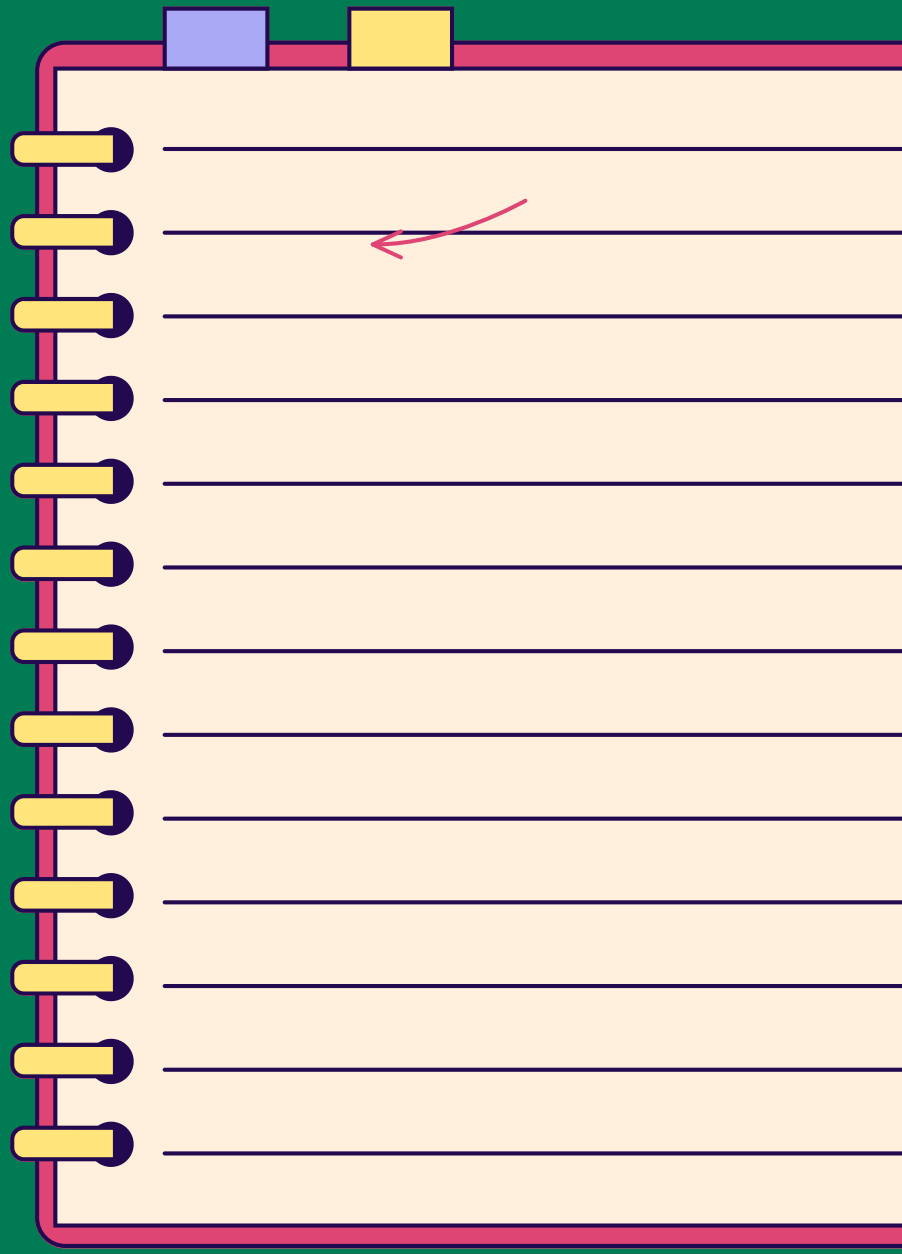
MODULE 1 - CHOISIR SON APPAREIL ET LE PROTEGER

CHAPITRE 3

PROTÉGER SES APPAREILS NUMÉRIQUEMENT

Skills to Connect



INTRODUCTION

Protéger ses appareils numériquement, c'est s'assurer de conserver ses données et d'éviter tout vol ou "hacking" de ses informations. Depuis l'explosion du numérique et des appareils, les pirates digitaux développent sans cesse de nouvelles stratégies pour obtenir nos données, ou même les "kidnapper" avec une rançon.

Il est donc essentiel de protéger ses appareils pour se prémunir des désagréments par la suite.

Dans ce chapitre, nous allons aborder différentes thématiques : les antivirus, les codes et autres systèmes pour verrouiller ses informations et éviter que n'importe qui y ait accès, l'importance des mises à jour et de vérifier si l'on fait confiance aux sites avec lesquels nous partageons nos informations.

C'est parti !

