USAGES **RESPONSABLES** ET **SECURISÉS** DES **PRODUITS NUMÉRIQUES**

Union des Agricultrices Wallonnes
&
Centre provincial de l'agriculture et de la ruralité

N Vanassche
www.nathalie.vanasche.be

OBJECTIF 1

REMPLIR EFFICACEMENT MES FORMULAIRES EN LIGNE

- Découvrir les champs de formulaire
- Gérer les captchas
- Les cases pré-cochées
- Accepter les conditions d'utilisation

OBJECTIF 2

PROTÉGER MES DONNÉES PERSONNELLES

- Qu'est ce que je laisse derrière moi ?
- Comment gérer mes cookies ?
- Bonnes pratiques
- Que font Facebook et Google de mes données ?

PROTÉGER MES DONNÉES PERSONNELLES SUR FACEBOOK > PARAMÉTRAGE

OBJECTIF 3

UTILISER LES SERVICES ADMINISTRATIFS EN LIGNE

- Qu'est ce que CSAM ?
- Me connecter à un service en ligne avec ma CI
- Configurer Itsme
- Me connecter à un service en ligne avec Itsme

OBJECTIF 4

LES MOTS DE PASSE

- Qu'est ce qu'un mot de passe sécurisé ?
- Créer un mot de passe sécurisé (et m'en rappeler !)
- Utiliser un gestionnaire de mots de passe
- Pratiquer l'authentification à deux facteurs

OBJECTIF 5

LA SÉCURITÉ SUR INTERNET

- Quelles sont les techniques des pirates informatiques ?
- Que faire si ... Analysons ensemble plusieurs cas concrets
- Qu'est ce que le pishing ? Comme le reconnaître ?
- Bonnes attitudes pour ne pas me faire avoir

OBJECTIF 6

ACHETER SUR INTERNET

- Quel produit sur quel site ?
- Comment faire des achats en ligne en toute sécurité ?
- Comment payer en ligne ?
- Gros plan sur l'application Payconiq

OBJECTIF 7

PROTÉGER SON SMARTPHONE

- Sécuriser l'accès à son smartphone
- Gérer les permissions des applications
- Éviter les logiciels malveillants

OBJECTIF 8

LE CYBERHARCÈLEMENT

- Comment réagir face au cyberharcèlement ?
- Conseils pratiques pour bloquer, signaler, et se protéger en ligne.

EXERCICES PRATIQUES

OBJECTIF 1

REMPLIR EFFICACEMENT MES FORMULAIRES EN LIGNE

- Découvrir les champs de formulaire
- Gérer les captchas
- Les cases pré-cochées
- Accepter les conditions d'utilisation

Remplir des formulaires en ligne est devenu une tâche courante, que ce soit pour créer un compte, faire un achat, ou accéder à divers services.

Cependant, il est important de savoir naviguer parmi les différents types de champs et de comprendre les éléments de sécurité tels que les captchas. De plus, la gestion des cases pré-cochées et la lecture attentive des conditions d'utilisation sont essentielles pour protéger nos informations personnelles et éviter des engagements involontaires.

Dans cette section, nous apprendrons à remplir efficacement et en toute sécurité nos formulaires en ligne

Fiche résumé

Comment remplir un formulaire en ligne ?

Les types de champs

Les champs à choix unique

- ○ Choix 1
- ○ Choix 2
- ◉ Choix 3

Choix 1
Choix 2
Choix 3

Le champ à choix multiples

- ☐ Option 1
- ☑ Option 2
- ☑ Option 3

Les champs à remplir au clavier

abcd

Mot de passe

••••••••

Chiffres

3

abcd
b
c
d

N'oubliez pas de cliquer sur

Envoyer

Pour que vos réponses soient prises en compte !

Les contraintes de champs

Certains champs texte n'acceptent que les réponses d'un format spécifique :

Dates

jj/mm/aaaa

Adresse mail

nom@boitemail.org

Prix

45 . 89 €

Euros Centimes

Certains champs doivent être obligatoirement remplis avant d'envoyer le formulaire :

* **Champ texte obligatoire**

*Ils seront souvent marqués d'une étoile * ou d'un mot comme « requis »*

Les tests de sécurité

Certains formulaires vous demanderont de passer des petits tests avant d'envoyer vos réponses :

Ces tests permettent aux sites de se protéger contre les programmes qui remplissent automatiquement leurs formulaires avec du contenu intempestif.

Les cases d'utilisation des données

☑ Je souhaite recevoir la newsletter

☑ J'accepte que mes données soient transmises à des services tiers

Vous n'êtes pas obligé de laisser ces cases cochées si vous ne voulez pas.

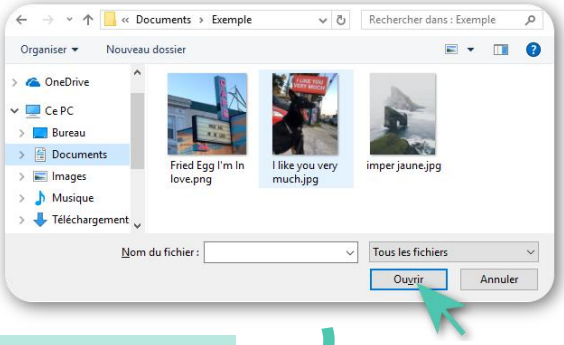
☐ J'accepte les conditions d'utilisation de ce site

Par contre, vous devrez cocher cette case pour envoyer le formulaire.

Ajouter un fichier

Choisissez un fichier

Cliquez sur le bouton.



Dans la fenêtre explorateur qui vient de s'ouvrir, trouvez votre fichier et cliquez dessus.

Puis cliquez sur « Ouvrir ».

Choisissez un fichier I like yo…much.jpg

À retenir
Remplir efficacement mes formulaires en ligne

Découvrir les champs de formulaire

Un formulaire en ligne est composé de **différents types de champs**, tels que des zones de texte, des cases à cocher ou des menus déroulants. Il est important de **bien comprendre ce que chaque champ** demande afin de ne pas commettre d'erreurs.

Gérer les captchas

Les captchas sont utilisés **pour vérifier que vous êtes bien un humain et non un robot**. Ils peuvent se présenter sous forme de mots à recopier, de cases à cocher ou d'identification d'images. Il est important de **bien comprendre comment les remplir** pour éviter des blocages lors de l'inscription ou de la connexion.

Les cases pré-cochées

Certaines cases sur les formulaires peuvent être pré-cochées, souvent pour s'inscrire à des newsletters ou accepter des offres commerciales. **Prenez toujours le temps de les vérifier avant de soumettre un formulaire** pour éviter des engagements non voulus.

Accepter les conditions d'utilisation

Avant de valider un formulaire, il est important de **lire les conditions d'utilisation des services ou sites web**. Ces conditions détaillent ce que l'entreprise peut faire de vos données personnelles et de vos informations.

