La sécurité informatique est un sujet crucial : sur nos PC, nos smartphones ou tout autre appareil connecté à Internet. Pour protéger nos données, il est essentiel d'adopter de bonnes habitudes.

1. Qu'est-ce que la sécurité informatique ?

La sécurité informatique inclut la protection du matériel, des données et de la vie privée contre des menaces telles que les virus, les pirates informatiques, le vol de données ou toute forme d'attaques malveillantes.

Les fiches de cette thématique présentent des moyens techniques, juridiques, pratiques et humains pour renforcer sa sécurité informatique, et plus particulièrement sa sécurité en ligne, aussi appelée cybersécurité. Pour être efficaces, tous ces moyens doivent être associés à une analyse et à une réduction des risques.

Il sera également question de :

- protéger et de préserver sa santé, aussi bien physique que mentale avec le numérique (voir fiche 9.11.).
- protéger l'environnement avec une utilisation raisonnée et raisonnable du numérique (voir fiche 9.12.).

2. 10 règles essentielles pour assurer sa cybersécurité

1. **Créez des mots de passe forts** (voir fiche 9.4. ; 9.7. et 9.8.)
   - Utilisez des MAJUSCULES, minuscules, chiffres, caractères spéciaux : @ ! - _ &
   - Utilisez des mots de passe différents pour chaque service.
   - Changez régulièrement vos mots de passe, plusieurs fois par an.
   - Mémorisez vos mots de passe ou utilisez des moyens pour vous en souvenir facilement.

2. **Sauvegardez régulièrement**
   Faites des sauvegardes régulières de vos données (voir fiche 9.5. et 9.9.) sur différents supports : disques durs externes, sauvegardes en ligne…

3. **Mettez à jour**
   Veillez à la mise à jour de vos appareils et logiciels (voir fiche 9.5. et 9.8.).
   Les mises à jour corrigent souvent des failles de sécurité ou renforcent la sécurité.

4. **Connaissez vos ennemis**
   Comprendre les différents types de menaces et s'en protéger (voir fiche 9.2. et 9.8.).
   - Posez un regard critique sur les informations que vous recevez
   - Utilisez des outils d'analyse comme l'antivirus

5. **Méfiez-vous des réseaux Wi-Fi publics**
   Évitez les réseaux Wifi publics ou inconnus (voir fiche 9.9. et 2.5.). Très faciles d'accès, ces réseaux peuvent être contrôlés par des personnes malintentionnées pour intercepter vos informations personnelles. Evitez autant que possible de réaliser des opérations à caractère sensible comme des paiements bancaires.

6. Contrôlez les paramètres
Contrôlez les permissions, l'accessibilité et les options de confidentialité de vos appareils (voir fiche 9.6.). Savoir qui a accès à quoi permet de limiter les risques de fuites d'informations et les pertes de données. Faites attention aux autorisations demandées par les applications et les sites web que vous visitez.

7. Séparez usages privés et professionnels
Séparez bien vos usages privés et professionnels (voir fiche 9.10. et 9.11.).
Évitez de partager des informations professionnelles sur vos réseaux sociaux personnels, et inversément. Le partage et l'interprétation d'informations peuvent très vite nuire à votre réputation dans la vie physique ou en ligne, ainsi qu'à celle de la structure pour laquelle vous travaillez.

8. Evitez les sites douteux ou illicites (voir fiche 9.6. et 9.8.).
N'utilisez pas de plateformes non-officielles et ne téléchargez pas de fichiers provenant d'un site de téléchargement illégal. Sur ces sites, de nombreux fichiers sont infectés et peuvent contenir des virus et autres logiciels malveillants.

9. Communiquez en conscience
Réfléchissez à toutes les informations que vous communiquez, partagez sur les réseaux sociaux ou les plateformes collaboratives (voir fiche 9.6. et 9.10.). De nombreuses informations personnelles peuvent tomber entre de mauvaises mains et être utilisées pour vous nuire. De même, ne relayez pas d'informations non vérifiées.

10. Restez vigilant·e
Dans le doute, demandez de l'aide à une personne de confiance ou à un·e professionnel·le. Les usages et pratiques évoluent sans cesse, il est donc important de se mettre régulièrement à jour et de demander conseils.

3. La sécurité à tout âge : CYBERSIMPLE.be

L'initiative **cybersimple.be** est le fruit d'une étroite collaboration entre Google et Test-Achats.
Elle vise à promouvoir un Internet plus sûr et à sensibiliser les consommateur·rices à mieux se protéger face aux risques possibles sur le net.

L'objectif est de fournir des connaissances utiles pour optimiser et maintenir sa sécurité sur le Web.

Le site aborde les problématiques principales auxquelles doit faire face chaque utilisateur·rice.

C'est simple et ludique, grâce à différents outils de sécurité et de nombreux conseils concrets.

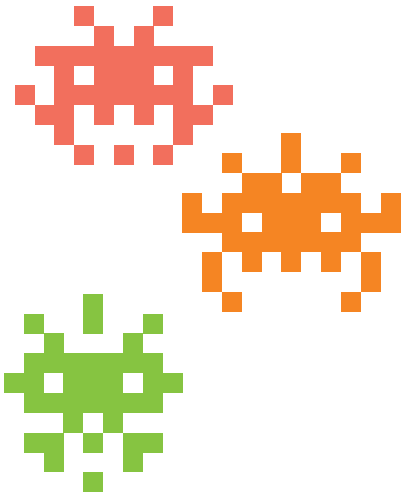
interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

Le monde numérique offre plein d'avantages mais il comporte aussi des risques : entre les fraudes, les arnaques par e-mails, les faux profils qui se font passer pour des proches et les logiciels malveillants, il est légitime de s'inquiéter. Comment se protéger au mieux des pirates du web ?

1. Les logiciels malveillants ou malwares

Les logiciels malveillants sont des logiciels conçus à des fins de piratage informatique.
Il en existe de différentes sortes en fonction de l'objectif visé :



- **Le virus** est un logiciel qui se réplique de lui-même, comme un virus humain. Il se diffuse, entre autres, via les pièces jointes des mails.
- **Le ransomware/rançongiciel** prend les données en otage. Il bloque l'accès aux fichiers contenus sur l'appareil et le paiement d'une rançon est exigé pour y avoir à nouveau accès. Les grandes sociétés et les citoyens peuvent être visés par cette menace.
- **Le spyware** ou logiciel espion va s'immiscer dans la machine afin de récolter des informations, espionner. Il est très discret, restant généralement caché le temps de récolter les données recherchées.
- **Le Trojan ou cheval de Troie** est quant à lui un logiciel malveillant qui se présente comme légitime à l'utilisateur·trice : après téléchargement, il agira en arrière-plan afin de tirer profit des ressources et données de la machine.

Face à autant de menaces, il apparait qu'utiliser le numérique n'est pas sans danger. Vigilance et bons réflexes sont donc importants, tout comme un nettoyage régulier de vos appareils.
Et évitez les sites de téléchargement illégaux. Ils sont truffés de logiciels malveillants.

2. Les pratiques malveillantes

Aujourd'hui, il existe des logiciels très performants, qui peuvent bloquer la plupart des logiciels malveillants. Mais il y a toujours un point faible dans la sécurité informatique : **l'humain**.

Le social engineering, ou **l'ingénierie sociale**, consiste à manipuler une personne pour qu'elle télécharge un logiciel malveillant ou dévoile ses données. Les cybercriminels utilisent l'appât du gain, la peur ou la confiance des victimes pour parvenir à leurs fins. Ils utilisent différents canaux et exploitent les informations qu'ils trouvent en ligne, notamment sur les réseaux sociaux :

- En se faisant passer pour un proche malade/dans le besoin
- En créant un lien et en faisant preuve d'empathie avec la victime

- **Le hameçonnage/phishing** consiste à envoyer des e-mails dans le but de soutirer des informations personnelles comme le mot de passe ou les données bancaires.
  La variante **par SMS** s'appelle **le vishing**.
- **Le spoofing** est une technique de fraude qui consiste à se faire passer pour un organisme ou personne de confiance (comme la banque ou un proche) pour pousser à dévoiler ses données. Par exemple, avec un faux e-mail de la banque pour connaitre vos données bancaires.
- **Le piratage de compte** est l'accès non autorisé à un compte en ligne (boite mails, réseaux sociaux...) suite au vol des identifiants de connexion.
- Et toutes les autres formes d'arnaques qui visent à voler des données et/ou de l'argent.

Conseils sécurité avec les e-mails

- Supprimez les mails suspects sans les ouvrir
- Vérifiez l'adresse e-mail de l'expéditeur
- Ne cliquez pas sur le lien depuis un e-mail. Rendez-vous directement sur le site (voir fiche 3.2.)
- Vérifiez les pièces jointes

Vigilance avec les e-mails

Les spams, **pourriels**, ou **courriers indésirables** peuvent contenir une pièce jointe avec un virus ou un lien menant vers un faux site ressemblant à un site de confiance. Méfiez-vous aussi :

- des messages qui affirment que vous avez droit à un remboursement ou une prime avec une apparence officielle, encore plus selon l'actualité (crise énergétique etc).
- des demandes d'argent, des appels à l'aide larmoyants de personnes coincées à l'étranger ou de gains à des concours auxquels vous n'avez pas joué... (voir aussi fiche 3.4.et 4.4.).

Les techniques des cybercriminels pour tromper sont nombreuses et la vigilance est de mise.

3. Le net n'est pas sécurisé alors ?

Si l'idée de risquer de se faire arnaquer ou de cliquer sur le mauvais lien peut être inquiétante, rappelez-vous que le vol de données ou d'argent et les arnaques existaient avant le numérique.
Prudence, bon sens, protection de vos appareils et données sont vos meilleurs alliés pour limiter les risques.