1 L'ANTIVIRUS

TOUT SAVOIR SUR LES ANTIVIRUS !

QU'EST-CE QU'UN ANTIVIRUS ?

- Un antivirus est un programme conçu pour détecter, neutraliser ou éradiquer les logiciels malveillants (virus, chevaux de Troie, rançongiciels, logiciels espions, etc.) des appareils informatiques.
- Il joue également un rôle préventif en empêchant les infections et en permettant des analyses régulières de votre ordinateur pour repérer les fichiers suspects. Un système sans antivirus est comme une maison avec une porte ouverte : il attire les intrus indésirables.
- L'antivirus agit comme un garde de sécurité, protégeant votre système contre les attaques.

POURQUOI UN ANTIVIRUS EST-IL NÉCESSAIRE ?

- En 2019, l'un des fournisseurs d'antivirus a indiqué avoir détecté 2,6 millions de menaces, c'est énorme ! Sécuriser son appareil est essentiel. En effet, tout appareil connecté à internet est potentiellement à la merci d'attaques et de la cybercriminalité. Mais cela ne s'arrête pas là. Un appareil peut aussi être infecté via une clé USB ou un disque dur externe, eux-mêmes infectés via un autre appareil. Vous pouvez donc infecter les autres ou être infecté par les autres.
- Les impacts possibles incluent :
  - Perturbation et ralentissement de l'ordinateur.
  - Blocage, suppression ou cryptage de fichiers en échange d'un paiement (rançongiciels).
  - Vol de données personnelles (coordonnées bancaire, travail réalisé).
  - Prise de contrôle à distance de l'ordinateur.
  - Phishing pour capturer des données de connexion ou de paiement.
  - Utilisation de la puissance de calcul de l'ordinateur à des fins malveillantes.

1 L'ANTIVIRUS

TOUT SAVOIR SUR LES ANTIVIRUS !

COMMENT L'ANTIVIRUS FONCTIONNE-T-IL ?

- Les antivirus utilisent trois méthodes principales de détection :
  - Détection spécifique : il compare les fichiers présents sur l'ordinateur avec des bases de données de logiciels malveillants connus pour les détecter.
  - Détection générique : recherche les variantes de virus connus.
  - Détection heuristique : identifie les virus inconnus en analysant le comportement des programmes.

COMMENT CHOISIR LE BON ANTIVIRUS ?

Caractéristiques importantes :

- **Protection globale :** Évaluez d'abord la protection générale avant de regarder les fonctionnalités supplémentaires.
- **Résultats des tests :** Vérifiez les performances spécifiques, notamment pour le phishing.
- **Fonctionnalités supplémentaires :** Certains antivirus incluent des outils comme des gestionnaires de mots de passe ou des VPN.
- **Un seul antivirus :** Installer plusieurs antivirus est contre-productif ; ils risquent de se bloquer mutuellement.

1 L'ANTIVIRUS

TOUT SAVOIR SUR LES ANTIVIRUS !

COMMENT COMPARER DIFFÉRENTS ANTIVIRUS ?

- Utilisez un comparateur d'antivirus (comme Test Achat en Belgique par exemple)
- Le système d'exploitation joue également un rôle. Les résultats des tests d'antivirus ne sont pas toujours exactement les mêmes pour une version Windows ou une version macOS (Apple) ;
- Pour les produits payants, cherchez les promotions en cours, en fonction du nombre d'appareils que vous souhaitez protéger ;
- Les produits gratuits intègrent de la publicité, plus ou moins encombrante.

Configuration requise

- Vérifiez la configuration minimale requise pour éviter de ralentir votre appareil.

Marques populaires

- Avast, AVG, Avira, Bitdefender, ESET, F-Secure, G Data, Kaspersky, McAfee, Microsoft, Norton, Panda Security, Sophos, Trend Micro.
- Certains proposent des versions gratuites avec publicité ; les versions payantes offrent un support client et moins de publicité.

Conseils d'achats

- Cherchez les promotions pour les produits payants.
- Décocher le renouvellement automatique si vous ne le souhaitez pas.
- Tester une version gratuite avant de s'engager financièrement, afin de voir si la prise en main se fait facilement et si vous le trouvez facile d'utilisation. Cela vous permet de faire un premier scan et une analyse de votre ordinateur.

1 L'ANTIVIRUS

TOUT SAVOIR SUR LES ANTIVIRUS !