Bonnes pratiques à retenir :

- **Lisez toujours chaque champ attentivement.**
- **Soyez vigilant face aux captchas et suivez les instructions.**
- **Désélectionnez les cases pré-cochées si vous ne souhaitez pas accepter des offres.**
- **Lisez les conditions d'utilisation avant d'accepter quoi que ce soit.**

OBJECTIF 2

PROTÉGER MES DONNÉES PERSONNELLES

- Qu'est ce que je laisse derrière moi ?
- Comment gérer mes cookies ?
- Bonnes pratiques
- Que font Facebook et Google de mes données ?

PROTÉGER MES DONNÉES PERSONNELLES SUR FACEBOOK > PARAMÉTRAGE

Chaque fois que nous naviguons sur Internet, **nous laissons des traces de notre activité** : informations personnelles, historiques de navigation, ou encore préférences.
Apprendre à gérer ces données est essentiel pour protéger notre vie privée.

Dans cette section, nous verrons ce que nous laissons derrière nous, comment gérer les cookies pour mieux contrôler ce qui est collecté, et **adopter des bonnes pratiques**.
Nous aborderons également l'utilisation de nos données par des entreprises comme Facebook et Google, afin de mieux comprendre **les enjeux de confidentialité dans le monde numérique**.

Fiche résumé
Comment protéger ses données personnelles ?

Où laissez-vous des informations sur vous sur internet ?

Chaque fois que vous cherchez une information sur internet ou que vous visitez un site, vous laissez des informations sur vous. On les appelle des “données personnelles” : elles permettent de vous identifier.

Sur les **réseaux sociaux** : quand vous publiez une photo, commentez un message, regardez une vidéo…

Dans un **moteur de recherche** : quand vous tapez des mots clés

Sur un **site internet** : quand vous visitez des pages, lisez un article…

Dans un **formulaire en ligne** pour créer un compte ou faire un achat : quand vous écrivez votre nom, prénom…

Sur une **application mobile** : quand vous l’autorisez à vous “géolocaliser” (c’est à dire, savoir où vous êtes).

Pourquoi ces informations sont-elles précieuses ?

Ces informations sont précieuses car elles permettent à des entreprises (réseaux sociaux, moteurs de recherche, sites, applications…) de savoir qui vous êtes et ce qui vous intéresse pour vous faire acheter.

Comment les entreprises utilisent-elles ces informations ?

1. Certaines entreprises, comme Google et Facebook, à qui vous avez donné des centaines d’informations sur vous, vous montrent des publicités qui correspondent à vos goûts sur les sites que vous visitez et sur Facebook. D’autres entreprises les paient pour montrer leurs publicités aux personnes intéressées. On appelle ça des **publicités “ciblées”**.

2. D’autres entreprises se servent de ces informations pour **vous montrer et vous faire acheter des objets qui ressemblent à ce que vous aimez** chaque fois que vous retournez sur leurs sites.

Comment protéger ses informations personnelles ?

1 **Refuser les cookies**

Un cookie est un fichier que les sites internet que vous visitez enregistrent sur votre ordinateur. Il contient des informations sur vous pour vous permettre de naviguer plus facilement sur ces sites. Certains cookies sont nécessaires pour que le site fonctionne bien. Mais d'autres enregistrent tout ce que vous faites pour vous montrer des publicités ciblées. Mieux vaut les refuser !

2 **Utiliser les options de son navigateur internet**

Dans les paramètres de votre navigateur, vous pouvez effacer les cookies que des entreprises ont enregistrés sur votre ordinateur. Vous pouvez aussi utiliser une fenêtre de navigation privée pour aller sur internet : elle efface automatiquement les cookies quand vous la fermez.

3 **Bien choisir son moteur de recherche**

Contrairement à Google, DuckDuckGo et Ecosia n'enregistrent pas d'informations sur vous pour gagner de l'argent. Pour les utiliser, tapez leur nom dans votre moteur de recherche actuel et cliquez sur le lien vers leur site (par exemple, « duckduckgo.com"). Utilisez la barre de recherche qui s'affiche pour faire vos recherches.

4 **Ne pas tout dire... ou mentir !**

Pour créer un compte sur un site ou une application, remplissez un formulaire. Ne vous inscrivez pas avec votre compte Facebook. Dans le formulaire, ne remplissez que les cases obligatoires, avec une étoile. Si vous créez un compte pour jouer à un jeu, vous pouvez écrire un faux nom, prénom, adresse...

5 **Lire les conditions avant de s'engager**

A la fin du formulaire pour créer un compte, lisez les conditions générales d'utilisation pour savoir comment l'entreprise utilise des informations sur vous.

6 **Paramétrer son compte**

Dans les paramètres de confidentialité de votre compte sur Facebook, vous pouvez choisir qui peut voir vos informations personnelles, comment le site peut les utiliser...

7 **En cas de besoin, utiliser son droit à l'oubli**

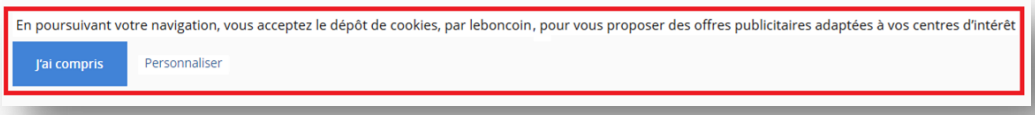
La loi vous donne des droits pour contrôler l'utilisation de vos informations par des entreprises. Par exemple, vous pouvez demander à un site internet d'effacer une photo de vous.

Whatsapp, l'application mobile pour envoyer des messages à des personnes dans d'autres pays, appartient à Facebook. **Youtube**, lui, appartient à Google. Donc si vous les utilisez, vous donnez des informations sur vous à Facebook et Google !

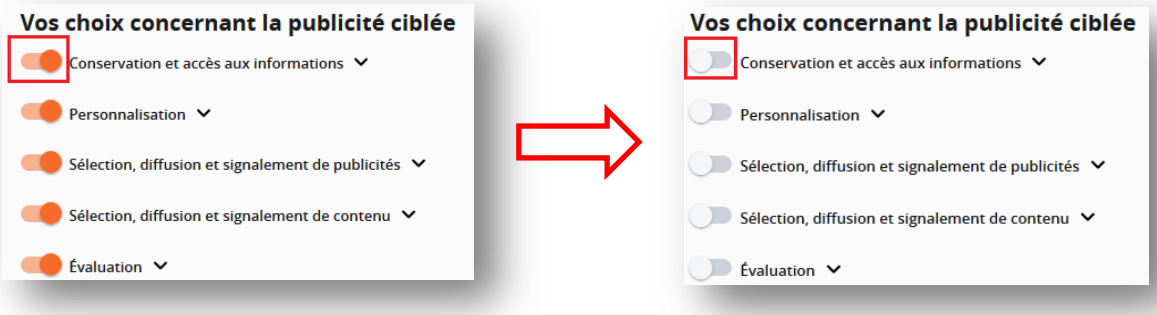
Fiche pratique n°1
Comment refuser et effacer des cookies ?

