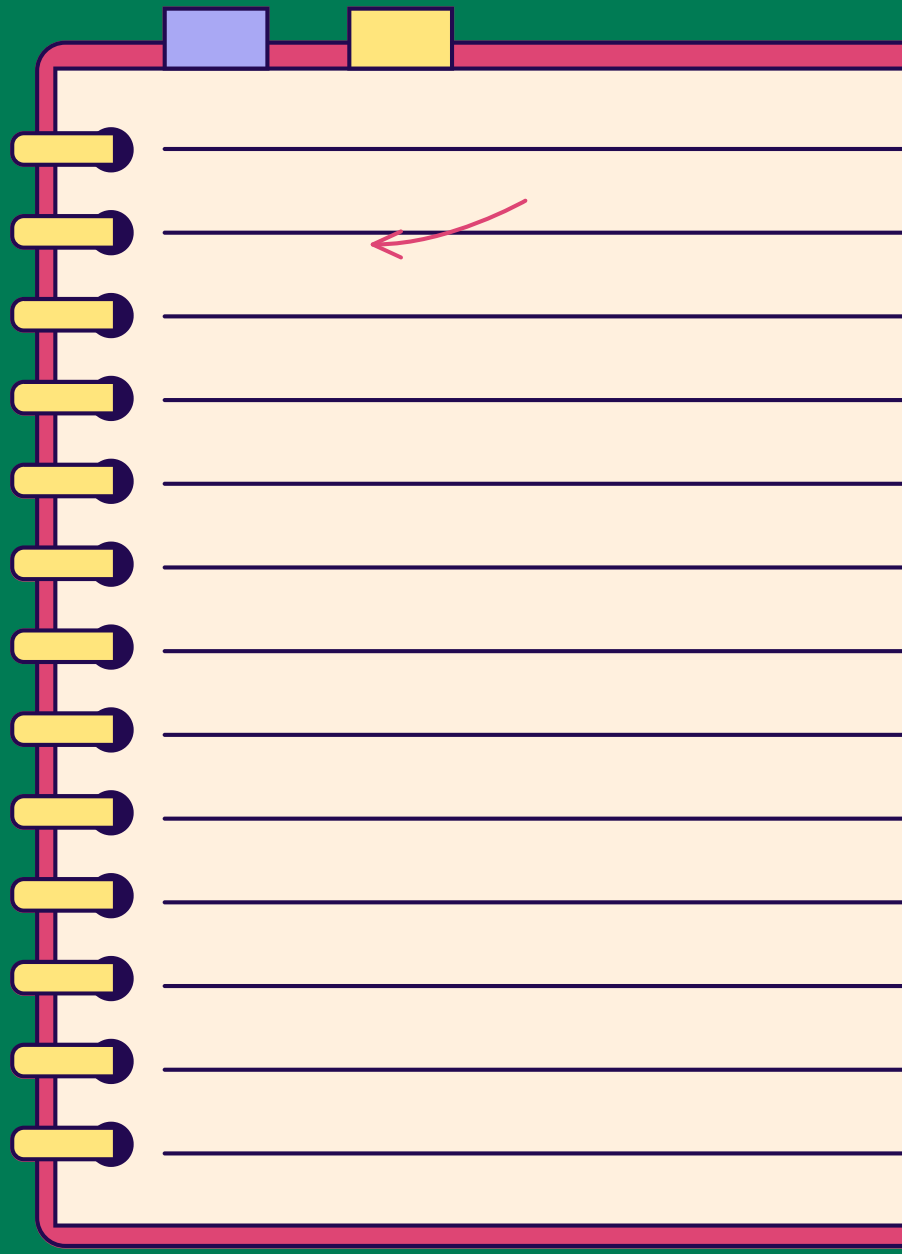
MODULE 5 - GÉRER, STOCKER ET RETROUVER SES DONNÉES

CHAPITRE 1

STOCKER SES DONNÉES

Skills to Connect



INTRODUCTION

Dans un monde numérique en constante évolution, la gestion efficace des données est devenue une nécessité cruciale, tant pour les individus que pour les entreprises.

Ce chapitre du Module 5 s'attaque à la problématique fondamentale du stockage, de la sécurisation et de la récupération des données personnelles et professionnelles.

Nous explorerons les diverses méthodes et technologies disponibles pour stocker les données de manière sûre et facilement accessible, telles que le cloud et les disques durs.

Ce guide vous fournira les connaissances nécessaires pour choisir la meilleure solution de stockage en fonction de vos besoins spécifiques, tout en garantissant que vos informations restent protégées et sous votre contrôle complet.