Il existe différentes ressources pour s'entrainer à se protéger en ligne comme :

- Le site Cybersimple.be qui reprend de nombreux conseils pour se protéger en ligne
- Space Shelter, un jeu interactif sur la sécurité en ligne https://spaceshelter.withgoogle.com
- Le site https://safeonweb.be

CYBERSIMPLE.be

Safeonweb.be
Indice de Santé digitale

SPACE SHELTER

interface3 namur
www.interface3namur.be/box-numerique

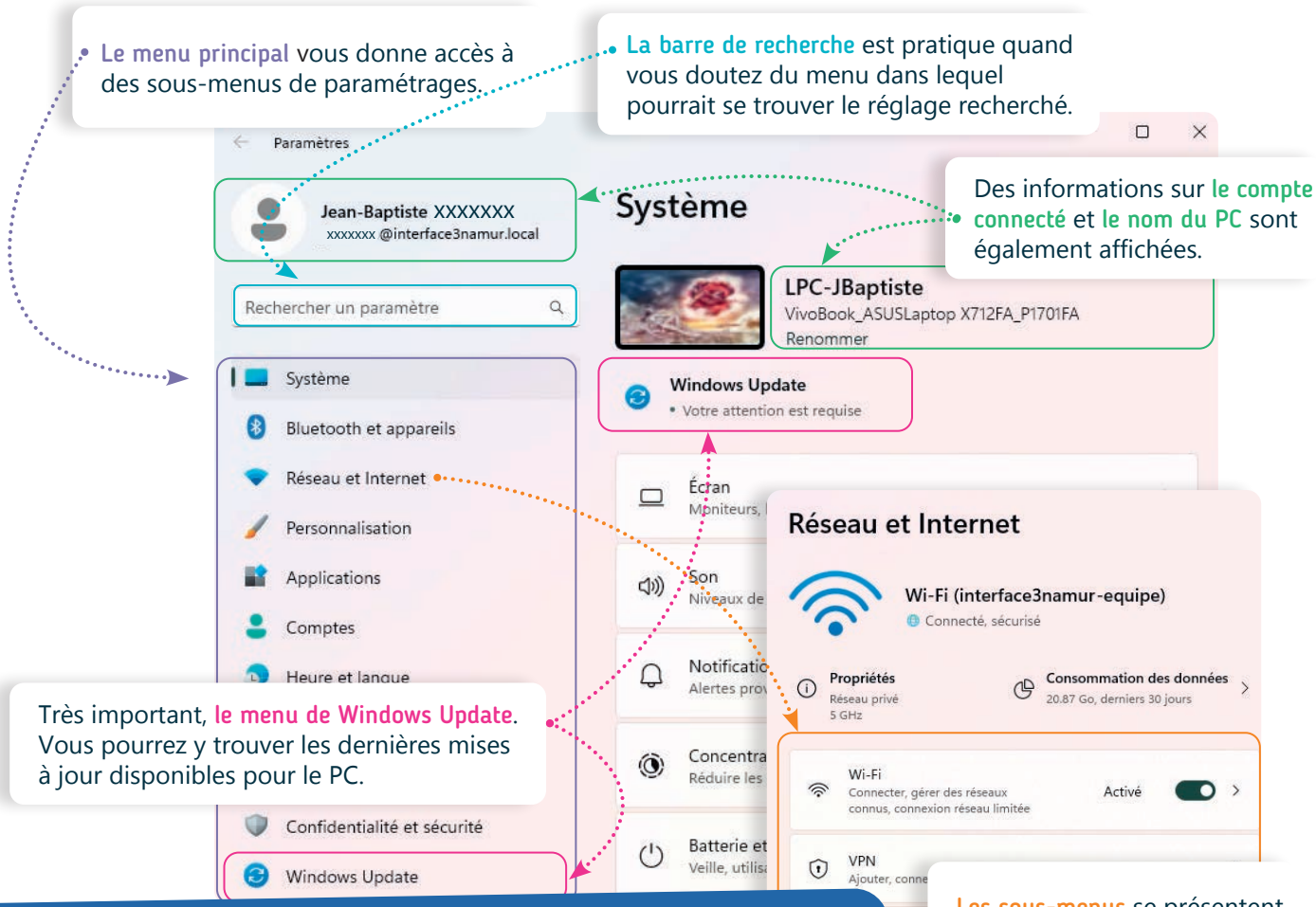
Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

Les PC, comme les smartphones, ont un menu « Paramètres ». Ce menu permet de configurer l'appareil en fonction des besoins et préférences : notifications et alertes visuelles ou sonores, options de confidentialité et de sécurité… Apprenez à accéder aux paramètres de vos appareils.

1. Accéder aux paramètres sur PC

Pour accéder aux paramètres d'un PC avec Windows, il y a plusieurs chemins possibles :

- Cliquez sur le menu **Démarrer** (voir fiche 1.3.) et sélectionnez l'application avec **une roue crantée** (au dessus de l'option Marche /Arrêt sur Windows 10, dans les applications épinglées sur Windows 11).
- Dans le champ de recherche de la barre des tâches (voir fiche 1.3.) (en bas à gauche sur Windows 10, vers le milieu sur Windows 11), tapez « **Paramètres** » et sélectionnez l'application.
- Appuyez sur la touche et la touche I en même temps et le menu s'ouvrira directement.



Le menu **Paramètres** est une étape importante de la gestion et de l'optimisation de votre PC.

Être capable d'adapter la luminosité de l'écran, modifier le volume ou avoir accès à des thèmes contrastés et une loupe permettent par exemple une utilisation plus confortable. Si vous faites des modifications dans les paramètres, lisez bien toutes les instructions et ne faites qu'une modification à la fois : cela vous permettra d'annuler plus facilement l'action si le résultat n'est pas celui recherché !

2. Accéder aux paramètres sur smartphone

Il existe plusieurs manières d'accéder à l'application Paramètres sur smartphone :

1. Via l'icône « Paramètres » :

Touchez l'icone de l'application Paramètres qui se trouve souvent sur l'écran d'accueil du smartphone ou dans le tiroir d'applications qui rassemble toutes les applications du téléphone.

1. Glissez votre doigt vers le haut ou appuyez sur le bouton pour accéder au tiroir d'applications.
2. Appuyez sur l'icône « Paramètres » pour ouvrir l'application.
3. Vous pouvez aussi rechercher l'application en tapant « Paramètres » dans le champ de recherche.
   Appuyez sur l'icone pour ouvrir les paramètres.

> Il se peut que le tiroir d'applications ne soit pas accessible selon le style d'écran défini (mode classique ou tiroir modifiable dans les paramètres).

2. Via le menu déroulant d'accès rapides aux paramètres :

A. Faites glisser votre doigt depuis le haut de l'écran pour dérouler le menu d'accès rapide aux paramètres sur l'écran.

B. Touchez l'icône « Paramètres »

Naviguer dans les paramètres

Comme sur PC, les paramètres sont organisés en différents menus. Touchez le nom du menu pour accéder aux sous-menus et options de réglages. Une flèche en haut à gauche vous permet alors de revenir au menu précédent.

Interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

Box Numérique

9. SÉCURITÉ

4. Verrouiller son smartphone

De nos jours, les smartphones sont devenus des outils indispensables pour la communication, la productivité et le divertissement. Chaque smartphone contient une quantité importante d'informations. Il est donc essentiel de le protéger contre tout accès non autorisé.

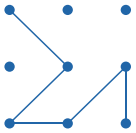
Verrouiller son smartphone est devenu une pratique courante pour garantir que seules les personnes autorisées puissent accéder aux informations stockées sur l'appareil. Plusieurs options de verrouillage sont disponibles, chacune ayant ses avantages et inconvénients.

1. Comment verrouiller/déverrouiller son smartphone ?

Les différents moyens de verrouiller un smartphone sont le code, le schéma, le mot de passe, l'empreinte digitale ou encore la reconnaissance faciale pour certains modèles. On peut classer les méthodes de déverrouillage en deux types :

1. Les méthodes basées sur un mot de passe/code.

Glissement : faire glisser un curseur sur l'écran pour déverrouiller l'appareil. C'est le plus simple des types de verrouillage, mais il n'offre pas de sécurité.



Modèle : dessiner un schéma sur l'écran pour déverrouiller l'appareil. C'est plus sécurisé que le verrouillage par glissement, mais moins sécurisé que le verrouillage par code ou mot de passe.

Code : saisir un code numérique sur l'écran pour déverrouiller l'appareil. C'est plus sécurisé que le verrouillage par modèle. Vous pouvez définir un code plus long pour une sécurité plus importante.

Mot de passe : saisir un mot de passe pour déverrouiller l'appareil. C'est le plus sécurisé de tous les types de verrouillage, car il vous permet de définir un mot de passe plus long et plus complexe pour une sécurité maximale, avec des lettres, majuscules et minuscules, chiffres...

2. Les méthodes basées sur la reconnaissance biométrique

empreintes digitales, reconnaissance faciale, reconnaissance de l'iris...

Scanner d'iris

Reconnaissance faciale

Analyse intelligente

Lecteur d'empreintes

Rapides et faciles à utiliser, notamment pour les personnes ayant des difficultés à saisir ou retenir un mot de passe. Ces types de verrouillages sont **propres à chaque individu** et offrent une sécurité supplémentaire.

Ces types de verrouillage nécessitent un matériel spécifique, comme un capteur d'empreinte digitale, et peuvent présenter des problèmes de fonctionnement, au contact de produits cosmétiques ou en cas de blessure par exemple.

2. Comment modifier le type de verrouillage

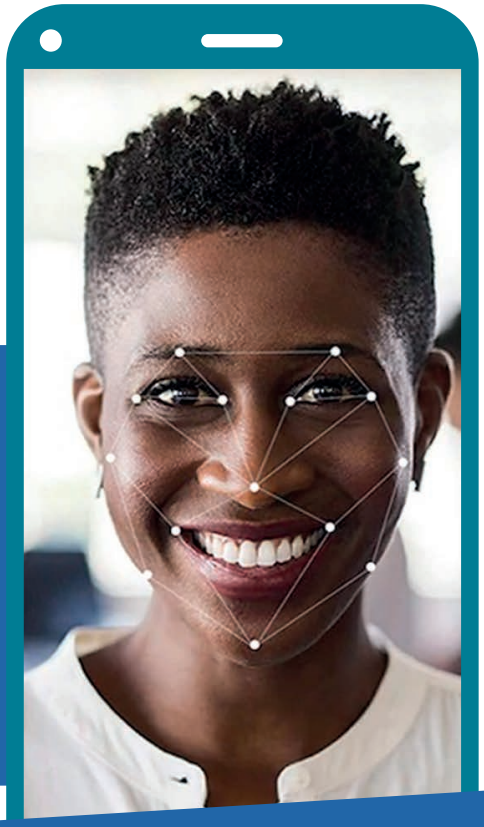
1. Ouvrez les « **Paramètres** » de votre appareil (voir fiche 9.3.).
2. Sélectionnez « **Sécurité** » ou « **Ecran de verrouillage** » (cela peut varier d'un appareil à l'autre), puis « **Mode de déverrouillage** ».
3. Touchez le nom du mode de verrouillage que vous souhaitez activer.
4. Suivez les instructions à l'écran pour configurer le mode de verrouillage.
5. Faites ce changement dans un moment calme pour bien conscientiser le verrouillage choisi et vous assurer de le retenir.