Comment refuser des cookies ?

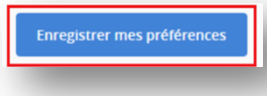
1 Quand vous allez sur un site internet, un message vous demande si vous acceptez que le site utilise des cookies pour enregistrer des informations sur vous. Cliquez sur “Personnaliser”.



2 La liste des cookies utilisés par le site s'affiche. Cliquez sur le bouton orange à gauche du nom de chaque cookie pour le désactiver (1). Le bouton devient gris : le cookie est désactivé. Sachez que certains cookies sont nécessaires pour que le site fonctionne bien. Ils ne sont pas utilisés pour vous vendre des produits. Vous ne pouvez pas les refuser.



3 Cliquez sur “**Enregistrer mes préférences**”. Vous pouvez maintenant naviguer sur le site en toute sécurité !



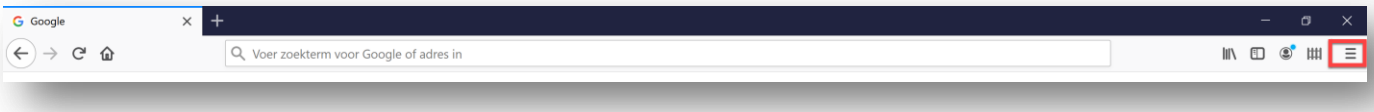
Comment effacer des cookies ?

Nous vous montrons comment effacer des cookies dans les paramètres de Mozilla Firefox sur votre ordinateur. Vous pouvez faire les mêmes gestes sur d’autres navigateurs (Google Chrome, Safari…).

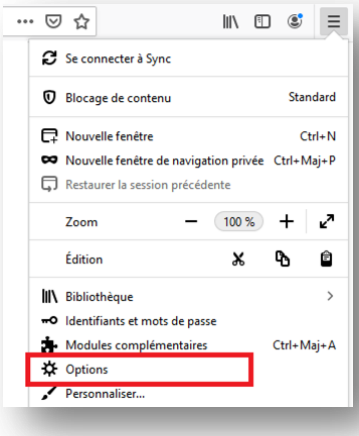
Si vous effacez les cookies sur votre ordinateur, vous serez déconnectez de vos comptes en ligne et votre navigateur ne se souviendra plus de vos mots de passe. Avant d’effacer les cookies, vérifiez que vous connaissez les mots de passe de vos comptes (Facebook, Forem, Actiris,..).

1 Sur le bureau de votre ordinateur, double cliquez sur l’icône de votre navigateur.

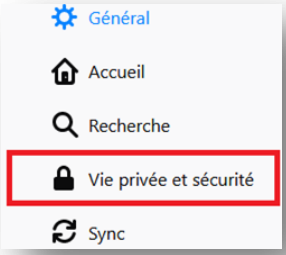
2 Cliquez sur l’icône en haut à droite de la page d’accueil pour afficher le menu de votre navigateur.



3 Dans le menu, cliquez sur “**Options**”.



4 Dans le menu de gauche, cliquez sur “**Vie privée et sécurité**”.

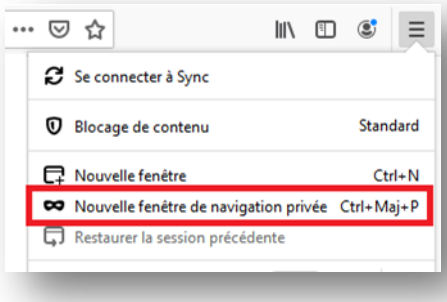


5 En-dessous du titre "**cookies et données de sites**" :

(1) Cliquez sur “Effacer les données” pour effacez tous les cookies enregistrés sur votre ordinateur, puis, dans la fenêtre qui s’affiche, cliquez sur "effacer" pour confirmer. Faites ce geste régulièrement.

(2) Vous pouvez aussi cliquer sur “**Supprimer les cookies et les données des sites à la fermeture de Firefox**". Les cookies seront automatiquement effacés chaque fois que vous fermerez la fenêtre de votre navigateur pour quitter internet.

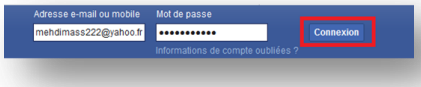
6 Vous pouvez aussi utiliser une fenêtre de navigation privée pour aller sur internet en cliquant sur “**Nouvelle fenêtre de navigation privée**" sur la page d’accueil de votre navigateur.



Fiche pratique n°2
Comment paramétrer son compte Facebook ?

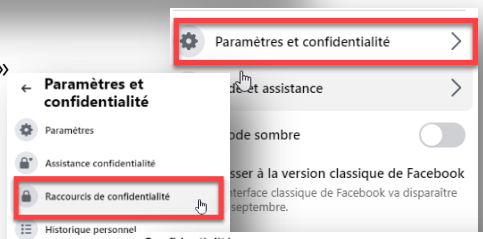
Ce tuto vous aidera à paramétrer votre compte Facebook pour choisir qui peut voir vos informations personnelles. Vous pouvez faire les mêmes gestes pour vos compte personnels en ligne ou sur une application mobile.

1. Allez sur le site “Facebook”. Sur la page d’accueil, écrivez votre adresse mail et votre mot de passe puis cliquez sur “**Connexion**” pour vous connecter à votre compte.



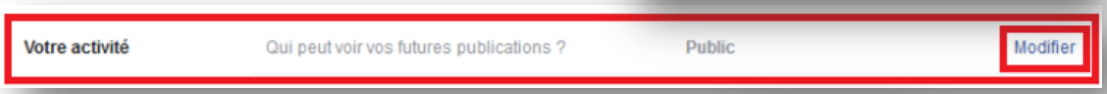
2. Pour aller dans les paramètres de confidentialité, cliquez d’abord sur la flèche bleue en haut à droite de votre écran pour afficher le menu.

3. Dans le menu, cliquez sur « **Paramètres et confidentialité** »

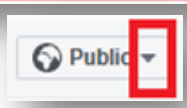


4. Puis, cliquez sur « **Raccourcis de confidentialité** ».
Après cliquez sur
“voir d’autres paramètres de confidentialité”.

5. Dans la partie "Votre activité",
sur la première ligne "**Qui peut voir vos futures publications** ?",
cliquez sur "**modifier**"



6. Cliquez sur la flèche grise à droite de "**Public**" pour faire apparaître le menu.



7. Cliquez sur "**Amis**" pour que seulement vos amis voient les photos et les messages que vous publiez. Puis cliquez sur Fermer en haut à droite.