1 STOCKER SES DONNÉES

OÙ ET COMMENT SAUVEGARDER SES DONNÉES

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).

Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1[@]email.fr ») ne sont pas, en principe, des données personnelles.
Source : CNIL, https://www.cnil.fr/fr/definition/donnee-personnelle

1 STOCKER SES DONNÉES

OÙ ET COMMENT SAUVEGARDER SES DONNÉES

SUR UN CLOUD

Le cloud est un espace de stockage en ligne. Tu sauvegardes tes fichiers sur des serveurs distants accessibles via Internet.

AVANTAGES :

- Accessible depuis n'importe où avec une connexion Internet.
- Souvent sécurisé avec des sauvegardes automatiques.
- Peu encombrant (pas besoin de matériel physique).

INCONVÉNIENTS :

- Nécessite une connexion Internet pour accéder à tes données.
- Peut avoir un coût (abonnement mensuel ou annuel).

Exemples de services cloud : Google Drive, Dropbox, OneDrive, ICloud, ...

SUR UN DISQUE DUR (EXTERNE OU INTERNE)

Un disque dur est un dispositif de stockage physique que tu connectes à ton ordinateur.

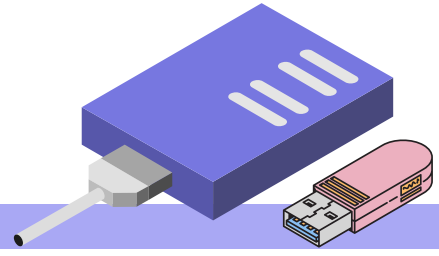
AVANTAGES :

- Accès rapide sans besoin de connexion Internet.
- Tu as un contrôle total sur tes données.
- Peut stocker de grandes quantités de données.

INCONVÉNIENTS :

- Risque de perte ou de dommage physique (chute, incendie, etc.).
- Moins pratique pour accéder à distance.

Exemples de disques durs : Disque dur externe USB, SSD (Solid State Drive).



1 STOCKER SES DONNÉES

OÙ ET COMMENT SAUVEGARDER SES DONNÉES

QUE CHOISIR ? CLOUD OU DISQUE DUR ?

TUTORIEL VIDÉO

Découvrez les comment stocker & sauvegarder vos données avec un Cloud ou un disque dur.

2 STOCKER SES DONNÉES

COMMENT SÉCURISER SES DONNÉES ?

Sécuriser ses données numériques est essentiel pour protéger sa vie privée, éviter les vols d'identité, et prévenir l'accès non autorisé à des informations personnelles ou sensibles. Cela réduit aussi les risques de pertes financières ou d'exploitation malveillante de vos données. Voici quelques mesures simples à mettre en place pour sécuriser vos données :

1 - UTILISER DES MOTS DE PASSE FORTS :

ALERTE MODULE

Pour en savoir plus, rendez-vous dans le module 1 qui vous explique comment bien choisir un mot de passe !

- Choisissez des mots de passe complexes (lettres, chiffres, symboles) et uniques pour chaque compte.
- Utilisez un gestionnaire de mots de passe pour vous aider à les gérer.

Un gestionnaire de mots de passe est un outil essentiel pour maintenir la sécurité et l'organisation des mots de passe, surtout quand on suit la recommandation de créer des mots de passe complexes et uniques pour chaque compte. Voici les deux aspects clés de ce que fait un gestionnaire de mots de passe :

STOCKAGE SÉCURISÉ :

Les gestionnaires de mots de passe permettent de stocker tous vos mots de passe dans un emplacement centralisé qui est sécurisé par un mot de passe maître. Ce dernier est le seul mot de passe que vous devez retenir. Les données stockées sont souvent chiffrées, ce qui signifie qu'elles ne peuvent pas être lues sans le mot de passe maître.

2 STOCKER SES DONNÉES

COMMENT SÉCURISER SES DONNÉES ?

GÉNÉRATION ET RÉCUPÉRATION DE MOTS DE PASSE :

Un gestionnaire de mots de passe peut également générer des mots de passe aléatoires et complexes pour vous, qui utilisent une combinaison de lettres, de chiffres, et de symboles, conformément aux meilleures pratiques de sécurité. Lorsque vous devez accéder à un compte, le gestionnaire peut automatiquement remplir le mot de passe pour vous, ce qui élimine le besoin de le mémoriser ou de le saisir manuellement.

2 - CHIFFRER VOS DONNÉES :

- Le chiffrement transforme vos données en un format illisible sans une clé de déchiffrement. De nombreux services cloud offrent cette option.
- Sur un disque dur, vous pouvez utiliser des logiciels comme VeraCrypt pour chiffrer vos fichiers.