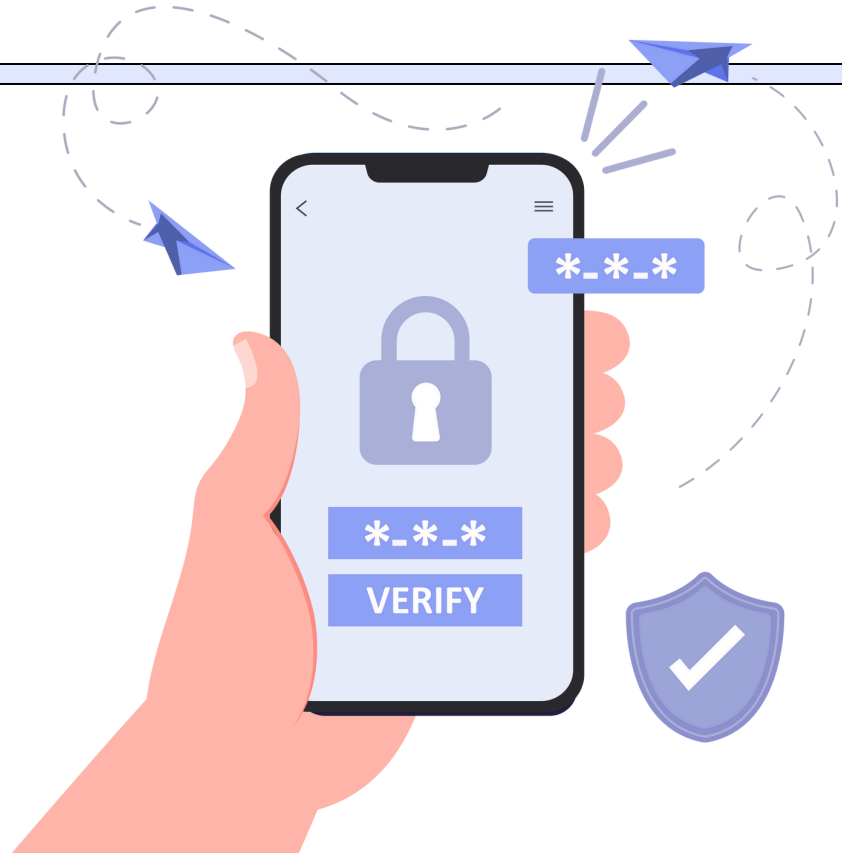
BONNES PRATIQUES D'UTILISATION DE L'ANTIVIRUS

- **Analyser les supports amovibles** : Scannez les clés USB et les disques durs externes pour éviter la contamination.
- **Mettre en quarantaine les fichiers suspects :** Évitez de les supprimer immédiatement, en les plaçant en quarantaine, vous pouvez vérifier leur nature avant de prendre une décision.
- **Faire des mises à jour régulières :** Assurez-vous que l'antivirus est à jour avant chaque scan. Activez les mises à jour automatiques si possible.
- **Faire des scans réguliers :** Programmez des scans réguliers de votre système pour détecter les menaces à temps.
- **Couper la connexion Internet en cas d'infection :** Cela empêche les logiciels malveillants de communiquer des données à distance.
- **Utiliser des mots de passe forts :** Changez régulièrement vos mots de passe et utilisez des mots de passe complexes.
- **Éviter les liens suspects :** Ne cliquez pas sur les liens douteux dans les emails ou les sites web non sécurisés.

2 DES APPLICATIONS SÉCURISÉES

POURQUOI LA SÉCURITÉ DES APPLICATIONS EST-ELLE IMPORTANTE ?

Quand vous téléchargez des applications sur votre téléphone, vous pouvez exposer vos informations personnelles sans le savoir. Certaines applications peuvent même contenir des logiciels malveillants qui volent vos données ou endommagent votre appareil.
Voici quelques conseils simples pour vous protéger.



2 DES APPLICATIONS SÉCURISÉES

CONSEILS DE SÉCURITÉ SUR LE TÉLECHARGEMENT D'APPLICATIONS

1. TÉLÉCHARGEZ SEULEMENT DEPUIS LES SOURCES OFFICIELLES

- Utilisez les magasins d'applications officiels comme Google Play Store pour Android ou l'App Store pour iPhone.
- Évitez les sites et les magasins d'applications inconnus qui peuvent proposer des applications non vérifiées.
- Ne téléchargez pas d'application en cliquant sur des liens dans des emails ou des SMS non sollicités.
- Évitez les sites web douteux qui proposent des applications gratuites ou piratées.
- Exemple : Si vous recevez un lien par SMS pour télécharger une nouvelle application de santé, vérifiez d'abord sa légitimité.