3. Empreintes digitales et reconnaissance faciale

De plus en plus de smartphones proposent également la possibilité de s'authentifier grâce aux **données biométriques** : empreintes digitales, reconnaissance faciale ou rétinienne…

Ces informations biométriques, qui permettent d'identifier une personne, peuvent être utilisées pour déverrouiller le smartphone ou s'authentifier sur des applications. **C'est un système d'authentification qui peut être confortable**.

Pour savoir si votre téléphone est doté de ce type de reconnaissance, rendez-vous dans les **Paramètres** (voir fiche 9.3.), puis « **Sécurité** » ou « **Ecran de verrouillage** » et recherchez « **Données biométriques** » ou « **Empreintes** »…



Où sont stockées les empreintes digitales et les visages ?

Les informations biométriques sont stockées dans un module sécurisé sur votre appareil Android. Ce module protège les données en les chiffrant et en les isolant du reste du système. Cela empêche les vols de données par des applications malveillantes ou des personnes malintentionnées.

Les empreintes digitales et les visages sont stockés dans le menu « **données biométriques et sécurité** ». Il est possible d'ajouter ou de supprimer des informations ultérieurement.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

5. Mise à jour et sauvegarde smartphone

Il est important de maintenir à jour votre smartphone Android et les applications installées pour bénéficier d'une utilisation optimale, d'une sécurité renforcée et de performances fiables.

1. En quoi consistent les mises à jour ?

Les mises à jour sont **de nouvelles versions des logiciels, applications**, installés sur le smartphone. Elles comprennent souvent des **correctifs de sécurité** pour protéger votre appareil, **des améliorations et de nouvelles fonctionnalités**. Cela garantit également la compatibilité de votre appareil avec les nouveaux logiciels et périphériques.

Pour profiter pleinement de votre smartphone, il est donc essentiel de le maintenir à jour. Il y a **2 grands types de mises à jour** :

- Les mises à jour du **système d'exploitation Android** (voir aussi la fiche 1.4.), c'est-à-dire les mises à jour du smartphone.
- Les mises à jour des **applications** installées sur le smartphone (voir aussi la fiche 1.14.).

2. Mettre à jour le système d'exploitation Android

1. Rendez-vous dans les paramètres (voir fiche 9.3.).
2. Recherchez **« Mise à jour »**. En fonction des smartphones, l'option se trouve en haut ou en bas.
3. Vérifiez que votre téléphone est à jour. Si une mise à jour est en attente, vous pouvez l'installer quand votre smartphone est **connecté à un réseau Wi-Fi** et **qu'il peut être inaccessible quelques minutes**. Lors de la mise à jour, le téléphone est fréquemment redémarré.

Comme les mises à jour du système sont importantes, quand une nouvelle mise à jour est disponible, vous en êtes averti·e par une notification. Si **une pastille rouge apparait sur l'icône** de l'application **Paramètres**, cela peut être une indication qu'une mise à jour est disponible.

3. Mettre à jour les applications

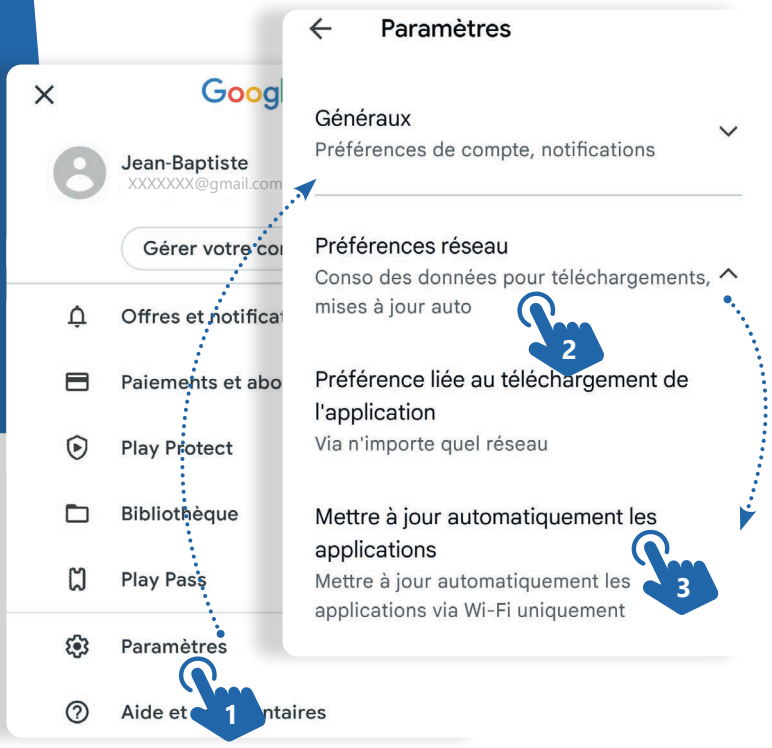
Les mises à jour d'applications améliorent et corrigent les bugs. **Elles se font souvent automatiquement** pour garantir une utilisation optimale de l'application. Pour vérifier :

1. Ouvrez l'application Google **Play Store**.
2. En haut à droite, appuyez sur l'icône du profil.
3. Appuyez sur **Gérer les applications et l'appareil**.

Les applis pour lesquelles une mise à jour est disponible sont signalées par la mention **« Mises à jour disponibles »**.

Mettre à jour les applications automatiquement ?

Si vous préférez que les mises à jour se fassent automatiquement, vérifiez dans les paramètres que les mises à jour se font uniquement via le Wi-Fi afin d'éviter des frais supplémentaires, dus à l'utilisation de la 4G/5G, lors du téléchargement des mises à jour (Voir fiche 2.2).



Toujours dans la partie **profil** de l'application Google **Play Store** :

1. Sélectionnez l'option **Paramètres**.
2. Puis appuyez sur **Préférences réseau**.
3. Et choisissez **Mettre à jour automatiquement les applications** > Via le Wi-Fi uniquement.

4. Sauvegarde du téléphone via votre compte Google

Avec votre compte Google, vous pouvez réaliser une sauvegarde automatique et régulière des données de votre téléphone. Cela comprend :

- Les données des applications (compatibles)
- L'historique des appels
- Les contacts
- Les paramètres de l'appareil
- Les photos et vidéos (si activé sur Google Photos)
- Les SMS (sur l'application Google Messages)

Si vous perdez ou remplacez votre appareil, vous pouvez facilement restaurer vos données à partir de cette sauvegarde. Au démarrage de votre nouveau mobile, il vous sera proposé de **« Copier vos applications et vos données »**.

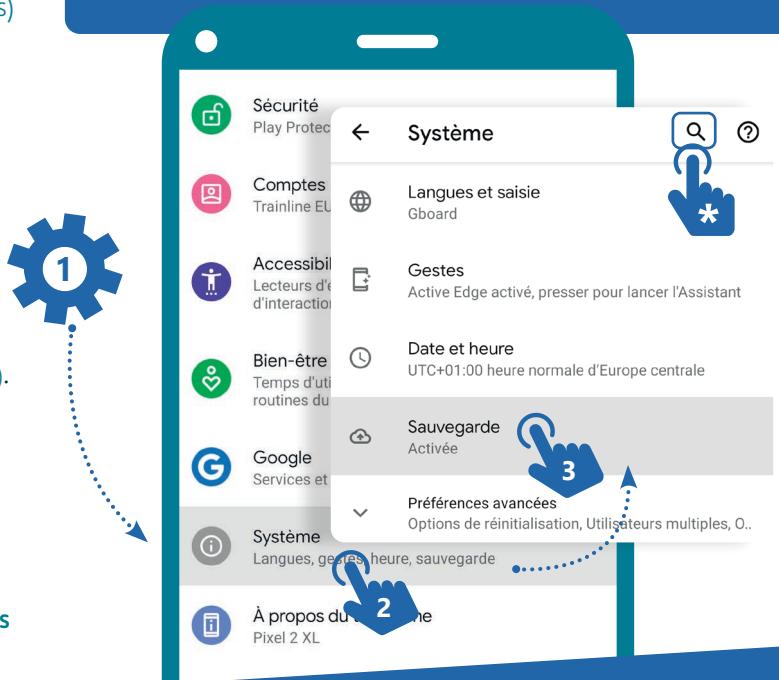
Votre compte Google offre **15 Go de stockage en ligne gratuit**, si vous avez besoin d'une quantité supplémentaire, vous pouvez souscrire à **un abonnement payant** via le service **Google One**. *Mais vous pouvez aussi transférer manuellement vos données vers d'autres supports de stockage ou bien encore faire un tri pour ne garder que ce qui vous semble essentiel!*

Pour vérifier si la sauvegarde automatique est bien activée :

1. Rendez-vous dans les **paramètres** (voir fiche 9.3.).
2. Appuyez sur **Système**
3. Et sélectionnez **Sauvegarde** ou **Sauvegarder et restaurer** ou une autre appellation.

Les menus de paramètres d'Android varient parfois légèrement en fonction des constructeurs.

Vous pouvez utiliser **l'outil de recherche des paramètres** et rechercher **« Sauvegarde »**.



interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

6. Réglages de confidentialité sur smartphone

Pour fonctionner, certaines applications ont besoin d'accéder à des données ou des fonctionnalités comme la localisation. Mais chaque autorisation doit être mesurée pour n'autoriser que le nécessaire et protéger votre vie privée.