8. Ensuite, dans la partie « **Comment les autres peuvent vous trouver et vous contacter** », sur la dernière ligne, cliquez sur "modifier".

9. Assurez-vous que la case est décochée. Si la case est cochée, cela signifie que vous autorisez n’importe qui à voir votre compte Facebook en tapant votre nom et prénom dans un moteur de recherche comme Google. Enfin, cliquez sur Fermer Votre compte est paramétré : N’oubliez pas de vous déconnecter.

À retenir
Protéger mes données personnelles

Qu’est-ce que je laisse derrière moi ?

À chaque fois que vous naviguez sur Internet, **vous laissez des traces** : votre adresse IP, votre historique de navigation, et même des informations personnelles.
Il est important **d’être conscient de ce que vous laissez derrière vous**.

Comment gérer mes cookies ?

Les cookies sont **des petits fichiers installés sur votre appareil** lorsque vous visitez des sites web, ils peuvent être acceptés sans danger sur les sites connus. Ils peuvent **collecter des informations sur vos préférences et habitudes en ligne**. Apprenez à gérer vos cookies via les paramètres de votre navigateur pour protéger votre vie privée.

Que font Facebook et Google de mes données ?

Les géants du numérique comme Facebook et Google collectent une grande quantité de données personnelles **pour personnaliser les publicités et améliorer leurs services**.
Il est important de savoir comment ces données sont utilisées et de configurer les paramètres de confidentialité.

Bonnes pratiques à retenir :

- **Soyez conscient des données que vous partagez en ligne.**
- **Gérer régulièrement les cookies et les permissions des sites.**
- **Lisez les politiques de confidentialité des sites ou services.**
- **Utilisez des outils de confidentialité comme la navigation privée ou des extensions de blocage de suivi.**

OBJECTIF 3

UTILISER LES SERVICES ADMINISTRATIFS EN LIGNE

- Qu’est ce que CSAM ?
- Me connecter à un service en ligne avec ma CI
- Configurer Itsme
- Me connecter à un service en ligne avec Itsme

Les services administratifs en ligne facilitent nos démarches avec les institutions, mais leur utilisation requiert **des outils spécifiques pour garantir sécurité et authenticité**.

Dans cette section, nous découvrirons le portail CSAM, qui centralise l'accès aux services publics en ligne.
Nous verrons comment se connecter à ces services en utilisant notre carte d’identité électronique et comment configurer et utiliser l'application Itsme, une solution mobile sécurisée.
Ces outils vous permettront de gérer vos démarches administratives en ligne de manière simple et sécurisée.

Résumé

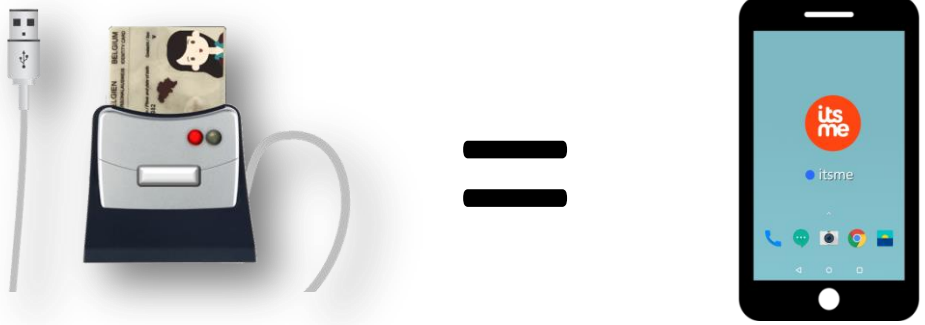
Créer votre compte itsme via eID

Votre identité numérique

Vos données personnelles se trouvent sur la **puce** de votre **carte d'identité électronique** (=eID). Les pouvoirs publics et bien d'autres organisations doivent demander ces informations afin de connaître votre identité.

« itsme », c'est quoi ?

« itsme » est une **application** sur votre smartphone qui **remplace votre carte d'identité électronique.** Après votre inscription sur « itsme », vos données personnelles apparaîtront également dans l'appli. Vous n'aurez plus besoin de votre eID et du lecteur de carte.



Comme pour votre eID, vous avez besoin d'un **CODE PIN personnel** pour accéder à « itsme ». L'avantage est que vous n'avez besoin que d'**un seul code** pour tous les services en ligne que vous souhaitez utiliser.

67021

À quoi sert « itsme » ?

À effectuer toutes sortes de tâches administratives : signer un contrat numérique, confirmer un paiement, déclarer vos impôts, consulter l'aperçu de votre carrière, postuler…

Comment créer un compte via eID ?

1. **Téléchargez** gratuitement l'application itsme® sur votre smartphone

Rendez-vous sur l'ordinateur

2. Surfez sur notre **site Web** : https://my.itsme.be/fr/register

3. Saisissez votre **numéro de GSM** et **adresse e-mail**. **Confirmez** vos données

4. Placez votre **carte eID** dans le **lecteur de carte. Synchronisez** vos données d'identité.

5. **Signez** le contrat itsme® avec votre eID en introduisant votre **code PIN**

6. Votre **token d'identification** (6 caractères) apparaît sur l'écran.

Revenez au smartphone

7. **Acceptez** les conditions générales

8. Saisissez votre **numéro de GSM**

9. Introduisez votre **token d'identification** (6 caractères)

10. Introduisez le code à 5 chiffres que vous avez reçu par SMS

11. Choisissez votre **code PIN** à 5 chiffres et **confirmez**

À retenir
Utiliser les services administratifs en ligne

Qu’est-ce que CSAM ?

CSAM (**Centre des Services Administratifs en ligne**) est une plateforme centralisée permettant d’accéder à divers **services publics en ligne**.
L’utilisation de cette plateforme nécessite une **identification sécurisée**.

Me connecter à un service en ligne avec ma carte d’identité

La carte d’identité électronique permet de vous **connecter à certains services en ligne de manière sécurisée**. Il est important de comprendre comment connecter cette carte pour effectuer des démarches administratives.

Configurer Itsme

Itsme est une **application de vérification d'identité** qui vous permet de vous connecter à divers services en ligne de manière sécurisée **en utilisant votre smartphone**. Il est devenu **indispensable** aujourd’hui de posséder et d’utiliser cette application

Me connecter à un service en ligne avec Itsme

Une fois Itsme configuré, vous pourrez vous connecter à différents services administratifs en ligne. Ce processus garantit une connexion sécurisée et authentifiée.

