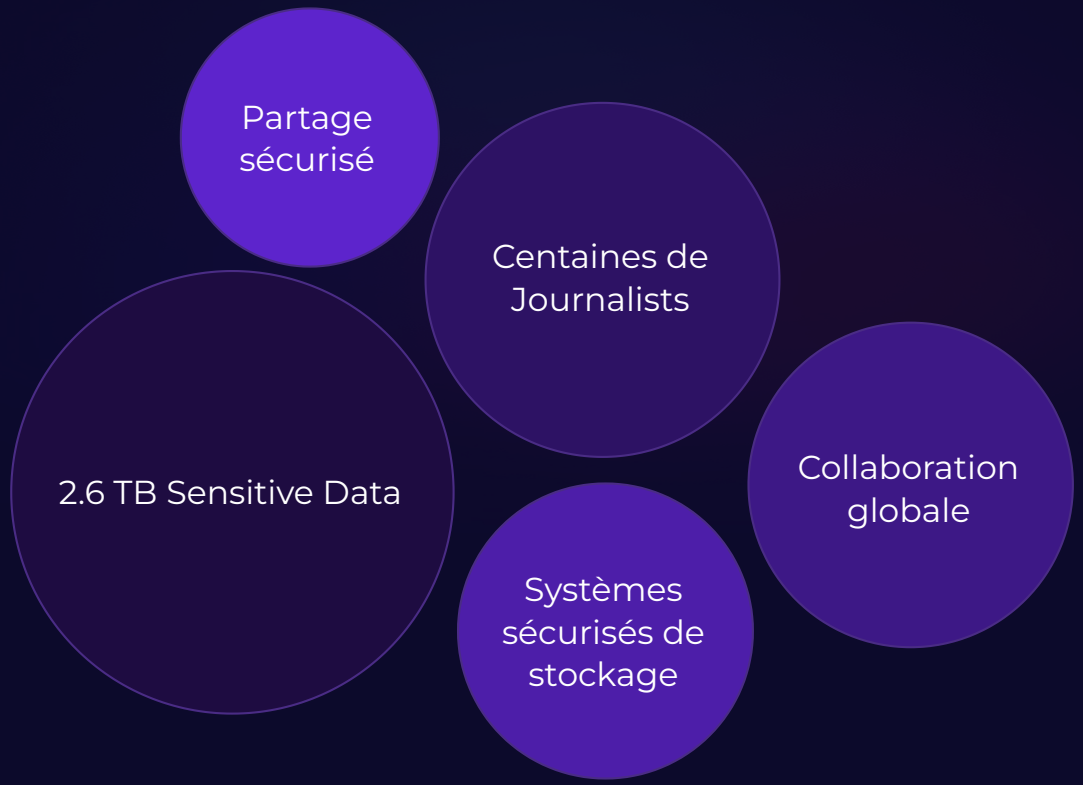
Confidentialité des sources

Documents protégés même en cas de vol

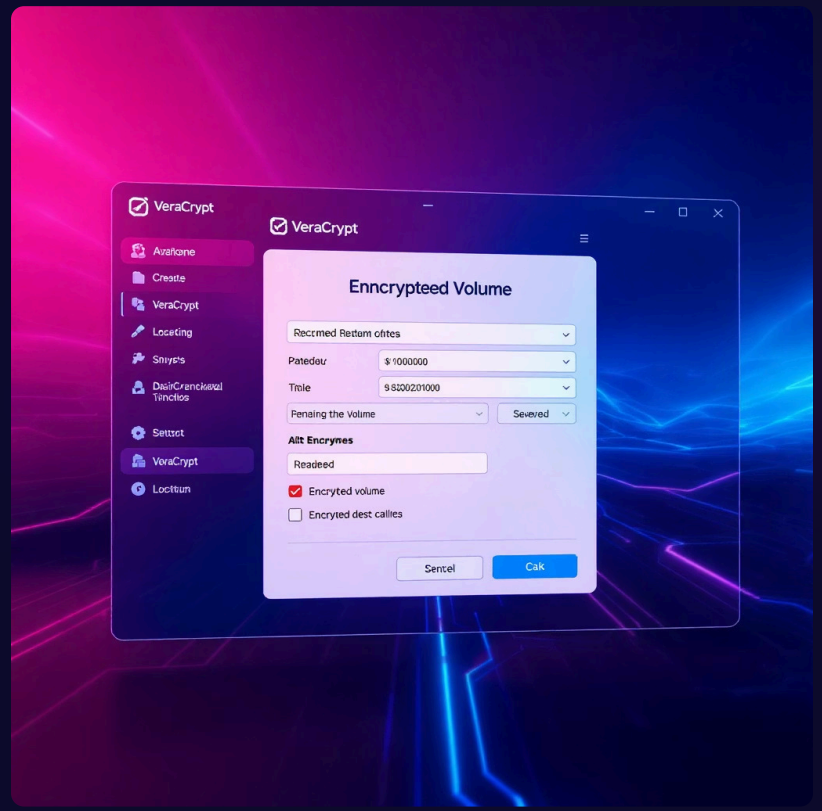
Obligation éthique

Devoir de protection envers vos informateurs

Cas concret : Panama Papers



VeraCrypt : Votre coffre-fort numérique



End-to-end Encryption

Metadata Awareness

Practical Applications

Secure Storage

Exercice pratique : VeraCrypt

Installer VeraCrypt

Vérifier signature du téléchargement

Créer un volume chiffré

Taille de 500 Mo minimum

Choisir un mot de passe fort

Phrase complexe, mémorisable

Placer des documents tests

Tester le verrouillage/déverrouillage

Partage sécurisé de fichiers

Comment transmettre sans traces ?