2. FAITES ATTENTION AUX PERMISSIONS DEMANDÉES

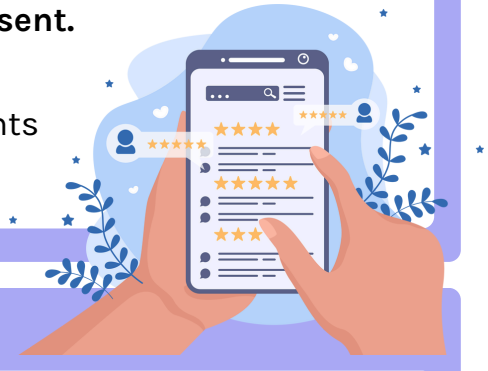
- Lorsque vous installez une application, elle demande des autorisations pour accéder à certaines fonctionnalités de votre téléphone.
- Si une application demande des permissions qui semblent exagérées, **soyez prudent !**
- Exemple : Une application de gestion de tâches ne devrait pas avoir besoin d'accéder à vos photos.

2 DES APPLICATIONS SÉCURISÉES

CONSEILS DE SÉCURITÉ SUR LE TÉLECHARGEMENT D'APPLICATIONS

3. LISEZ LES AVIS ET LES NOTES

- Avant de télécharger une application, **regardez ce que les autres utilisateurs en disent.**
- Méfiez-vous des applications avec peu d'avis ou de nombreux avis négatifs.
- Exemple : Si vous cherchez une application pour suivre vos trajets entre vos différents bénéficiaires, choisissez en une avec de bons avis et ceux-ci doivent être nombreux



4. METTEZ VOS APPLICATIONS À JOUR RÉGULIÈREMENT

- Les mises à jour corrigent souvent des problèmes de sécurité.
- Activez les mises à jour automatiques pour ne pas avoir à y penser.

5. ATTENTION AUX APPLICATIONS GRATUITES

- Certaines applications gratuites peuvent financer leurs services en affichant des publicités ou en contenant des logiciels espions. Préférez les applications d'éditeurs connus et bien notées. Par exemple, une application gratuite pour prendre des notes pourrait collecter vos données pour les vendre à des annonceurs.

2 DES APPLICATIONS SÉCURISÉES

CONSEILS DE SÉCURITÉ SUR LE TÉLECHARGEMENT D'APPLICATIONS

6. SURVEILLEZ LES PERFORMANCES DE VOTRE TÉLÉPHONE

- Si votre téléphone devient soudainement lent ou agit de manière étrange après avoir installé une application, désinstallez cette application.
- Dans vos paramètres de téléphone, il est possible de vérifier combien de batterie et de données les applications utilisent. Si cela semblent trop élevé, quitter la page et/ou désinstallez l'application

7. ATTENTION AUX APPLICATIONS FREEMIUM !

- Certaines applications sont gratuites au début, mais deviennent payantes après une période d'essai ou demandent des paiements pour débloquer des fonctionnalités supplémentaires. Par exemple, une application devient payante après un mois d'utilisation gratuite mais vous demandera directement d'encoder vos données bancaires et vous débitera par la suite
- Lisez attentivement les conditions d'utilisation et vérifiez s'il y a des coûts cachés avant d'installer une application.

3 CODES ET AUTRES VERROUILLAGES

POURQUOI LA SÉCURITÉ DE VOS APPAREILS EST-ELLE IMPORTANTE ?

Les appareils mobiles, comme les téléphones et les tablettes, contiennent souvent des informations personnelles sensibles. Protéger ces appareils est essentiel pour éviter que ces informations ne tombent entre de mauvaises mains.
Parmi les protections disponibles, les codes, empreinte, etc sont des méthodes de verrouillages : votre appareil ne peut être vu sans être déverrouillé.

Ceux-ci permettent d'éviter que n'importe qui puisse avoir accès à vos appareil.

VOICI QUELQUES CONSEILS SIMPLES POUR SÉCURISER VOS APPAREILS À L'AIDE DE CES MÉTHODES DE VERROUILLAGE :

3 CODES ET AUTRES VERROUILLAGES

POURQUOI LA SÉCURITÉ DE VOS APPAREILS EST-ELLE IMPORTANTE ?

QU'EST-CE QU'UN MOT DE PASSE OU UN CODE PIN ?

- Un mot de passe est une série de lettres, de chiffres et parfois de symboles que vous créez pour protéger votre appareil.
- Un code PIN est un code numérique (souvent à 4 ou 6 chiffres) que vous entrez pour déverrouiller votre appareil.
- Ils empêchent les personnes non autorisées d'accéder à vos informations personnelles si elles prennent votre téléphone.

COMMENT CRÉER UN MOT DE PASSE ?

