



FICHE PRATIQUE : SÉCURITÉ & SÛRETÉ DES DONNÉES EN 5 ÉTAPES

1. CARTOGRAPHIE



Connaitre la nature et l'emplacement des données que l'on possède



- Explorer les dossiers : Documents, Images, Téléchargements.
- Identifier les Clouds actifs : OneDrive, Google Drive, Dropbox, iCloud..
- Tri des fichiers sensibles :
 - Niveau 1 & 2 (Faible à Modéré)
 - Niveau 3 & 4 (Élevé à Critique)



- Galerie : Purger photos de cartes bancaires, documents d'identité, ordonnances...
- Téléchargements : Documents administratifs
- Apps : Supprimer si inutilisées > 3 mois



WindirStat : visualiser et rechercher fichiers et dossiers sur PC
<https://windirstat.net/download.html>

2. SÉCURITÉ



Empêcher le piratage, l'intrusion et le vol d'identifiants d'accès



- Session : Ajouter MDP / PIN
- Comptes online : MDP fort
- Activer 2FA là où c'est possible



- Activer PIN fort : 6 chiffres (éviter 000000, 123456, 999999, dates)
- Biométrie : Activer Touch ID/Face ID ou empreinte digitale
- Affichage : Masquer les SMS de validation (2FA)



Bitwarden : Génération et stockage de mots de passe forts sur Internet
<https://vault.bitwarden.eu/#/login>

KeePassXC : Génération et stockage de mots de passe forts sur PC et Smartphone

<https://keepassxc.org/download/#windows>

2FA = Authentification à 2 facteurs
MDP = Mot de passe

3. SÛRETÉ



Récupérer les données en cas de panne, vol, casse ou incendie

Règle 3-2-1 :

- 3 copies : Données Niv. 3 & 4
- 2 supports : PC + Clé USB / Disque externe
- 1 Cloud : Ex: Google Drive, iCloud... fichiers chiffrés uniquement)

Routine & support de stockage :

- 1x / mois : Copie externe puis stockage à l'abri du support choisi
- Cloud : Privilégier RGPD (UE/Suisse)



FreeFileSync : copie/synchronisation de données entre supports de stockage
<https://freefilesync.org/download.php>

Veracrypt : création/utilisation de supports de stockage chiffrés
<https://veracrypt.io/en/Downloads.html>

Cryptomator : création/utilisation d'espaces de stockage Cloud chiffrés
<https://cryptomator.org/downloads/#win>

LocalSend : échange de données entre PC et Smartphone
<https://localsend.org/fr/download>

4. SYNCHRONISATION



Éviter la dispersion de fichiers privés sur des serveurs étrangers



- OneDrive : Désactiver l'auto-sync Bureau / Documents / Images
- Google Drive / iCloud : Décocher les dossiers locaux synchro.



- Photos : Synchro en Wi-Fi uniquement
- Carte d'identité / Passeport : Chiffrer les scans en archive ZIP avec MDP (via 7-Zip)

5. HYGIÈNE NUMÉRIQUE



Acquérir et entretenir les bons comportements pour minimiser les risques numériques

Réflexes quotidiens

- Phishing/Smishing (Email/SMS suspects)
 - Règle des 10 min : ne jamais cliquer dans l'urgence. Attendre 10 minutes, vérifier l'adresse de l'expéditeur ou contacter directement l'expéditeur par un canal officiel différent.
- Wi-Fi Public : Ne jamais consulter son compte bancaire ni effectuer de paiement sur un réseau Wi-Fi public ouvert. Utiliser la connexion 4G/5G du smartphone
- Applications : Télécharger uniquement depuis Google Play ou Apple Store. Sur PC, télécharger les logiciels uniquement depuis les plateformes officielles des éditeurs

D'autres conseils sont également disponibles sur le site de la Chouette Savante : <https://lcslab.ch/conseils>