Bonnes pratiques à retenir :

- **Utilisez des moyens d’identification sécurisés comme la carte d’identité électronique ou Itsme.**
- **Configurez correctement ses outils de sécurité comme Itsme pour une utilisation optimale.**
- **Assurez-vous que la plateforme à laquelle vous accédez est légitime et sécurisée avant de soumettre des informations personnelles.**

OBJECTIF 4

LES MOTS DE PASSE

- Qu'est ce qu'un mot de passe sécurisé ?
- Créer un mot de passe sécurisé (et m'en rappeler !)
- Utiliser un gestionnaire de mots de passe
- Pratiquer l'authentification à deux facteurs

La sécurité de nos comptes en ligne repose en grande partie sur la qualité de nos mots de passe.

Dans cette section, nous explorerons les critères qui définissent un mot de passe sécurisé et apprendrons à en créer de manière simple mais efficace, tout en **utilisant des astuces pour s'en souvenir**.
Nous découvrirons aussi l'importance d'un **gestionnaire de mots de passe** pour stocker nos accès en toute sécurité et la valeur ajoutée de **l'authentification à deux facteurs** pour renforcer la protection de nos données.

Fiche résumé

Comment créer un mot de passe sécurisé ?

Qu'est-ce qu'un mot de passe?

Un mot de passe est comme une clé, qui sécurise vos espaces personnels sur internet. Il est donc **personnel** et **confidentiel** !

La définition d'un bon mot de passe

Un mot de passe sécurisé est :

- Long : au moins 8 caractères
- Composé de chiffres, lettres, caractères spéciaux
- Difficile à deviner : sans lien avec votre vie personnelle

Première technique : les mots choisis au hasard

1. Choisir 2 ou 3 mots sans rapport → **bicyclette lionceau**
2. Mettre la première lettre en majuscule → **B**icyclette lionceau
3. Séparer les mots d'un caractère spécial → Bicyclette**?**lionceau
4. Ajouter un chiffre → Bicyclette?lionceau**4**

Deuxième technique : la phrase facile à retenir

1. Trouver une phrase longue facile à retenir → **J'ai deux enfants qui s'appellent Laura et Tom**
2. Garder uniquement la première lettre de chaque mot et les chiffres → **Ja2eqsaLeT**
3. Ajouter un caractère spécial s'il n'y en a pas encore → Ja2eqsaLeT@

Comment mémoriser plusieurs mots de passe ?

Pour des raisons de sécurité, mieux vaut utiliser le même mot de passe sur chaque site.

 **Astuce** : gardez le même mot de passe et rajoutez les trois premières lettres du site sur lequel vous vous créez un compte. Exemple :

Ja2eqsaLeT@ →
- Sur 2ememain.be : Ja2eqsaLeT@**leb**
- Sur Gmail : Ja2eqsaLeT@**gma**

Autres mesures de sécurité

- Vos mots de passe sont confidentiels : ne les donnez à personne.
- Evitez d'écrire vos mots de passe sur papier.
- Quand vous créez une adresse mail, pensez aussi à renseigner votre numéro de téléphone : cela vous permettra de récupérer votre mot de passe si vous l'oubliez.

À retenir
Les mots de passe

Qu’est-ce qu’un mot de passe sécurisé ?

Un mot de passe sécurisé doit être **long**, **complexe** et **unique** pour chaque compte. Un mot de passe fort **combine des lettres majuscules et minuscules, des chiffres et des symboles**.

Créer un mot de passe sécurisé (et m’en rappeler !)

Il est important de créer un mot de passe qui soit **difficile à deviner**, tout en étant **suffisamment mémorisable**. Utilisez des **phrases de passe** ou des générateurs de mots de passe pour plus de sécurité.

Utiliser un gestionnaire de mots de passe

Un gestionnaire de mots de passe est un outil qui vous **permet de stocker vos mots de passe en toute sécurité**. Il vous aide à créer des mots de passe complexes et à les retrouver facilement.

Pratiquer l’authentification à deux facteurs (2FA)

L'authentification à deux facteurs **ajoute une couche de sécurité supplémentaire** en demandant **une deuxième vérification** (par exemple, un code envoyé par SMS) en plus de votre mot de passe.

Bonnes pratiques à retenir :

- **Créez des mots de passe longs et complexes pour chaque compte.**
- **Utilisez un gestionnaire de mots de passe pour garder une trace de vos identifiants en toute sécurité.**
- **Activez l’authentification à deux facteurs pour chaque compte qui le permet.**

OBJECTIF 5

LA SÉCURITÉ SUR INTERNET

- Quelles sont les techniques des pirates informatiques ?
- Que faire si … Analysons ensemble plusieurs cas concrets
- Qu'est ce que le pishing ? Comme le reconnaître ?
- Bonnes attitudes pour ne pas me faire avoir

Naviguer sur Internet comporte des risques, notamment face aux techniques de piratage de plus en plus sophistiquées.

Dans cette section, nous découvrirons les méthodes utilisées par les pirates pour tromper les utilisateurs et accéder à leurs informations.
Nous analyserons des cas concrets pour savoir comment réagir en cas de tentative d'attaque. Une attention particulière sera portée au phishing, l'une des escroqueries les plus courantes en ligne, en apprenant à le reconnaître pour mieux s'en protéger.
Enfin, nous aborderons **les bonnes pratiques à adopter au quotidien** pour sécuriser efficacement notre navigation.

Fiche résumé

La sécurité sur internet

Quelles sont les techniques des pirates ?

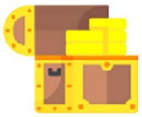
Les pirates sont des personnes qui détournent internet pour arnaquer des utilisateurs, détériorer leur matériel informatique, ou obtenir les données confidentielles d'entreprises ou d'internautes. Ils utilisent les moyens suivants :

Installer un virus ou logiciel malveillant qui détériore l'ordinateur

Exploiter les sites non sécurisés pour obtenir des informations personnelles

Obtenir les informations laissées par les internautes sur des réseaux wifi non sécurisés

Envoyer des mails frauduleux



Faire des propositions trop belles pour être vraies, pour tromper l'internaute

Se faire passer pour un proche qui a besoin d'argent

Comment protéger son ordinateur des attaques ?

Installez un **anti-virus** (Windows defender/ Avast...) et un pare-feu

Mettez régulièrement à jour vos logiciels

Les règles à appliquer pour naviguer sur internet en sécurité

1 Reconnaître les sites **fiables**

2 Créer des **mots de passe sécurisés**

Un mot de passe sécurisé est un mot de passe long, composé de chiffres, lettres et caractères spéciaux, difficile à deviner par d'autres.

i En 2017, les mots de passe les plus piratés étaient : *123456*, *motdepasse*, *bienvenue*, *football*...