- Créer un mot de passe ou un code pin fort est la meilleure manière de garantir la sécurité de son appareil. Plus c'est complexe, plus il sera difficile de le découvrir. Un code pin "1234" est beaucoup trop simple. De même, il est conseillé de ne pas utiliser de mot de passe trop simple, par exemple le nom de ses enfants, car il est trop facile pour les pirates de trouver ces infos et déverrouiller vos appareils.
- **Critères d'un bon mot de passe ou code PIN :**
  - Fort : Utilisez une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles. Par exemple, "A!d3_@D0m1c1l3".
  - Longueur : Plus le mot de passe est long, mieux c'est. Essayez d'utiliser au moins 12 caractères.
  - Complexité : Mélangez différents types de caractères (lettres, chiffres, symboles).
  - Diversité : Évitez d'utiliser le même mot de passe pour plusieurs comptes.
  - Code PIN : Utilisez un code à 6 chiffres plutôt qu'à 4 chiffres pour plus de sécurité. Par exemple, "482193" est bien plus sûr que "1111".

4 VERROUILLER SES APPAREILS

UTILISER UN MOT DE PASSE OU UN CODE PIN

VOICI QUELQUES ASTUCES :

MÉTHODES POUR RETENIR VOS MOTS DE PASSE ET CODES PIN

- **Mémorisation** : Créez des phrases faciles à retenir et utilisez les premières lettres de chaque mot. Par exemple: "Mon Chien Bruno Adore Jouer Dans Le Parc!" devient "MCB@JDL_P!".
- **Gestionnaire de mots de passe :** Utilisez un gestionnaire de mots de passe pour stocker et générer des mots de passe complexes et sécurisés. Il vous suffit de retenir un seul mot de passe principal.
- **Notes sécurisées :** Si vous devez absolument écrire vos mots de passe, ne les écrivez pas tels quels, utilisez des indices ou des codes que vous seul comprenez et gardez-les dans un endroit sécurisé (ex: activité préférée de Bruno : jouer dans le parc)

4 VERROUILLER SES APPAREILS

UTILISER L'EMPREINTE DIGITALE

L'EMPREINTE DIGITALE

- **Qu'est-ce que l'empreinte digitale ?**
  - C'est une méthode de sécurité qui utilise votre empreinte digitale pour déverrouiller votre appareil.
- **Pourquoi l'utiliser ?**
  - C'est rapide et pratique. Il suffit de poser votre doigt sur le capteur pour déverrouiller votre appareil.
  - C'est plus sécurisé que de simples mots de passe ou codes PIN, car chaque empreinte digitale est unique.
- **Comment l'activer ?**
  - Allez dans les paramètres de votre téléphone.
  - Recherchez les options de sécurité ou de biométrie.
  - Suivez les instructions pour enregistrer votre empreinte digitale.

4 VERROUILLER SES APPAREILS

UTILISER LA RECONNAISSANCE FACIALE

LA RECONNAISSANCE FACIALE

- **Qu'est-ce que la reconnaissance faciale ?**
  - C'est une méthode de sécurité qui utilise une caméra pour reconnaître votre visage et déverrouiller votre appareil.
- **Pourquoi l'utiliser ?**
  - Comme l'empreinte digitale, c'est rapide et pratique.
  - C'est sécurisé car il est difficile pour quelqu'un de simuler votre visage.
- **Comment l'activer ?**
  - Allez dans les paramètres de votre téléphone.
  - Recherchez les options de sécurité ou de biométrie.
  - Suivez les instructions pour enregistrer votre visage.

4 VERROUILLER SES APPAREILS

CONSEILS GÉNÉRAUX POUR LA SÉCURITÉ DES APPAREILS

1

Ne partagez pas vos mots de passe ou codes PIN !

Gardez ces informations pour vous afin de protéger vos données.

2

Changez régulièrement vos mots de passe !

Mettez à jour vos mots de passe de temps en temps pour une sécurité renforcée.

3

Utilisez une protection supplémentaire pour les applications sensibles !

Si vous avez des applications contenant des informations sensibles (comme les applications bancaires), ajoutez une couche de sécurité supplémentaire (comme un mot de passe ou une empreinte digitale pour accéder à ces applications).

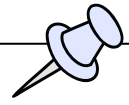
4

Soyez attentif aux environnements non sécurisés !

Évitez de déverrouiller votre téléphone ou d'entrer vos mots de passe en public où quelqu'un pourrait voir ce que vous faites.

5 AUTHENTIFICATION À 2 FACTEURS

QU'EST-CE QUE L'AUTHENTIFICATION À DEUX FACTEURS ?



- L'authentification à deux facteurs (ou 2FA pour "Two-Factor Authentication") ou encore “validation en 2 étapes” est une méthode de sécurité qui ajoute une couche supplémentaire de protection lors de la connexion à vos comptes en ligne.
- Elle nécessite non seulement un mot de passe, mais aussi un second élément de vérification, souvent appelé "facteur", qui est quelque chose que vous avez (comme votre téléphone) ou quelque chose que vous êtes (comme une empreinte digitale) et qui permettra de prouver que c’est bien vous.