1. Les autorisations des applications Android

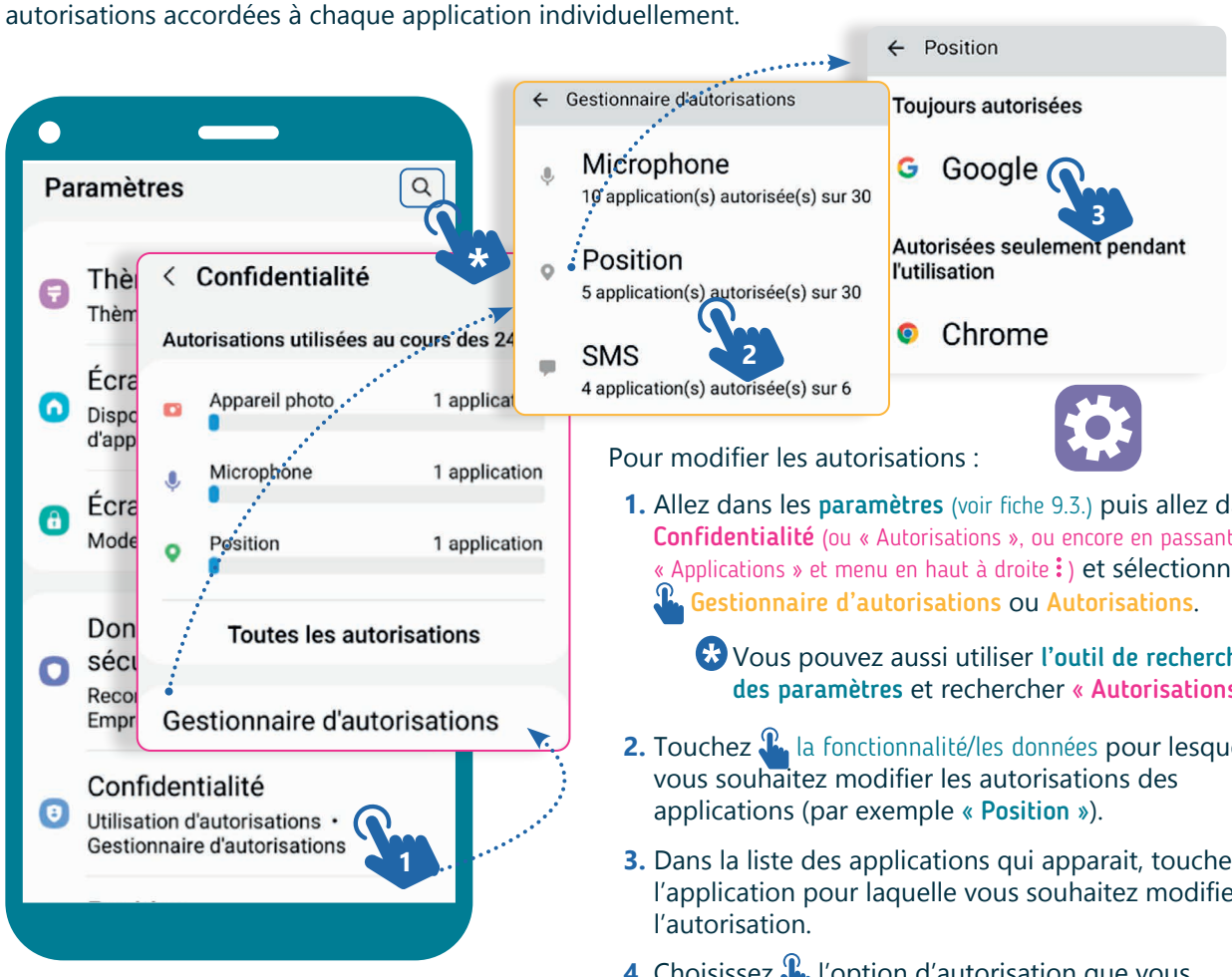
Les réglages de confidentialité permettent de contrôler l'accès global aux données du smartphone comme la localisation, le micro ou l'appareil photo. Via les **paramètres** (voir fiche 9.3.), vous pouvez activer ou désactiver l'accès à ces fonctionnalités pour toutes les applications (comme la localisation par exemple : voir fiche 9.7.).

Les autorisations des applications sont des demandes que les applications font aux utilisateur·rice·s pour accéder à certaines fonctionnalités (appareil photo, micro…) ou certaines données (les photos, les messages privés…). Pour bien fonctionner, certaines applications ont besoin d'autorisation. Par exemple, une application GPS a besoin d'accéder à la localisation du téléphone.

Les demandes d'autorisation des applications apparaissent la première fois qu'une application a besoin d'accéder à un composant matériel ou à des données du smartphone.

2. Modifier les autorisations des applications Android

Le gestionnaire d'autorisations regroupe les applications par autorisation. Il vous permet de contrôler les autorisations accordées à chaque application individuellement.

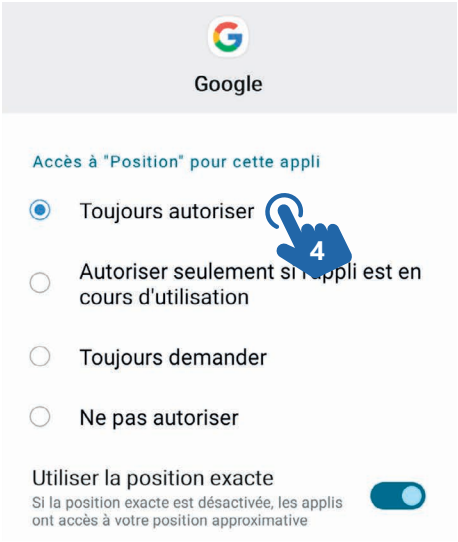


Pour modifier les autorisations :

1. Allez dans les **paramètres** (voir fiche 9.3.) puis allez dans **Confidentialité** (ou « Autorisations », ou encore en passant par « Applications » et menu en haut à droite ⋮) et sélectionnez **Gestionnaire d'autorisations** ou **Autorisations**.

   ✱ Vous pouvez aussi utiliser **l'outil de recherche des paramètres** et rechercher « **Autorisations** ».

2. Touchez la fonctionnalité/les données pour lesquelles vous souhaitez modifier les autorisations des applications (par exemple « **Position** »).
3. Dans la liste des applications qui apparait, touchez l'application pour laquelle vous souhaitez modifier l'autorisation.
4. Choisissez l'option d'autorisation que vous souhaitez parmi les options proposées (voir verso).



Attention à n'autoriser que ce qui est nécessaire au fonctionnement d'une application. Il est légitime qu'une application de GPS accède à votre position, beaucoup moins pour une application calculatrice.

- **Toujours autoriser :** même si vous n'utilisez pas l'application, elle peut continuer à collecter des informations sur votre position.
- **Autoriser seulement pendant l'utilisation :** accès à votre position uniquement pendant l'utilisation de l'application. Dès que vous quittez l'application, l'accès à votre position sera coupé.
- **Toujours demander :** une autorisation d'accéder à la localisation sera demandée à chaque lancement de l'application.
- **Ne pas autoriser :** l'application ne peut pas accéder à votre position.

3. En quoi consistent les autorisations des sites Web ?

Certains sites Web peuvent également demander l'accès à certaines informations ou fonctionnalités du smartphone comme la caméra, les contacts... Vous pouvez accepter ou refuser. Les autorisations peuvent aider à améliorer votre expérience sur le site, mais peuvent également poser des risques de confidentialité si elles sont accordées à des sites non fiables.

Lorsqu'un site Web demande l'utilisation du microphone, cela signifie qu'il souhaite accéder au microphone de l'appareil pour enregistrer du son.

4. Comment modifier les autorisations des sites Web ?

Une fois que l'autorisation est accordée ou refusée, **il est toujours possible de modifier votre choix en appuyant sur le cadenas à côté de la barre d'adresse du site internet**, puis en sélectionnant « Autorisations » pour voir la liste des autorisations accordées au site.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

7. Localiser son smartphone

Perdre son smartphone peut être stressant, surtout si des données importantes y sont enregistrées. Heureusement, il existe des fonctionnalités pour aider à retrouver son appareil, notamment grâce au compte Google connecté et associé au téléphone.

1. Retrouver les informations de connexion

Chaque smartphone Android nécessite **un compte Google associé**, configuré à la première utilisation du téléphone. Pour accéder à ce compte, vous devez connaitre **l'identifiant** (**adresse e-mail** comme : monadresse@gmail.com) et le **mot de passe**. Ils vous permettent aussi d'accéder aux fonctionnalités de localisation et de verrouillage de l'appareil à distance.

Pour retrouver les informations du compte associé et de connexion sur un smartphone Android :

A. Ouvrez les paramètres (voir fiche 9.3.).

B. Accédez à la section **« Comptes »** ou **« Comptes et sauvegarde »** ou encore **« Mots de passe et comptes »** (peut différer selon l'appareil ou la version d'Android installée).

C. Sélectionnez **« Gestion des Comptes »**. Vous verrez alors l'adresse email du **compte Google** associé au téléphone.

Si vous avez oublié votre mot de passe, appuyez sur **« Mot de passe oublié »** pour recevoir des instructions pour le réinitialiser.

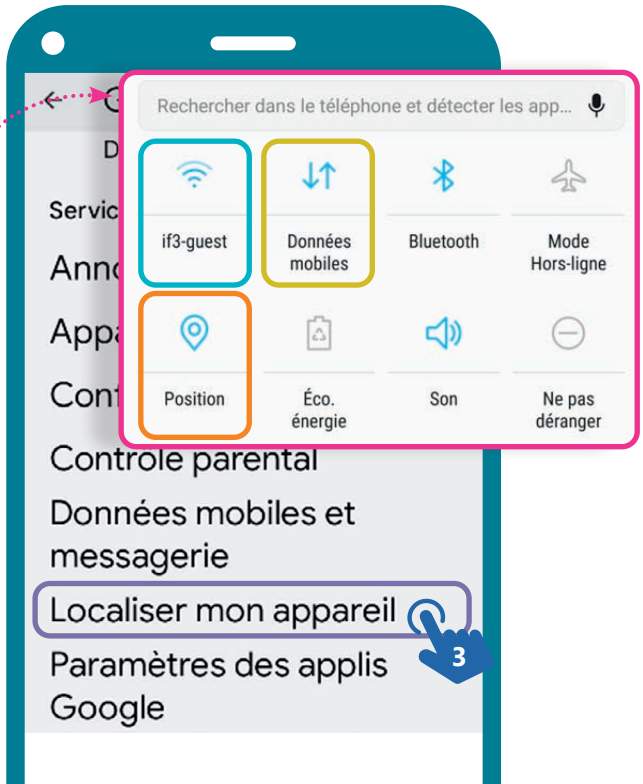
2. S'assurer que votre appareil peut être localisé

Pour pouvoir localiser un smartphone, le verrouiller ou effacer les données depuis un autre appareil, les conditions suivantes doivent être remplies :

- Votre appareil est associé à **un compte Google**.
- L'appareil est connecté à Internet via un réseau **Wi-Fi** ou **les données mobiles (3G/4G)**.
- La fonctionnalité de localisation **« Position »** est activée.

  Faites apparaitre **le menu d'accès rapide aux paramètres** (voir fiche 9.3.) pour vérifier.