3 **Se déconnecter** de ses comptes en ligne après avoir utilisé un ordinateur public

4 Pour faire des transactions bancaires, se connecter sur un **réseau wifi sécurisé**

Comment reconnaître les mails malveillants ?

Vous pouvez reconnaître un mail malveillant grâce aux indices suivants :

- Le message comporte une **adresse e-mail bizarre**
- On me demande d'**envoyer de l'argent pour payer des frais**
- L'e-mail contient des **fautes d'orthographe**
- Le message m'adresse des **menaces irréalistes**
- L'offre contenu dans le message est **trop belle pour être vraie**
- Le message me **demande des informations personnelles**

Si vous recevez un mail malveillant, signalez-le comme SPAM.

N'oubliez pas que vous êtes maître de votre sécurité en ligne : vous pouvez éviter les attaques des pirates en faisant attention aux données personnelles que vous diffusez sur internet et en appliquant les règles de sécurité ci-dessus.

À retenir
La sécurité sur Internet

Quelles sont les techniques des pirates informatiques ?

Les pirates utilisent diverses techniques pour accéder à vos informations personnelles, telles que le **phishing**, les **wangiri**, et les **quishing** . Comprendre ces techniques vous aidera à vous protéger.

Qu'est-ce que le phishing ? Comment le reconnaître ?

Le phishing est une technique où des criminels se font passer pour des institutions fiables (banques, sites de e-commerce) pour voler des informations personnelles.

Que faire si...

1. Commencez par faire opposition sur votre carte bancaire
2. Désinstallez l'éventuel logiciel que l'escroc vous a fait installer
3. Changez tous vos mots de passe

Bonnes pratiques à retenir :

- **Restez vigilant face aux tentatives de phishing.**
- **Ne cliquez jamais sur des liens ou ouvrez des pièces jointes suspectes.**
- **Ne rappelez pas un numéro inconnu qui ne vous a pas laissé de message**
- **Ne scannez pas un QR code dont vous ne pouvez pas vous assurer la provenance**
- **Utilisez des logiciels antivirus pour détecter les malwares.**
- **Apprenez à reconnaître les signaux d'une attaque pour savoir comment réagir.**

OBJECTIF 6

ACHETER SUR INTERNET

- Quel produit sur quel site ?
- Comment faire des achats en ligne en toute sécurité ?
- Comment payer en ligne ?
- Gros plan sur l'application Payconiq

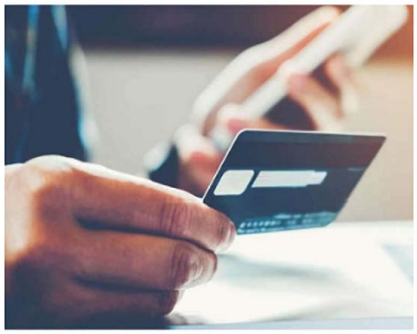
Acheter sur Internet est devenu une habitude pour beaucoup, mais il est important de savoir **le faire en toute sécurité**.

Dans cette section, nous verrons **comment choisir les bons sites** pour trouver les produits souhaités, et quelles vérifications effectuer pour éviter les mauvaises surprises.
Nous explorerons ensuite **les méthodes de paiement en ligne sécurisées**, et mettrons un coup de projecteur sur **l'application Payconiq**, une solution pratique et sécurisée pour régler nos achats.
Grâce à ces conseils, vous pourrez faire vos achats en ligne en toute confiance.

Fiche résumé

Découvrir les achats en ligne
et le paiement sécurisé sur Internet.

Quels sont les avantages du paiement sur Internet ?



- **Avoir plus de choix**
- **Avoir des promotions** uniquement disponibles sur Internet
- **Comparer les prix** sur plusieurs sites
- **Gagner du temps**

Quels sont les moyens de paiement sur Internet ?

Les moyens de paiement sur Internet les plus utilisés sont les suivants :

La carte bancaire & digipass

L'appli Payconiq by Bancontact

payconiq
Bancontact

Le compte bancaire virtuel

PayPal

Quels produits et services acheter sur Internet ?

- Faire des courses
- Payer ses factures d'électricité, de gaz, de téléphone…
- Réserver des spectacles
- Réserver des vacances
- Acheter des vêtements

Comment réaliser un paiement sécurisé sur Internet ?

Avant de commencer votre paiement, assurez-vous d'avoir :

Une connexion à internet sécurisée et fiable pour éviter les coupures de réseau.

Votre téléphone et votre boite mail afin de suivre votre paiement.

Votre carte bancaire pour l'étape du paiement.

⚠ Attention à ne pas faire vos achats en ligne en utilisant un réseau Wifi Public

1 Le paiement en ligne par carte bancaire et lecteur de carte

1 Se connecter au site de son choix

Vérifier que le site est sécurisé.

- 
- Le “s” dans le ***https*** de l’adresse du site Internet.

2 Sélectionner le produit de son choix

Parcourez le site et ajoutez l’article souhaité à votre panier.

3 Vérifier la commande puis valider

Vérifiez les informations de votre commande dans le panier, puis validez la commande.

4 Se connecter ou créer un compte

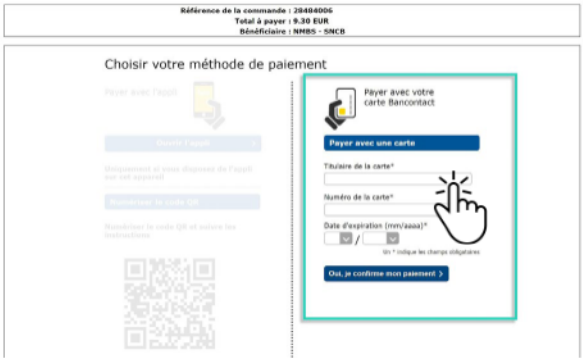
Pour recevoir votre commande chez vous et définir vos préférences de paiement vous devez paramétrer vos données personnelles.

5 Choisir un mode de paiement

Sélectionnez le mode de paiement que vous souhaitez utiliser.

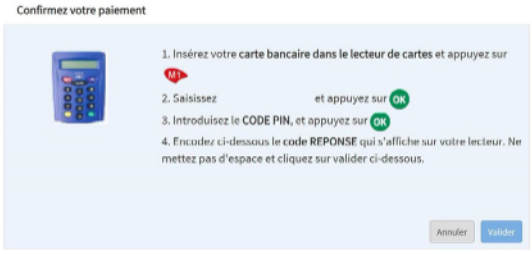
6 Renseigner les informations de ma carte

Remplissez le formulaire affiché à l’écran (nom du titulaire de la carte, numéro de carte et date d’expiration)



7 Insérer la carte dans le lecteur de carte

Insérez votre carte Bancontact dans le lecteur de carte de votre banque et suivez les instructions affichées à l’écran.



8 Confirmer

Une fois le paiement accepté, vous recevez une confirmation visuelle sur le site et un e-mail de confirmation.