EN RÉSUMÉ: VOUS VOUS IDENTIFIEZ 2 FOIS AU LIEU D’UNE !

5 AUTHENTIFICATION À 2 FACTEURS

POURQUOI METTRE EN PLACE L'AUTHENTIFICATION À DEUX FACTEURS ?

RENFORCER LA SÉCURITÉ

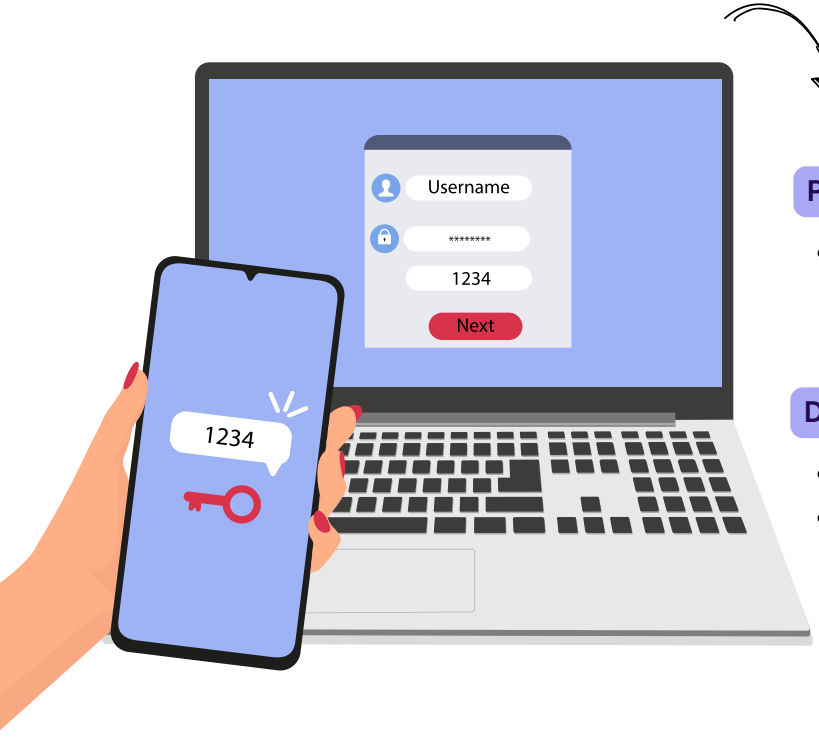
- Même si quelqu'un découvre votre mot de passe, il lui sera difficile d'accéder à votre compte sans le second facteur. Cela réduit donc considérablement le risque de piratage, car un attaquant aurait besoin à la fois de votre mot de passe et du second facteur.
- Les mots de passe peuvent être volés ou devinés, mais le deuxième facteur, généralement une information physique que vous possédez, est beaucoup plus difficile à compromettre. Vous pouvez être plus serein en sachant que vos comptes sont mieux protégés.

PROTÉGER VOS DONNÉES SENSIBLES

- Vos données sont bien plus sécurisées avec une double authentification qu'un seul mot de passe. Pensez notamment à vos comptes bancaires, vos emails, etc.
- En tant qu'aide à domicile, vous pouvez avoir (accès à) des informations personnelles et sensibles sur votre téléphone ou ordinateur (comme des rendez-vous, des notes sur les bénéficiaires, etc.). Il est donc important de tout faire pour que ces données soient protégées!

5 AUTHENTIFICATION À 2 FACTEURS

POURQUOI METTRE EN PLACE L'AUTHENTIFICATION À DEUX FACTEURS ?



PREMIÈRE ÉTAPE :

- Vous entrez votre nom d'utilisateur et votre mot de passe comme d'habitude.

DEUXIÈME ÉTAPE :

- Vous êtes invité à fournir un deuxième élément de vérification.
- Ce peut être :
  - **Code envoyé par SMS :** Vous recevez un code sur votre téléphone que vous devez entrer.
  - **Application d'authentification :** Une application comme Google Authenticator ou Microsoft Authenticator génère un code unique à usage limité dans le temps.
  - **Clé de sécurité physique :** Un petit appareil que vous insérez dans votre port USB.
  - **Reconnaissance biométrique :** Utilisation de votre empreinte digitale ou de la reconnaissance faciale.

5 AUTHENTIFICATION À 2 FACTEURS

COMMENT ACTIVER L'AUTHENTIFICATION À DEUX FACTEURS ?