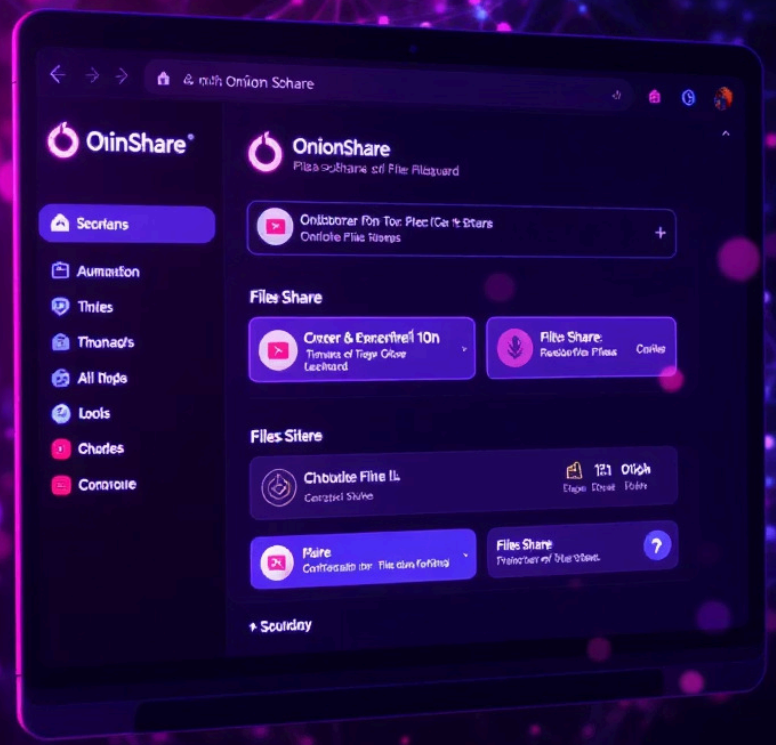
Le partage traditionnel laisse des traces numériques

Les gros fichiers exigent des solutions spécifiques

Cas concret : Documentation de violations

ONG documentant des exactions

- Vidéos haute définition
- Témoignages sensibles
- Besoin d'anonymat total



OnionShare : Partage anonyme

Fonctionne via Tor

Masque votre identité et localisation

Serveur temporaire

Pas d'intermédiaire, connexion directe

URL à usage unique

Disparaît après téléchargement

Exercice : Transmission via OnionShare

15 minutes

1. Installer OnionShare et Tor Browser
2. Partager un dossier avec un collègue
3. Vérifier la réception et l'intégrité

Alternative : Proton Drive pour envois moins sensibles mais chiffrés

Suppression sécurisée

Problème

La suppression standard ne détruit pas vraiment les données

Risque

Les fichiers "supprimés" peuvent être récupérés

Solution

Outils d'effacement sécurisé qui écrasent les données

Cas concret : Journaliste en danger

Égypte, 2019 : Journaliste arrêté avec son ordinateur

Certains collègues avaient effacé leurs données à temps

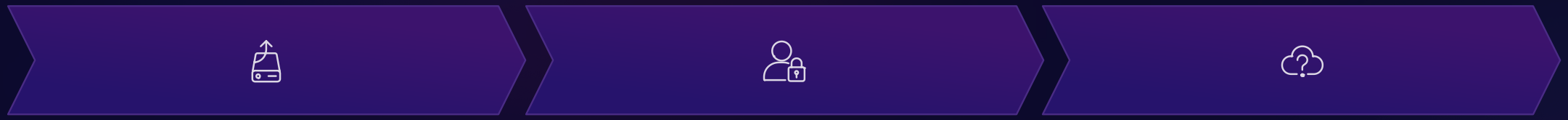
D'autres ont vu leurs sources exposées

BleachBit : Nettoyage en profondeur

- Supprime définitivement les fichiers
- Nettoie les traces d'utilisation
- Efface l'espace disque non utilisé
- Options de suppression DoD ou Gutmann

Sauvegardes chiffrées

Préserver sans compromettre



Risques matériels

Vol, panne, saisie, destruction

Protection des données

Chiffrement obligatoire

Redondance

Local + distant

Stratégie de sauvegarde 3-2-1

3 copies

Original + 2 sauvegardes

2 types

Supports différents

1 hors-site

Géographiquement distant

Solutions recommandées

Stockage local

- Disque USB chiffré avec VeraCrypt
- Cryptomator pour chiffrer dossiers

Cloud sécurisé

- Proton Drive (Suisse)
- Tresorit (chiffrement E2E)
- NextCloud (auto-hébergeable)

⚠ Évitez les solutions grand public non chiffrées (Dropbox, Google Drive standard)

Cas pratique : Gestion d'une fuite

Scénario

Les emails de votre rédaction ont été compromis

Documents sensibles potentiellement exposés

Exercice en groupe : Plan d'action

Changement des accès

Mots de passe, 2FA, révocation de clés

Protection des sources

Identification et notification des personnes à risque

Sécurisation des documents

Chiffrement d'urgence, déplacement vers stockage sûr

Documentation

Rapport d'incident et leçons apprises

Votre workflow de sécurité documentaire

Création

Environnement sécurisé

Stockage

Volumes chiffrés

Partage

Canaux sécurisés

Suppression

Effacement sécurisé

Sauvegarde

Stratégie 3-2-1