2 STOCKER SES DONNÉES

COMMENT SÉCURISER SES DONNÉES ?

C’EST QUOI LE PROCESSUS DE CHIFFREMENT DES DONNÉES ?

Le chiffrement des données, c’est un peu comme mettre vos informations dans un coffre-fort sécurisé.
Ce processus consiste à transformer les données en un format illisible, appelé « texte chiffré », pour que seules les personnes ayant la bonne clé puissent les lire.

COMMENT ÇA MARCHE ?

Le chiffrement utilise une clé, un peu comme un mot de passe très complexe, pour « coder » les données. Sans cette clé, personne ne peut comprendre le contenu.

Voici comment ça se passe en pratique :

- Transformation des données : Quand on chiffre des données, on applique un algorithme (une sorte de formule mathématique) qui mélange et transforme les informations d’origine en une suite de caractères incompréhensibles.
- Utilisation d'une clé : Ce « mélange » est guidé par une clé de chiffrement unique. Cette clé est comme une clé de coffre-fort : elle est nécessaire pour pouvoir déchiffrer (ou lire) les données chiffrées.

2 STOCKER SES DONNÉES

COMMENT SÉCURISER SES DONNÉES ?

POURQUOI EST-CE UTILE ?

Le chiffrement protège vos informations sensibles contre les accès non autorisés. Même si quelqu'un interceptait vos données, il ne pourrait rien en faire sans la clé.

COMMENT FAIRE DU CHIFFREMENT DES DONNÉES EN PRATIQUE ?

Sur votre ordinateur ou dans le cloud, vous pouvez utiliser des logiciels comme VeraCrypt pour chiffrer vos fichiers. Dans les services cloud, certaines options de chiffrement sont intégrées, mais vous pouvez aussi créer vos propres mots de passe ou clés pour renforcer la sécurité.

Pour illustrer concrètement le chiffrement, voici un exemple de chiffrement simple, appelé **le chiffrement de César.** C'est un type de chiffrement de substitution parfait pour comprendre le concept.

2 STOCKER SES DONNÉES

COMMENT SÉCURISER SES DONNÉES ?

CHIFFREMENT DE CÉSAR

Supposons que vous voulez chiffrer le mot "CHAT" en utilisant un décalage de 3.

- Étape 1 : Définir la clé
- Dans cet exemple, la clé est "décalage de 3". Cela signifie que chaque lettre va être remplacée par la lettre qui est 3 positions plus loin dans l'alphabet.
- Étape 2 : Appliquer le décalage
- On applique le décalage de 3 à chaque lettre du mot "CHAT" :
  - C devient F
  - H devient K
  - A devient D
  - T devient W
- Ainsi, "CHAT" devient "FKDW" après le chiffrement.
- Étape 3 : Déchiffrer avec la clé
- Pour retrouver le mot original, il suffit de décaler chaque lettre de 3 positions dans l'autre sens :
  - F redevient C
  - K redevient H
  - D redevient A
  - W redevient T

En déchiffrant, on retrouve bien "CHAT".

2 STOCKER SES DONNÉES

COMMENT SÉCURISER SES DONNÉES ?

3 - FAIRE DES SAUVEGARDES RÉGULIÈRES :

- Ne gardez pas toutes vos données au même endroit. Fais des copies sur un disque dur et dans le cloud pour minimiser les risques de perte.
- Programmez des sauvegardes automatiques si possible.

4 - METTRE À JOUR VOS LOGICIELS :

- Gardez votre système d'exploitation et vos logiciels à jour pour bénéficier des dernières protections de sécurité.

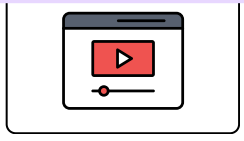
ALERTE MODULE

Pour en savoir plus, rendez-vous dans le module 1 qui vous explique comment mettre à jour vos appareils + installer un anti virus

5 - UTILISER UN ANTIVIRUS :

- Installez et maintenez à jour un logiciel antivirus pour vous protéger contre les malwares et autres menaces

TUTORIEL VIDÉO



Découvrez comment mieux sécuriser vos fichiers sur le Cloud

A RETENIR !

Pour bien gérer vos données :

- Stockez-les sur le cloud pour l'accès à distance et la sécurité.
- Utilisez un disque dur pour les sauvegardes locales.
- Sécurisez vos données avec des mots de passe forts, le chiffrement, et des logiciels à jour.
- Faites des sauvegardes régulières pour éviter les pertes.