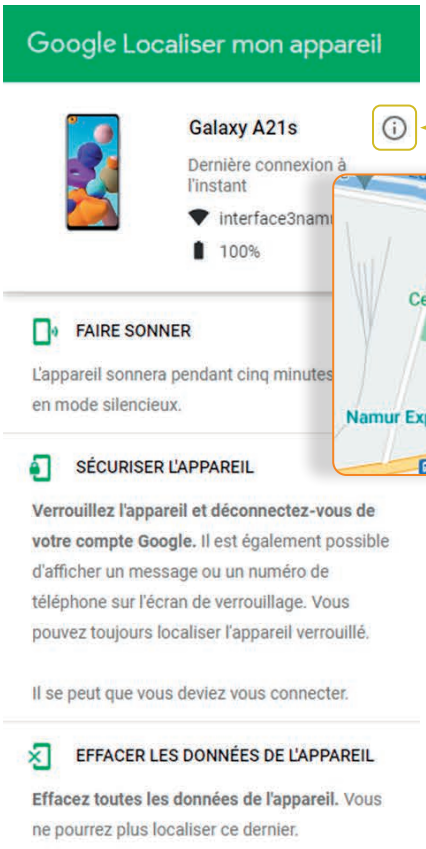
- L'option **« Localiser mon appareil »** du service Google est bien activée.



Pour activer l'option **« Localiser mon appareil »** :

1. Ouvrez les **paramètres** de votre smartphone Android (voir fiche 9.3.).
2. Accédez à la section **« Google (services Google) »**.
3. Sélectionnez **« Localiser mon appareil »**.
4. Assurez-vous que l'option est activée.

3. Localiser et/ou verrouiller son smartphone depuis un PC ou un autre smartphone



Informations provenant de l'appareil : Code IMEI

A. Pour localiser votre smartphone depuis un ordinateur ou un autre smartphone, rendez-vous sur le site google.com/android/find (voir fiche 3.2.).

B. Connectez-vous à votre compte Google avec votre **identifiant** (adresse e-mail) et votre **mot de passe**.

C. Apparait une liste des appareils associés à votre compte Google. Sélectionnez celui que vous souhaitez localiser.

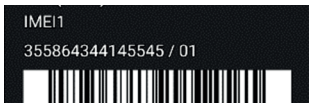
D. Sur la carte, vous verrez **l'emplacement actuel de votre appareil**. Si l'emplacement n'est pas disponible, cliquez / appuyez sur **«localiser maintenant»** pour actualiser la carte.

- **FAIRE SONNER** le smartphone à fort volume peut être utile si vous l'avez simplement égaré à la maison, par exemple.
- **SÉCURISER L'APPAREIL** verrouille le smartphone à distance et affiche un message ou un numéro de téléphone sur l'écran de verrouillage.
  Si quelqu'un trouve votre appareil, il pourra vous contacter grâce à l'information affichée sur l'écran.
- **EFFACER LES DONNÉES DE L'APPAREIL** : Toutes les données sont effacées (photos, contacts, messages, applications...).
  Si vous pensez que votre appareil a été perdu ou volé, cela évite que vos données personnelles tombent entre de mauvaises mains.

4. Verrouiller son smartphone grâce au numéro IMEI

L'IMEI (International Mobile Equipment Identity) est un numéro unique de **15 chiffres** attribué à chaque appareil mobile. Il identifie un appareil mobile sur le réseau de téléphonie mobile et **peut être utilisé pour bloquer un appareil volé ou perdu**.

L'IMEI peut être trouvé :



- Sur la boîte de votre appareil.
- En tapant ***#06#** sur le clavier du téléphone.
- Dans les **paramètres** (voir fiche 9.3.), en sélectionnant **« À propos du téléphone »** ou **« Informations sur le téléphone »**.
- Via android.com/find, en cliquant / appuyant sur **l'icone « i »** à côté de l'appareil (voir plus haut).

Connaître votre IMEI peut être utile en cas de perte ou de vol de votre appareil, car vous pouvez le fournir à votre opérateur de téléphonie mobile pour bloquer l'utilisation de votre appareil sur le réseau.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

Afin de garantir la sécurité de votre PC, il y a plusieurs gestes préventifs à réaliser régulièrement. Que ce soit le verrouillage du PC quand vous ne l'utilisez pas, les mots de passe, les mises à jour et d'autres bons réflexes, la protection de l'ordinateur commence avec vous.

1. Verrouillage de l'ordinateur

Comme pour un smartphone, il est possible de verrouiller le PC lorsque vous ne l'utilisez pas, sans l'éteindre, pour éviter que d'autres personnes y accèdent.
Quand vous verrouillez le PC, il est mis en veille : les programmes et fichiers restent ouverts et vous pouvez reprendre là où vous en étiez.

Le verrouillage peut se faire avec un mot de passe aux différentes formes :

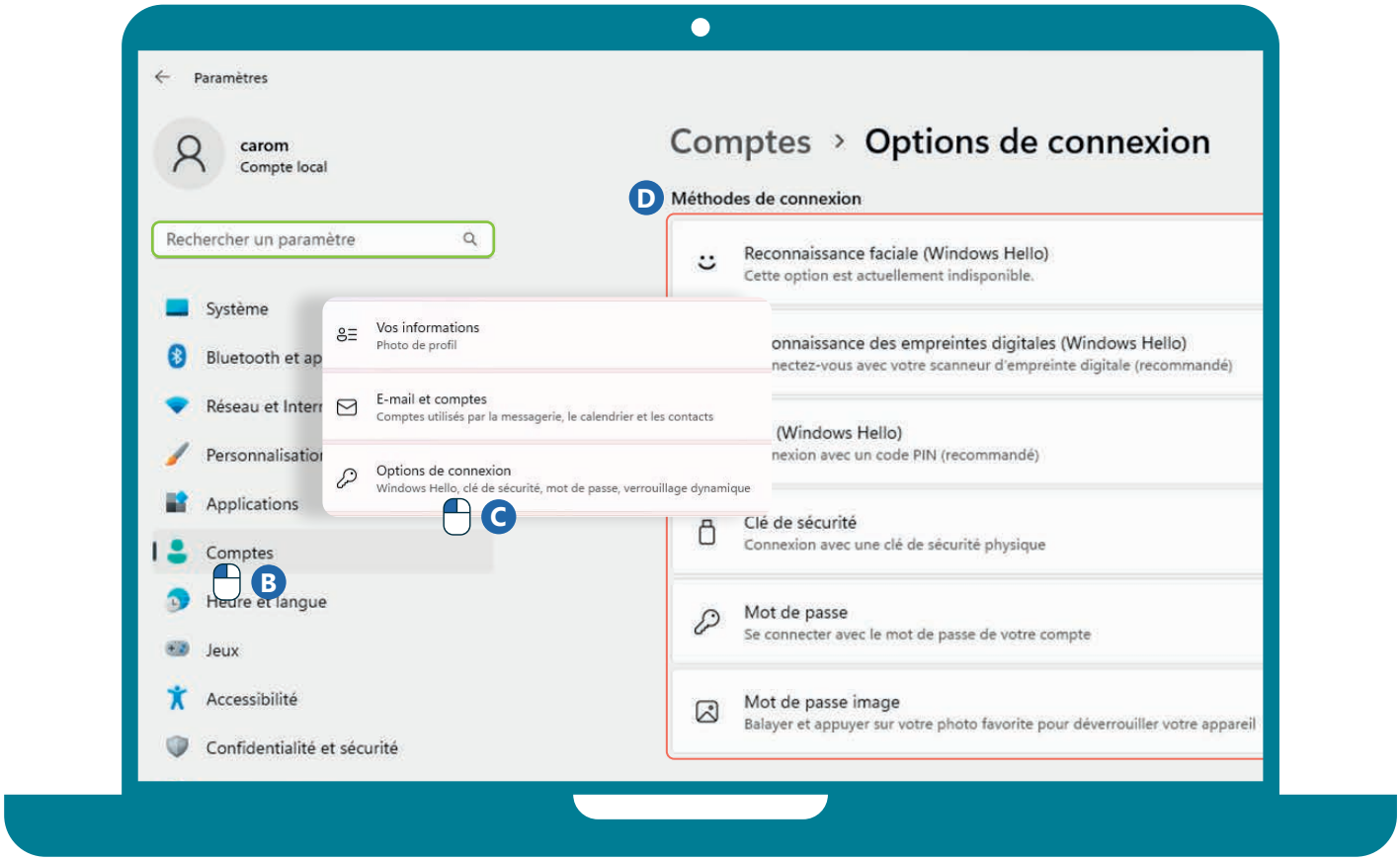
- **mot de passe**
- **code PIN**
- **reconnaissance faciale**
- **reconnaissance des empreintes**
- **image favorite**
- **clé de sécurité**

Les possibilités sont différentes selon la version de Windows installée sur la machine.
Vous pouvez aussi en configurer plusieurs, comme sur un smartphone.

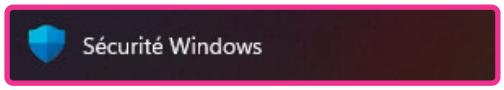
Pour changer le mot de passe, **appuyez en même temps** sur les touches **Ctrl + Alt + Suppr(Delete)** et choisissez « **Modifier un mot de passe** ».

Ctrl + Alt + Del

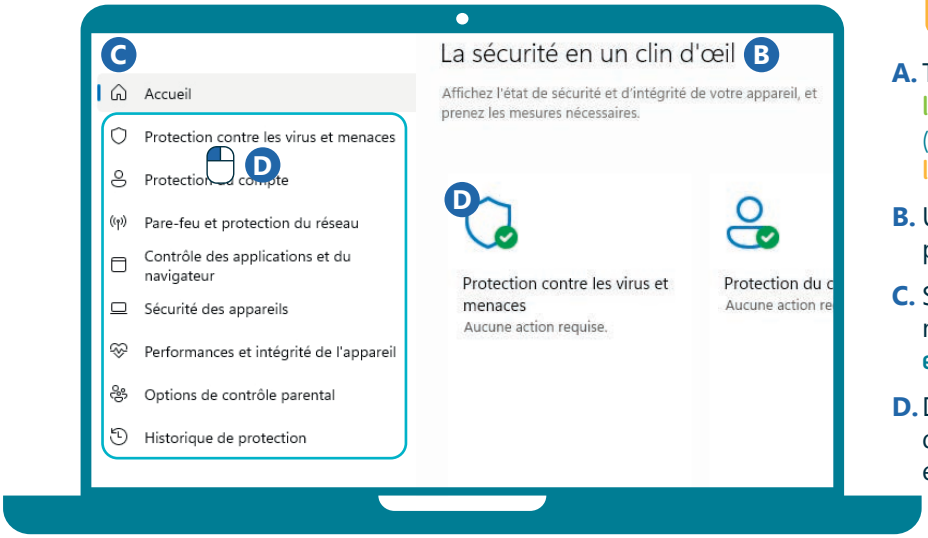
A. Allez dans les **paramètres** (voir fiche 9.3.).
B. Sélectionnez « **Comptes** ».
C. Dans ce menu, cliquez sur « **Options de connexion** ».
D. Vous pouvez désormais définir les différents modes de connexion.