2 Commande sur PC et paiement via smartphone

1 Se connecter au site de son choix

Vérifier que le site est sécurisé.

- 
- Le “s” dans le ***https*** de l’adresse du site Internet.

2 Sélectionner le produit de son choix

Parcourez le site et ajoutez l’article souhaité à votre panier.

3 Vérifier votre commande puis valider

Vérifiez les informations de votre commande dans le panier, puis validez la commande.

4 Se connecter ou créer un compte

Pour recevoir votre commande chez vous et définir vos préférences de paiement vous devez paramétrer vos données personnelles.

5 Choisir un mode de paiement

Sélectionnez le mode de paiement que vous souhaitez utiliser.

6 Scanner le code QR

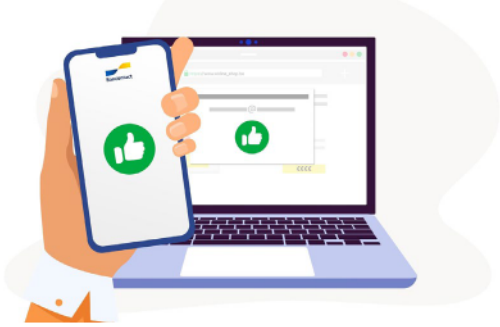
Scannez le code QR pour envoyer les informations du paiement vers votre GSM

7 Finaliser le paiement via Payconiq

Confirmez le transaction et insérez votre code de sécurité pour valider le paiement.

8 Confirmer

Une fois le paiement accepté, vous recevez une confirmation visuelle sur le site et un e-mail de confirmation.



3 Commande et paiement sur smartphone

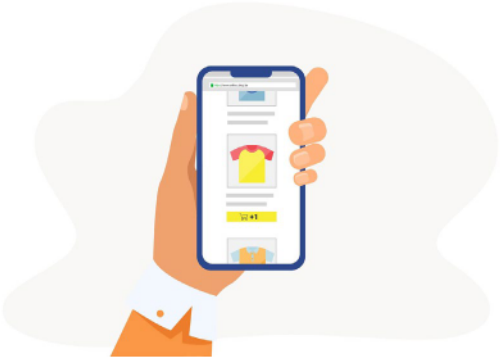
1 Se connecter au site de son choix

Vérifier que le site est sécurisé.

- ✔ 🔒
- ✔ Le “s” dans le ***https*** de l’adresse du site Internet.

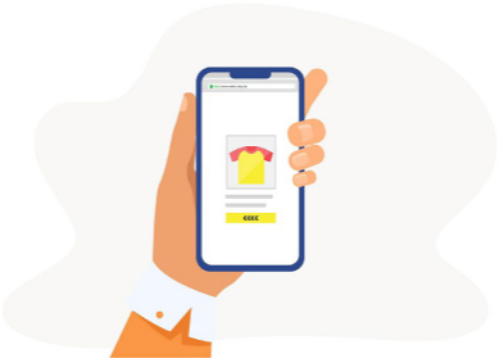
2 Sélectionner le produit de son choix

Parcourez le site et ajoutez l’article souhaité à votre panier.



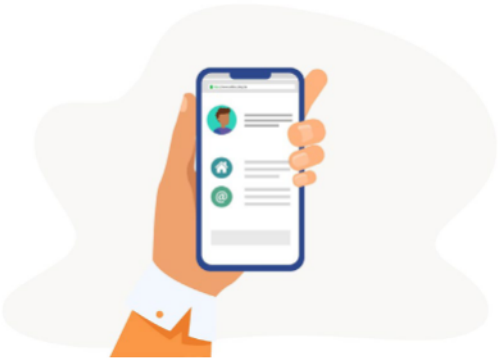
3 Vérifier votre commande puis valider

Vérifiez les informations de votre commande dans le panier, puis validez la commande.



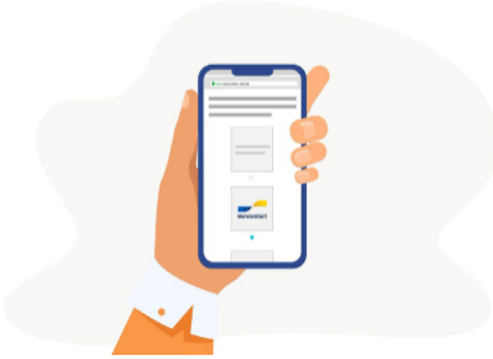
4 Se connecter ou créer un compte

Pour recevoir votre commande chez vous et définir vos préférences de paiement vous devez paramétrer vos données personnelles.



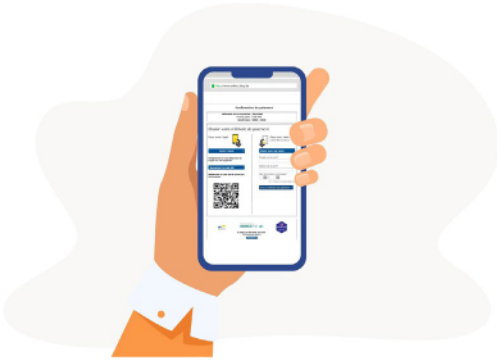
5 Choisir un mode de paiement

Sélectionnez le mode de paiement que vous souhaitez utiliser.



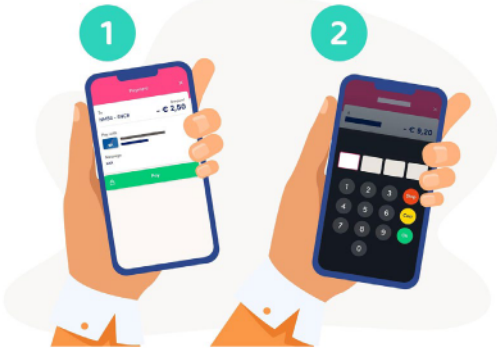
6 Scanner le code QR

Scannez le code QR pour envoyer les informations du paiement vers votre GSM.



7 Finaliser le paiement via Payconiq

Confirmez le transaction et insérez votre code de sécurité pour valider le paiement.



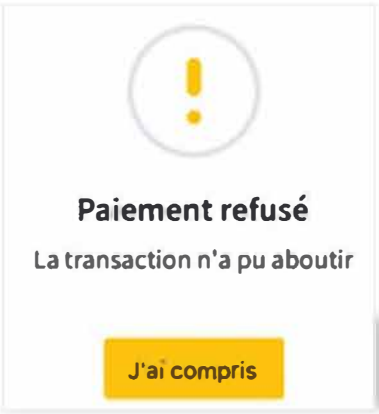
8 Confirmer

Une fois le paiement accepté, vous recevez une confirmation visuelle sur le site et un e-mail de confirmation.