SUR UN COMPTE GOOGLE

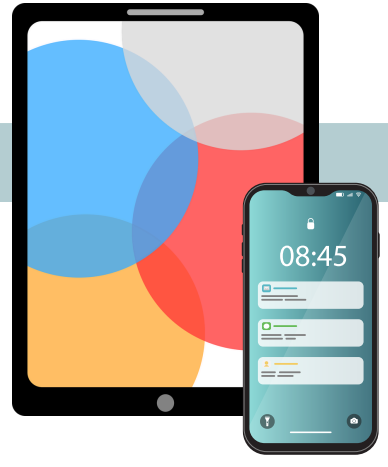
- Allez dans les paramètres de votre compte Google.
- Sélectionnez "Sécurité" puis "Validation en deux étapes".
- Suivez les instructions pour ajouter votre numéro de téléphone ou une application d'authentification.

Pour Android (smartphone et tablette)

SUR UN COMPTE ICLOUD

- Allez dans les "Réglages", puis appuyez sur votre nom en haut.
- Sélectionnez "Mot de passe et sécurité" puis "Activer l'authentification à deux facteurs".
- Suivez les étapes pour configurer.

Pour Apple (smartphone et tablette)



SUR UN ORDINATEUR WINDOWS :

- Allez sur le site de votre compte Microsoft.
- Sous "Sécurité", sélectionnez "Plus d'options de sécurité" puis "Configurer l'authentification à deux facteurs".
- Choisissez votre méthode préférée et suivez les instructions.

6 LES MISES À JOUR

C’EST QUOI LES MISES À JOUR ?

- Les mises à jour de votre téléphone, ordinateur ou tablette sont comme des visites régulières chez le médecin. Elles sont cruciales pour maintenir la sécurité et les performances de votre appareil. Elles corrigent les failles de sécurité, ajoutent de nouvelles fonctionnalités et améliorent la stabilité des applications.
- Par exemple, si vous utilisez une application pour vos déplacements chez vos bénéficiaires, une mise à jour pourrait corriger un bug qui vous faisait perdre du temps en proposant des chemins peu optimisés ou ne prenant pas en compte certains changements.
- Pensez à activer les mises à jour automatiques pour vous assurer que votre appareil reste sécurisé sans que vous ayez à y penser.

6 LES MISES À JOUR

COMMENT ACTIVERS LES MISES À JOUR

POUR LES APPAREILS ANDROID

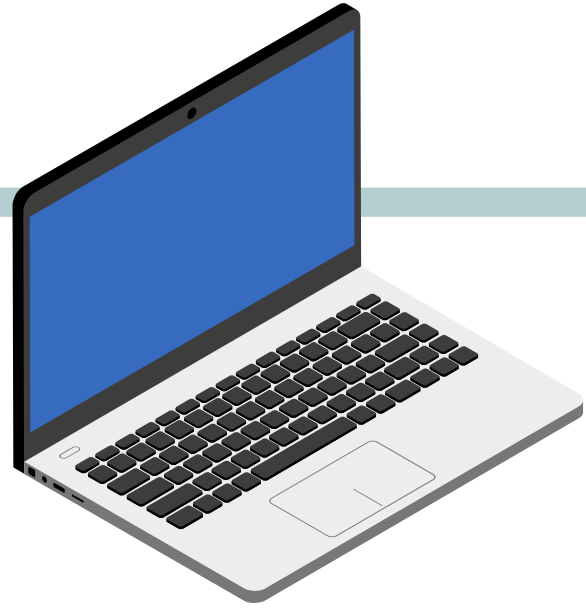
- Appuyez sur l'icône "Paramètres" de votre téléphone.
- Faites défiler vers le bas et appuyez sur "Système".
- Appuyez sur "Avancé" puis sur "Mises à jour système".
- Appuyez sur "Vérifier les mises à jour". Si une mise à jour est disponible, suivez les instructions pour l'installer.
- Assurez-vous que l'option de mises à jour automatiques est activée.

6 LES MISES À JOUR

COMMENT ACTIVERS LES MISES À JOUR

POUR LES ORDINATEURS WINDOWS :

- Cliquez sur le menu "Démarrer" et sélectionnez l'icône "Paramètres" (roue dentée).
- Cliquez sur "Mise à jour et sécurité".
- Cliquez sur "Windows Update" dans le menu de gauche.
- Cliquez sur "Rechercher des mises à jour". Si des mises à jour sont disponibles, elles s'installeront automatiquement.
- Assurez-vous que les mises à jour automatiques sont activées. Windows installe généralement les mises à jour automatiquement par défaut.



6 LES MISES À JOUR

COMMENT ACTIVERS LES MISES À JOUR

POUR LES APPAREILS IOS (APPLE) :

- Appuyez sur l'icône "Réglages".
- Faites défiler vers le bas et appuyez sur "Général".
- Appuyez sur "Mise à jour logicielle".
- Appuyez sur "Mises à jour automatiques" et activez "Télécharger les mises à jour iOS" et "Installer les mises à jour iOS".

7 LA FONCTION “LOCALISER”

C’EST QUOI ?