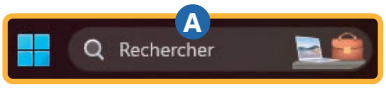


2. Entretien de base



Sur Internet, vous entendrez beaucoup parler de **virus**, **d'anti-virus**, de **protection contre les malwares**...
On peut vite s'y perdre. Mais saviez-vous que Windows a de base une protection pré-installée sur le PC ?





A. Tapez « **Sécurité Windows** » dans **la barre de recherche des paramètres** (voir recto) ou celle présente dans **la barre des tâches** (voir fiche 1.3.).

B. Un aperçu de l'état de sécurité se présente à vous.

C. Sur la gauche, **différents sous-menus**, notamment « **Protection contre les virus et menaces** ».

D. Dans ce sous-menu, apparaissent la date de la dernière analyse de sécurité et les paramètres de protection.

Vous pouvez aussi lancer des analyses :

- avec le bouton d'analyse rapide dans le menu de protection.
- via un logiciel à installer tel que **CCleaner** ou **Malwarebytes** (voir fiche 1.14.).

CCleaner et Malwarebytes sont des **freemium**, c'est-à-dire qu'ils proposent **une version de base gratuite** et des avantages payants (premium).

CCleaner

CCleaner permet de faire un nettoyage rapide du pc mais aussi de vos navigateurs, notamment l'historique de navigation et les cookies.

Malwarebytes permet de faire une analyse plus poussée pour voir s'il existe des malwares et autres logiciels malveillants.

3. Bons réflexes

Aucune protection logicielle n'étant infaillible, il est **important** en tant qu'utilisateur·trice de faire preuve de **vigilance.**

- **Vérifier la clé USB :** Ne branchez pas **n'importe quelle** clé USB donnée par **n'importe qui** sur le PC.
- **Attention aux sites visités :** Sur les sites de téléchargements illégaux (films, musique...), **le risque est grand de télécharger aussi des fichiers malveillants.**
- **Ne cliquez pas sur tous les liens dans les mails :** Assurez-vous que l'adresse du site est sécurisée et légitime. Ou rendez-vous sur le site **sans cliquer sur le lien dans l'email**.
- **Si c'est trop beau pour être vrai... :** En naviguant sur le Web, vous verrez des publicités pour des anti-virus miracles. Comme les crèmes de beauté, c'est souvent un mensonge déguisé. **Évitez de cliquer sur ces publicités et renseignez-vous sur les logiciels mentionnés avant de prendre une décision.** Une simple recherche pourra identifier si l'anti-virus miracle est un piège ou non.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

9. Sécuriser ses données sur PC

Dans le cadre privé ou professionnel, il est essentiel de sécuriser et sauvegarder ses données sensibles et fichiers importants pour éviter de les perdre suite à un problème matériel, des logiciels malveillants ou une mauvaise manipulation.
Attention, si vous utilisez un PC public, vous trouverez des conseils spécifiques au verso.

1. Sauvegarder ses données de son PC

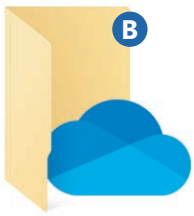
Chaque ordinateur possède un espace de stockage, un **« disque dur »** sur PC.
Y sont stockés le système d'exploitation (voir fiches 1.3.), les logiciels, vos fichiers,...
Par mesure de sécurité, il est conseillé de copier les fichiers sur d'autres supports de stockage comme une clé usb, un disque dur externe ou un espace de stockage en ligne (voir fiche 1.8.).

Une solution ne nécessitant pas d'investir dans du matériel parfois coûteux consiste à sauvegarder vos données en ligne, dans le cloud (voir fiche 5.1.). L'avantage étant **la quasi impossibilité d'une perte de données**. Il existe plusieurs offres selon les fournisseurs de stockage en ligne, gratuites ou payantes selon vos besoins (capacité de stockage).

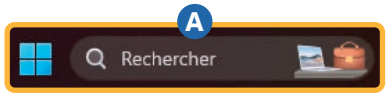
La bonne pratique est de sauvegarder vos fichiers les plus importants sur plusieurs supports. Cela permet, en cas de panne du disque dur par exemple, de pouvoir accéder aux fichiers sur un autre support.

Sauvegarder automatiquement ses données en ligne

Il est possible de sauvegarder automatiquement ses fichiers en activant **la synchronisation** avec votre espace de stockage en ligne (OneDrive, Google Drive...). Une copie de tous les fichiers synchronisés sera automatiquement créée en ligne.



L'application **OneDrive** étant déjà installée sur **Windows**, il vous suffit de :



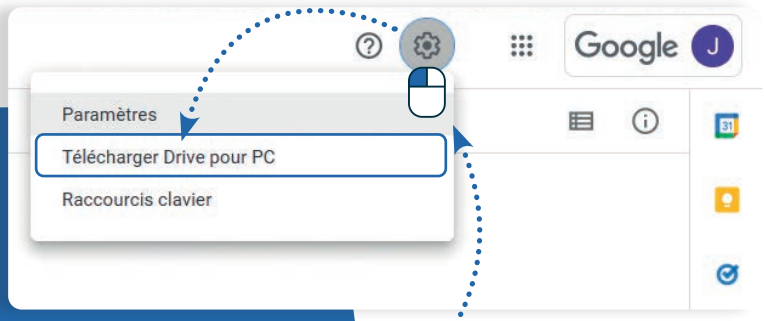
A. Taper **« OneDrive »** dans le champ de recherche de votre **barre des tâches**.

B. Puis sélectionner l'application **OneDrive**.

C. Vous connecter avec le compte que vous souhaitez utiliser pour **la synchronisation** et finalisez la configuration.

Si vous désirez utiliser un autre support de stockage en ligne tel que Google Drive, vous devez d'abord installer l'application :

- ✓ En allant sur le site internet https://www.google.com/intl/fr_be/drive/download/
- ✓ **Ou** en passant directement via votre espace **Google Drive** (voir fiche 5.3.) et en cliquant sur **les paramètres.**



2. Sauvegardez le contenu de son PC

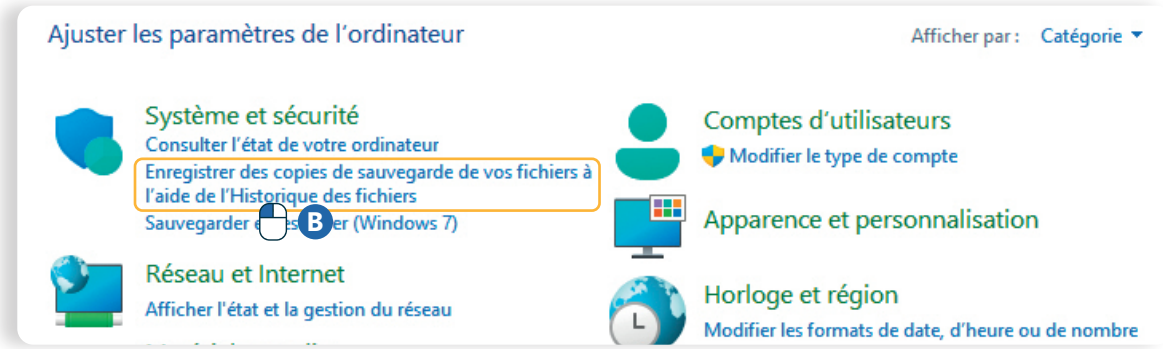
Il est également possible de sauvegarder l'ensemble de votre PC automatiquement. En créant par exemple **« une image système (backup) »**. C'est un moyen pratique d'avoir une sauvegarde complète de tout ce qui se trouve sur **le disque dur** du PC.

A. Dans la barre de recherche (en bas à gauche sur Windows 10, au milieu sur Windows 11), tapez **« Panneau de configuration »** et sélectionnez l'application.

B. Sélectionnez « **Historique des fichiers** » (dans Système et sécurité).

C. Sélectionnez le support de stockage pour accueillir l'image système. Si vous souhaitez faire cette sauvegarde sur un disque dur externe, veillez à ce qu'il soit bien connecté au PC et vérifiez qu'il y a suffisamment de place dessus.

Pensez à faire cette manipulation régulièrement !



3. Si vous utilisez un PC partagé

Si vous utilisez un PC **« public »** (dans un **E**space **P**ublic **N**umérique - **EPN**, à la bibliothèque...), les bonnes pratiques sont différentes pour protéger vos données.

- ✓ Adoptez les bonnes pratiques pour naviguer de manière plus sécurisée (voir fiche 3.6.).
- ✓ Pensez à **activer la navigation privée** (voir fiche 3.6.). Cette fonctionnalité permet, à la fermeture du navigateur, d'effacer toutes traces de votre navigation sur votre appareil (mots de passe, accès boite mails, historique de navigation, etc.).
- ✓ Surtout, **n'acceptez jamais d'enregistrer les mots de passe**.
- ✓ Si vous utilisez un espace de stockage en ligne pour sauvegarder vos fichiers, connectez-vous toujours via le navigateur (voir fiche 5.3.) et transférez vos fichiers manuellement (voir fiches 5.8. ou 5.9.). **Ne synchronisez jamais** les fichiers du PC avec votre espace de stockage en ligne.
- ✓ **Avant de quitter le PC**, supprimez les documents personnels que vous auriez pu enregistrer sur le PC.
- ✓ **Si vous n'avez pas activé la navigation privée**, supprimez votre **historique de navigation** (menu du navigateur) et pensez à vous déconnecter de tous les services auxquels vous vous êtes connecté·e.
- ✓ **Fermez votre session** (bouton de déconnexion de session du menu démarrer).
- ✓ **Avant de partir**, n'oubliez pas de récupérer vos documents, si vous avez utilisé une imprimante.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

10. Protéger ses données privées

Une donnée personnelle est toute information qui se rapporte à une personne physique identifiée ou identifiable : nom, adresse postale, e-mail, numéro de téléphone, données de localisation… Ces données peuvent être collectées lors de l'utilisation de sites web, d'applications mobiles ou de réseaux sociaux.

Pour éviter que ces informations ne soient partagées avec des tiers, individus ou des organisations non autorisées, utilisez les **paramètres de confidentialité**.