Comment faire en cas de paiement refusé ?

Vous pouvez essayer à nouveau, en cas d'échec, voici les raisons possibles :

- Le site ou la banque bloque le paiement.
- Problème technique sur le site Internet.
- Nouvelle carte bleue pas activée.
- Solde bancaire insuffisant.
- Opposition à votre carte bancaire après un vol. .



Rappel :

Pour le paiement sur Internet vous ne devez jamais communiquer votre code de carte bancaire à 4 chiffres.

À retenir
Acheter sur Internet

Quel produit sur quel site ?

Avant d'acheter un produit, il est essentiel de **vérifier la réputation du site**. Utilisez des sites fiables et lisez les **avis des autres clients** pour vous assurer que vous achetez un produit de qualité.

Comment faire des achats en ligne en toute sécurité ?

Assurez-vous que le site utilise un **protocole de sécurité HTTPS** et vérifiez la présence d'un **cadenas** dans la barre d'adresse.
Évitez de partager des informations sensibles sur des sites non sécurisés.

Comment payer en ligne ?

Il est préférable d'utiliser des moyens de paiement sécurisés comme **l'application Payconiq** ,**PayPal** ou des cartes bancaires virtuelles, plutôt que de divulguer directement vos informations bancaires.

Bonnes pratiques à retenir :

- **Vérifiez toujours que le site est sécurisé (HTTPS).**
- **Utilisez des méthodes de paiement sécurisées comme Payconiq**
- **Ne partagez jamais vos informations bancaires sur des sites non sécurisés.**

OBJECTIF 7

PROTÉGER SON SMARTPHONE

- Sécuriser l'accès à son smartphone
- Gérer les permissions des applications
- Éviter les logiciels malveillants

Nos smartphones contiennent une grande quantité de données personnelles et sont devenus des cibles privilégiées pour les cyberattaques.
Pour bien protéger cet outil essentiel, il est crucial de sécuriser l'accès à son téléphone, de savoir gérer les permissions accordées aux applications, et de se protéger contre les logiciels malveillants.
Grâce à ces bonnes pratiques, vous saurez comment protéger votre smartphone et les informations précieuses qu'il contient.

Fiche résumé
Sécurisez vos appareils mobiles

Comment sécurisez vos appareils mobiles ?

Activez le verrouillage automatique de votre smartphone par un mot de passe ou un code numérique

- Ouvrir les **paramètres**
- Sélectionner "**Sécurité**" ou "**Sécurités et confidentialité**"
- Choisir "**Verrouillage de l'écran**" et sélectionner le type de verrouillage, vous aurez le choix entre plusieurs options : Mot de passe, PIN, ou Schéma.
- Vous pouvez également configurer des **méthodes biométriques** comme l'empreinte digitale ou la reconnaissance faciale pour renforcer la sécurité.

Activez la mise à jour automatique du matériel et des logiciels

- Ouvrir les **paramètres**
- Sélectionner "**A propos du téléphone**"
- Choisir "**Mise à jour du système**" et assurez-vous que l'option "Mise à jour automatique est activée".

Activez la double authentification (2FA) sur toutes vos applications

Téléchargez vos applis via des apps stores reconnus

Google Play

Supprimez les applications que vous n'utilisez pas

- Accéder à l'écran d'accueil ou au tiroir d'applications
- Appuyez longuement sur l'icône de l'application et sélectionnez **Désinstaller**

Vérifiez souvent les données exploitées par vos applications

- Accéder aux **paramètres de confidentialité** : **Paramètres**, puis sélectionnez **Applications** ou **Applications et notifications**
- Appuyez sur **Autorisations des applications** pour voir quelles applications ont accès à vos données (contacts, position, caméra, etc.).
  Désactivez les permissions inutiles ou trop intrusives pour certaines applications.

Choisissez un code PIN sûr pour votre carte SIM

Choisissez un code PIN unique et difficile à deviner
(évitez des combinaisons simples comme 1234 ou 0000)

À retenir
Protéger son smartphone

Sécuriser l'accès à son smartphone

Protégez votre smartphone avec un **code PIN**, une **empreinte digitale** ou une r**econnaissance faciale** pour éviter que des personnes non autorisées y accèdent.

Gérer les permissions des applications

Les applications demandent parfois des autorisations excessives. **Vérifiez régulièrement les permissions accordées aux applications** et révoquez celles qui ne sont pas nécessaires.

Éviter les logiciels malveillants

Téléchargez uniquement des applications **provenant de sources fiables**, comme les stores officiels. Méfiez-vous des applications piratées ou non vérifiées.

Bonnes pratiques à retenir :

- **Utilisez un mot de passe ou une méthode biométrique pour sécuriser l'accès à votre smartphone.**
- **Vérifiez les permissions des applications et révoquez celles qui sont inutiles.**
- **Téléchargez uniquement des applications officielles et évitez les sources non fiables.**

OBJECTIF 8

LE CYBERHARCÈLEMENT

- Comment réagir face au cyberharcèlement ?
- Conseils pratiques pour bloquer, signaler, et se protéger en ligne.

Le cyberharcèlement est un problème croissant dans nos interactions en ligne, touchant des personnes de tous âges et ayant des conséquences importantes sur la santé mentale.

Dans cette section, nous verrons comment réagir efficacement face à une situation de harcèlement en ligne, et comment promouvoir un environnement en ligne sûr et respectueux. **Sensibilisés et informés, nous serons mieux armés pour protéger notre bien-être numérique et celui des autres**.

Fiche résumé
Le cyberharcèlement

Comprendre ce qu'est le cyberharcèlement

Le cyberharcèlement désigne **toute forme d'intimidation**, de **harcèlement** ou de violence exercée **via les technologies numériques**. Il peut se manifester par des insultes, des menaces, ou encore la diffusion de rumeurs.

Reconnaître les signes de cyberharcèlement

Les victimes de cyberharcèlement peuvent ressentir de l'anxiété, de la peur ou de la honte. Les signes peuvent inclure un changement de comportement ou des évitements de certaines situations.

Comment réagir face au cyberharcèlement

Si vous êtes victime de cyberharcèlement, il est important de **ne pas répondre aux attaques**, de **garder des preuves** et de **signaler les comportements** aux autorités compétentes.

Prévenir et sensibiliser

Il est essentiel de promouvoir un comportement respectueux en ligne et de sensibiliser les autres à ce phénomène pour réduire les cas de cyberharcèlement.

Bonnes pratiques à retenir :

- **Signalez toute forme de cyberharcèlement aux autorités compétentes.**
- **Ne répondez pas aux messages de harcèlement et gardez des preuves.**
- **Respectez les autres en ligne et encouragez un environnement numérique sûr.**
- **Sensibilisez-vous et sensibilisez les autres aux dangers du cyberharcèlement.**