- La fonction "Localiser" est essentielle pour aider à retrouver son téléphone. C’est encore plus intéressant quand on a un travail mobile. Imaginez que vous perdez votre téléphone en route entre deux domiciles. Grâce à cette fonction, vous pouvez le localiser sur une carte, le faire sonner pour le retrouver ou même verrouiller l'accès à distance pour protéger vos données sensibles et celles de vos bénéficiaires.
- Activez cette fonctionnalité dans les paramètres de votre téléphone pour avoir l'esprit tranquille et assurer la sécurité de vos informations professionnelles.

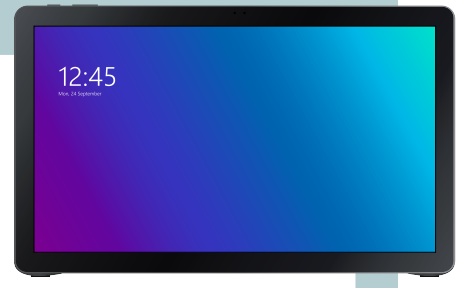
7 LA FONCTION “LOCALISER”

COMMENT ACTIVER LES MISES À JOUR

POUR LES SMARTPHONES ANDROID :

- Appuyez sur l'icône "Réglages".
- Appuyez sur votre nom en haut de l'écran.
- Appuyez sur "Localiser" puis sur "Localiser mon iPhone"
- Activez "Localiser mon iPhone" et "Envoyer la dernière position".

POUR LES TABLETTES ANDROID :



- Appuyez sur l'icône "Paramètres".
- Faites défiler et appuyez sur "Sécurité".
- Appuyez sur "Trouver mon appareil".
- Assurez-vous que la fonctionnalité est activée.

POUR LES ORDINATEURS MACOS (APPLE)

- Cliquez sur le menu "Démarrer" et sélectionnez l'icône "Paramètres".
- Cliquez sur "Mise à jour et sécurité".
- Cliquez sur "Trouver mon appareil" dans le menu de gauche.
- Cliquez sur "Modifier" sous "Trouver mon appareil est désactivé" et activez la fonction.

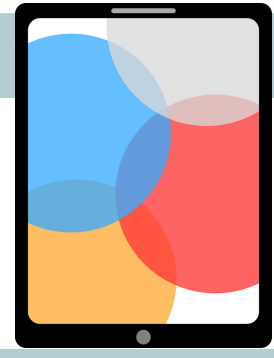
7 LA FONCTION “LOCALISER”

COMMENT ACTIVERS LES MISES À JOUR

POUR LES SMARTPHONES IOS (APPLE) :

- Appuyez sur l'icône "Réglages".
- Appuyez sur votre nom en haut de l'écran.
- Appuyez sur "Localiser" puis sur "Localiser mon iPhone"
- Activez "Localiser mon iPhone" et "Envoyer la dernière position".

POUR LES TABLETTES IOS (APPLE) :



- Appuyez sur l'icône "Réglages".
- Appuyez sur votre nom en haut de l'écran.
- Appuyez sur "Localiser" puis sur "Localiser mon iPad".
- Activez "Localiser mon iPad" et "Envoyer la dernière position".

POUR LES ORDINATEURS MACOS (APPLE)

- Cliquez sur le menu "Apple" en haut à gauche de l'écran et sélectionnez "Préférences Système".
- Cliquez sur "Identifiant Apple" puis "iCloud".
- Cochez la case "Localiser mon Mac". Vous devrez peut-être vous connecter avec votre identifiant Apple.

EN SUIVANT CES ÉTAPES, VOUS POUVEZ ASSURER QUE VOS APPAREILS SONT À JOUR ET QUE VOUS POUVEZ LES RETROUVER EN CAS DE PERTE OU DE VOL. CELA GARANTIT LA SÉCURITÉ DE VOS INFORMATIONS PERSONNELLES ET PROFESSIONNELLES, ESSENTIELLES POUR LES AIDES À DOMICILE.

Voici des ressources généralement recommandées pour vérifier et approfondir ces procédures :

1. **Sites officiels de Microsoft :**
   - Support Microsoft pour Windows Update
   - Support Microsoft pour la fonction "Trouver mon appareil"
2. **Sites officiels d'Apple :**
   - Support Apple pour les mises à jour sur macOS :
   - Support Apple pour les mises à jour sur iOS
   - Support Apple pour "Localiser mon Mac"
   - Support Apple pour "Localiser mon iPad"
3. **Sites officiels d'Android et de Google :**
   - Support Google pour les mises à jour Android

Ces ressources sont régulièrement mises à jour et offrent des instructions détaillées et des captures d'écran pour faciliter la mise en œuvre de ces mesures de sécurité sur divers appareils.