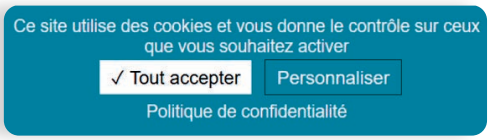
1. Les cookies ?

Lorsque vous visitez un site web, un petit fichier texte appelé **« cookie »** peut être enregistré sur votre appareil. Les cookies ne sont pas dangereux pour votre appareil. Mais ils peuvent contenir des informations personnelles et être utilisés à des fins diverses :

- **Cookies de session** : conservent votre panier quand vous faites des achats en ligne.
- **Cookies techniques :** sont nécessaires pour que le site fonctionne correctement.
- **Cookies permanents :** retiennent vos noms d'utilisateurs, vos mots de passe, vos coordonnées ou vos préférences linguistiques. Ce sont eux qui vous permettent de remplir instantanément un formulaire.
- **Cookies analytiques :** collectent vos habitudes d'utilisation d'un site pour permettre au responsable du site d'améliorer l'expérience des utilisateurs.
- **Les cookies tiers** sont là pour scruter votre comportement sur le web (par exemple via votre historique de navigation) dans l'unique but de faire apparaitre des publicités ciblées sur vos habitudes . Ces données sont souvent utilisées par les annonceurs pour cibler et personnaliser les publicités sur les sites que vous visitez.

Les propriétaires de sites Web doivent vous informer sur l'utilisation de ces cookies.

Vous devez donner votre consentement de manière explicite et consciente à l'utilisation des cookies. Via la fenêtre **« Accepter les cookies »**, vous pouvez choisir quels cookies vous acceptez et ainsi mieux contrôler les données collectées et leur utilisation.



2. Le RGPD, qu'est-ce que c'est ?

Le **Règlement Général sur la Protection des Données (RGPD)** est un texte juridique qui encadre le **traitement des données personnelles** en Europe. Il doit être appliqué par toute organisation qui traite des données qui permettent d'identifier une personne physique. Et en tant que citoyen·e, **vous avez notamment le droit** de :

- **Être informé·e** sur **quelles données sont collectées**, par **qui**, dans quel **but** et pour combien de **temps**
- Avoir **accès** à vos données en possession d'une organisation
- Demander à ce que vos **données** soient **rectifiées ou supprimées**

Toute organisation doit avoir un responsable du traitement des données que vous pouvez contacter pour exercer vos droits. Sur un **site Web**, vous trouverez généralement son nom dans la partie **vie privée et confidentialité** ou **politique de protection** tout en bas du site.

Pour mieux comprendre comment le RGPD protège votre vie privée, nous vous conseillons la vidéo d'explication de l'Autorité de Protection des Données, APD, qui veille à la protection de la vie privée dans le traitement des données personnelles.
Site Web de APD : www.autoriteprotectiondonnees.be

Pour voir la vidéo, scannez le QR code !

3. Vie privée

Il existe des **extensions** libres permettant de protéger ses données privées et de bloquer les cookies des pages web visitées.

Extension (voir fiche 3.8.) **:** petit programme qui peut être ajouté à son navigateur (Google Chrome, Mozilla Firefox, etc.) et qui lui apportera de nouvelles fonctionnalités.

Ghostery et **AdBlock** sont des extensions de navigateurs permettant aux utilisateurs de bloquer les cookies publicitaires ou indésirables sur les sites web qu'ils visitent. Comme beaucoup d'extensions, il existe :

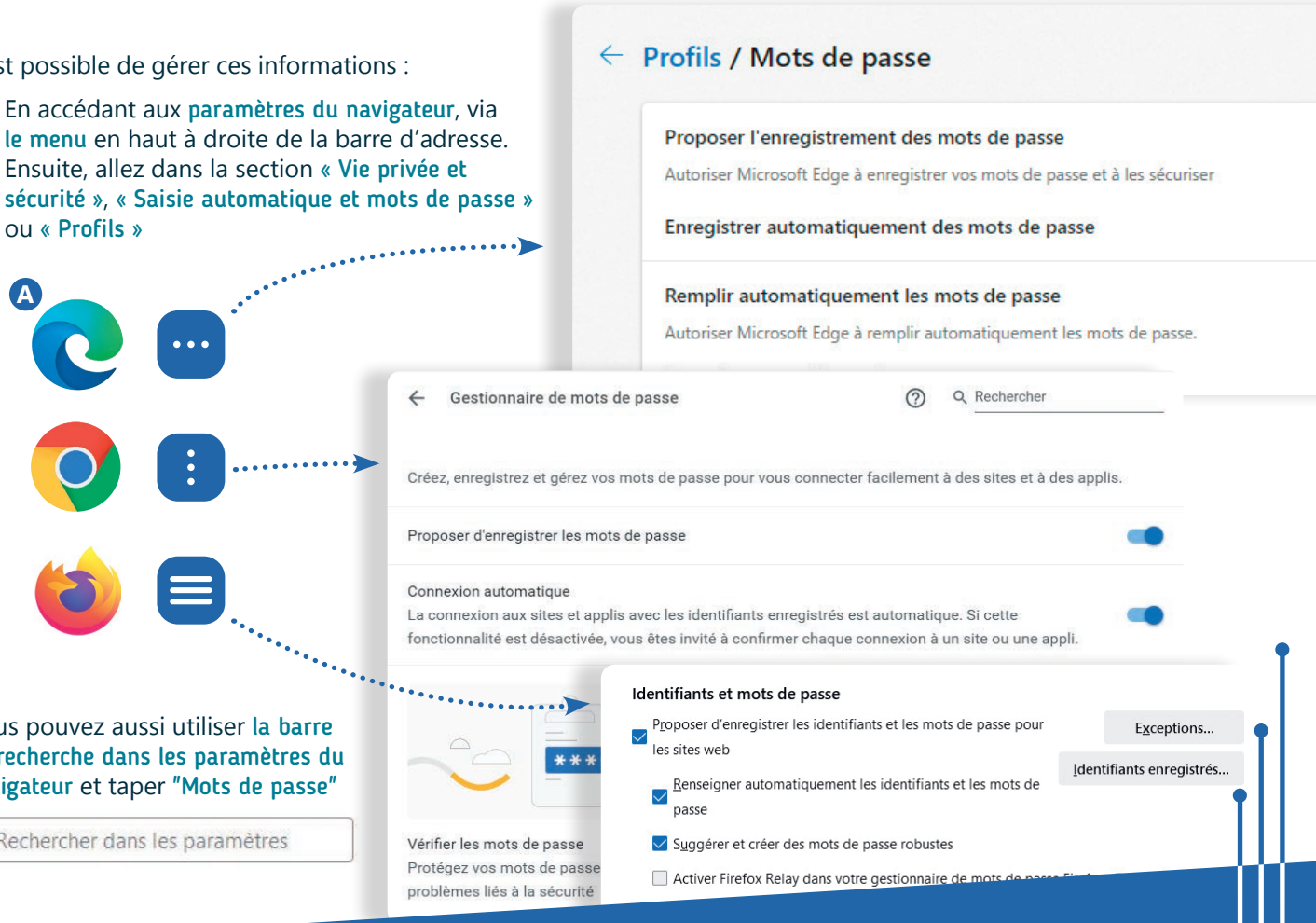
- **une version gratuite** offrant les principales fonctionnalités qui seront suffisantes pour la plupart des utilisateurs.
- **une version payante** donnant accès à des fonctionnalités avancées.

4. Enregistrement automatique du mot de passe

Lorsque vous vous connectez sur un site Web, le navigateur peut vous proposer de sauvegarder vos informations de connexion. Si cela facilite vos connexions futures, cela signifie également que si quelqu'un accède à votre appareil, il pourra accéder à vos comptes sans avoir besoin de votre mot de passe. **Pour éviter cela, il est recommandé de ne pas autoriser la sauvegarde de vos informations de connexion sur les appareils qui ne vous appartiennent pas ou qui sont partagés avec d'autres personnes.**

Il est possible de gérer ces informations :

A. En accédant aux **paramètres du navigateur**, via **le menu** en haut à droite de la barre d'adresse.
B. Ensuite, allez dans la section **« Vie privée et sécurité »**, **« Saisie automatique et mots de passe »** ou **« Profils »**



Vous pouvez aussi utiliser **la barre de recherche dans les paramètres du navigateur** et taper **"Mots de passe"**

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

D'une démarche à quatre pattes jusqu'à tenir sur nos deux pieds, le corps humain n'a cessé d'évoluer. Notre utilisation des technologies peut aussi avoir un impact sur notre corps entrainant douleurs, tendinites ou déformations comme la « bosse du smartphone » qui modifie votre auriculaire...

D'un point de vue **ergonomique**, il y a de précieux conseils pour éviter les douleurs au dos, aux poignets, au cou... conséquences de nos usages numériques et de nos mauvaises postures.

1. Bien se positionner face à un PC

Les pieds au sol, le dos soutenu et la tête droite :

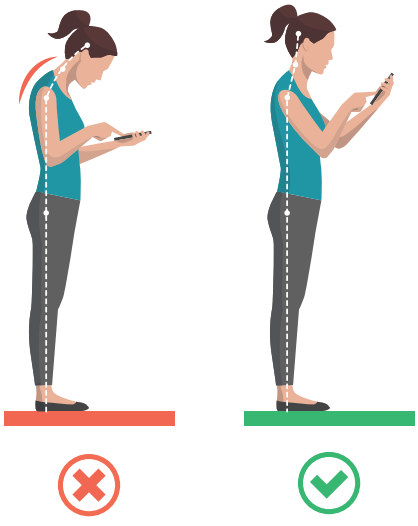
- Les pieds doivent être bien au sol et les cuisses parallèles au sol. Utilisez un repose-pied pour avoir les pieds correctement positionnés.
- Le dos doit être soutenu par le dossier. Adaptez votre position grâce à une chaise réglable.
- Pour protéger la nuque, la tête doit rester droite, le regard à l'horizontal ou légèrement vers le bas avec l'écran disposé à une distance d'un bras.

Position du clavier et de la souris pour épargner les poignets :

- Le niveau du clavier doit être légèrement en dessous du niveau des coudes, et idéalement à 10 cm du bord du bureau. Une fois les mains sur le clavier, les bras forment un angle de 90° au niveau des coudes.
- La souris doit être disposée à proximité du clavier. Pour réduire la pression sur les poignets, il existe des reposes poignets ou encore des souris ergonomiques.

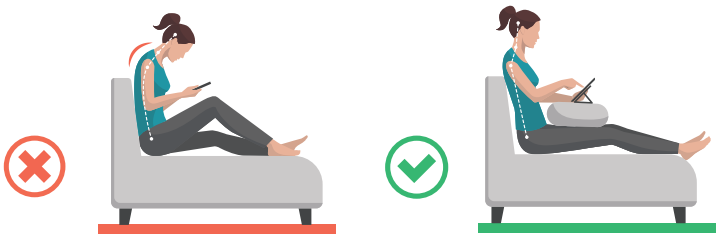
2. Bien se positionner avec son smartphone

La position la plus problématique avec l'utilisation du téléphone est lorsque la tête est penchée et le bras tendu de façon prolongé.



Voici quelques conseils pour améliorer votre posture :

- Veillez à ne pas garder votre tête penchée trop longtemps. Changez de position régulièrement. Pensez à redresser votre tête.
- Adaptez votre position pour soulager vos bras et vos poignets. Par exemple, plutôt que d'avoir vos bras tendus, vous pouvez consulter votre téléphone sur une table.
- N'utilisez pas que votre pouce pour naviguer sur votre téléphone, utilisez aussi votre index. Cela permet de ne pas trop solliciter votre pouce ni vos poignets.

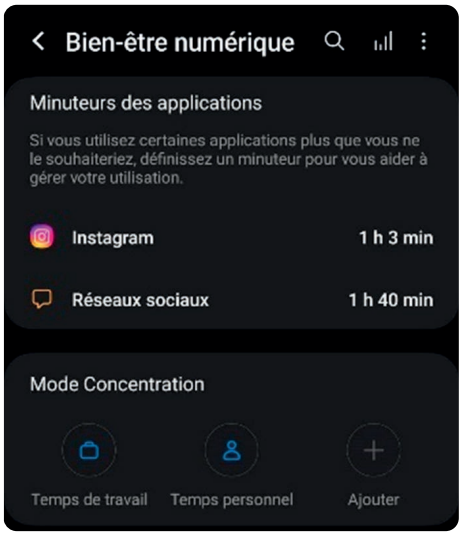


3. Préserver sa santé mentale

Au-delà de la santé physique, la santé mentale peut également être impactée par la technologie.

Au travail comme à la maison l'accès permanent à Internet et à son flot d'information peut générer stress, troubles du sommeil et de l'attention, peur de passer à côté d'une information importante alias FOMO (Fear Of Missing Out) ou encore de la sécheresse oculaire... Être hyperconnecté·e pour augmenter son efficacité au quotidien peut donc finir par produire le contraire.

Au travail, pour prévenir les risques d'addiction numérique et le stress lié à la connexion permanente, il existe le **droit à la déconnexion**.



Quel que soit le contexte, prendre conscience de ses usages et de la dépendance au numérique est le premier pas pour un mieux-être avec le numérique.

Des outils existent pour modérer sa consommation :

- Dans les options d'un smartphone Android, vous pouvez retrouver un menu « **Bien-être numérique** » où vous pouvez consulter votre temps d'écran jour par jour et semaine par semaine. Vous pouvez y définir un objectif de temps d'écran. Il existe également « **un mode concentration** » qui bloque toutes les applications sélectionnées et leurs notifications.
- Sur le PC, l'option « **assistant de concentration** » bloque les notifications des applications sélectionnées durant le temps souhaité.

4. Le numérique au service de la santé

Bien que la technologie comporte des risques pour notre bien-être, elle peut toutefois être utilisée au service de la santé.

De plus en plus de smartphones proposent une application qui comptabilise le nombre de pas effectués dans la journée. Il est possible de voir combien de kilomètres ont été parcourus et de se fixer un objectif journalier.

L'application « **Totemus** » vous propose des promenades rythmées d'énigmes. A chaque promenade, vous gagnez des totems qui peuvent être échangés contre des cadeaux.

L'application « **Decathlon Coach** » permet de suivre des séances de sport à la carte ou de planifier un programme de coaching selon vos affinités et votre temps disponible. Si vous avez un compte décathlon, vous pouvez gagner des points de fidélités selon les actions que vous réalisez.

Des aides et des ressources en lien avec **la méditation**, **la relaxation** peuvent être accessibles en faisant une petite recherche. Sur YouTube, vous pouvez retrouver une gigantesque bibliothèque de vidéos sur ces thèmatiques.

L'application « **RespiRelax+** » vous propose de reprendre le contrôle de votre respiration.

L'application « **Petit BamBou** » vous propose de découvrir la méditation de manière simple.

Petit BamBou

www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin

12. Utilisation plus verte du numérique

Gérer ses mails de manière écologique (voir fiche 4.8.) est un bon début ! Voici quelques astuces pour avoir un impact plus important sur la diminution des émissions de CO2 et la consommation de matières premières. Il s'agit des 4R : réduire, reconditionner, réparer et recycler.

1. Réduire votre quantité de matériel

Le matériel le moins polluant, c'est celui que l'on n'achète pas (et donc que l'on ne fabrique pas). L'idée n'est pas de se priver d'un matériel utile, mais plutôt de réfléchir à ses besoins et conditions d'utilisation. Cela permet souvent d'éviter un achat inutile.

- Se rendre dans un magasin de photocopie au lieu d'acheter une imprimante.
- Emprunter un GPS pour votre week-end à la mer.
- Louer un projecteur pour regarder la finale de la coupe du monde entre amis...

En y réfléchissant bien, l'achat n'est pas toujours obligatoire !

Savez-vous qu'il faut un peu plus de **800kg** de matières premières pour construire un **ordinateur portable de 2kg** et un peu plus de **200kg pour un smartphone de 300g** ? (chiffres de l'ADEME)

2. Reconditionner et offrir une deuxième vie au matériel numérique

Et si l'achat vous semble le meilleur choix, pensez **aux alternatives à l'achat neuf** : vous pouvez par exemple acheter un smartphone reconditionné sur asmartworld.be ou aller dans un magasin **Oxfam** (oxfambelgique.be/shop-finder) pour trouver un PC d'occasion. **Un bon geste pour la planète et pour le portefeuille : ces appareils reconditionnés sont moins chers et garantis minimum un an !**

Revendez ou donnez vos « vieux » appareils toujours fonctionnels et donnez-leur une deuxième vie ! L'application ObyO (obyo.be) permet par exemple d'estimer le prix de reprise de votre smartphone **« obsolète »**.

Obsolescence programmée, obsolescence psychologique ?

À côté de l'**obsolescence programmée** (réduction délibérée de la durée de vie d'un appareil par le fabriquant), il y a aussi l'**obsolescence psychologique**. Par exemple, votre smartphone acheté il y a un an peut sembler complètement démodé. Les campagnes marketing vous poussent à abandonner votre appareil avec des offres «à 1€» et des arguments convaincants pour obtenir le dernier cri qui impressionnera vos amis. Si vous optez pour un nouvel appareil, pensez à **revendre** ou à donner votre «vieux» smartphone encore fonctionnel.

3. Réparer dès que c'est possible

Pour éviter les réparations, le bon entretien matériel et logiciel de vos appareils numériques est primordial (voir notamment les fiches 9.1. à 9.10.).
Mais parfois vous n'avez pas le choix :

- Ecran cassé après une chute
- Café dans le clavier
- Batterie qui ne charge plus...

Réparer permet de prolonger la vie de votre appareil et d'éviter ainsi un nouvel achat.

Des sites, comme sosav.be ou fr.ifixit.com, vous permettent de tenter la réparation par vous-même. Vous pouvez aussi vous adresser à un **repair café** (repairtogether.be) pour être conseillé·e sur la pièce à acheter et pour confier la réparation à un bricoleur plus expérimenté.

4. Recycler le matériel hors d'usage

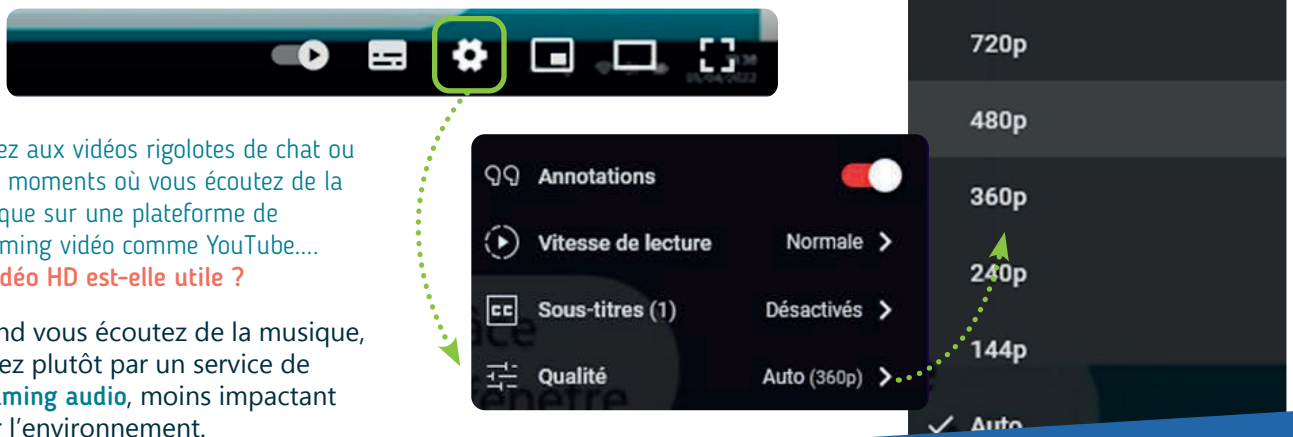
Si votre appareil ne fonctionne plus, il est important de le faire entrer dans une filière de recyclage officielle. Les PC, smartphones et autres matériels numériques sont des déchets d'équipements électriques et électroniques (DEEE), vous devez donc les emmener au parc à conteneur pour le recyclage.

Ne laissez pas trainer dans vos tiroirs vos anciens appareils !

5. Ecouter de la vidéo en HD, est-ce bien raisonnable ?

Nous regardons des vidéos, films au quotidien. Cela constitue **80 %** des **usages mondiaux d'Internet** (chiffres du Shift Project 2019). L'idée n'est pas de se passer de ce plaisir, mais de le faire de manière plus responsable.

Pensez par exemple à **réduire la qualité de la vidéo** à **480p** ou **360p** quand celle-ci ne nécessite pas une image en haute définition.



Pensez aux vidéos rigolotes de chat ou à ces moments où vous écoutez de la musique sur une plateforme de streaming vidéo comme YouTube....
La vidéo HD est-elle utile ?

Quand vous écoutez de la musique, passez plutôt par un service de **streaming audio**, moins impactant pour l'environnement.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin