# Les cahiers de la Mission Inclusion Numérique



## # 01 Cybersécurité : protégez les usages numériques de votre famille ou de votre petite entreprise


La sécurité du numérique est l'affaire de chacun. Elle repose sur des mesures de bases simples et pratiques.

Votre mairie a décidé de vous sensibiliser à cet enjeu en vous offrant ce supplément spécial « cybersécurité », en lien avec Cybermalveillance.gouv.fr et la Mission Inclusion Numérique de la communauté d'agglomération Pau Béarn Pyrénées.

Aussevielle

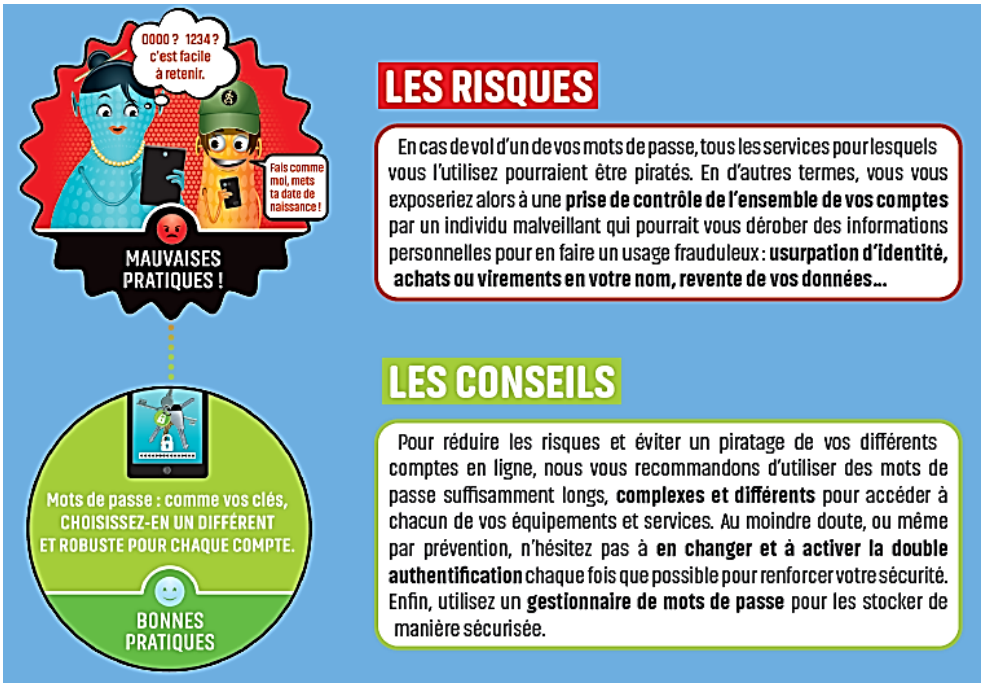
# 01 - Le mot de passe : la clé qui ouvre tous vos comptes !



En tant que parents, qu'adultes, nous bénéficions de nombreux comptes, d'accès à des services que nous utilisons au quotidien : messagerie (mails), comptes bancaires, services en ligne (cantine scolaire, activités périscolaires, billetterie, etc). Nous gérons des rendez-vous médicaux ou nos dossiers administratifs en ligne (CAF, AMELI, Impôts, etc) et nous discutons sur les réseaux sociaux ...

A chaque fois, il nous est demandé un « mot de passe ». Par paresse ou par peur de l'oublier, nous utilisons le même pour tout et nous choisissons la facilité : « 1 2 3 4 5 6 », « abcde », le nom du chat, la date de naissance du conjoint, etc. Des mots de passe faciles à retenir (et donc … à deviner). Parfois même, nous le notons dans un petit carnet …

**ERREUR FATALE !!!**




L'astuce de la Mission Inclusion Numérique pour avoir un mot de passe solide et facile à mémoriser : prenez la première lettre des mots d'une chanson que vous connaissez. Par exemple, « au clair de la lune, mon ami Pierrot » soit « acdll,maP » et opérez une petite transformation : « @C2lL,^^aP » : vous venez de créer un mot de passe solide de 9 signes, avec des majuscules, des minuscules, des caractères spéciaux (évitez le «€») et 1 chiffre. L'idéal est de construire un mot de passe de 12 caractères et d'en avoir un pour chaque compte. A vous de jouer !

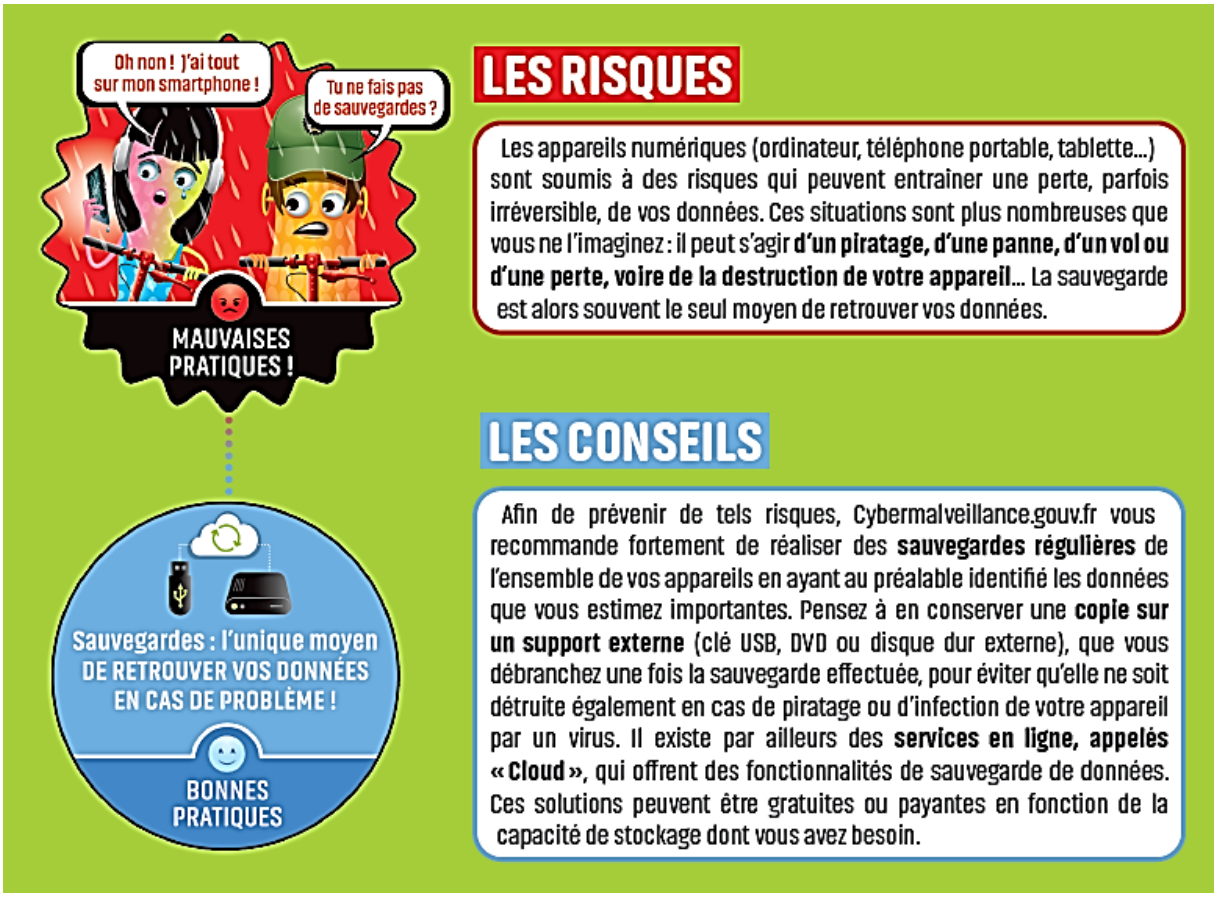
Pour activer la double authentification, suivez bien les conseils de votre opérateur ou de votre banque ! Et inscrivez-vous à notre module « cybersécurité » pour tout savoir sur les gestionnaires de mots de passe.

# 02 – Pensez à sauvegarder vos données

Nous utilisons de nombreux équipements numériques pour créer et stocker nos données importantes : photos, videos, contacts téléphoniques, documents bancaires, administratifs, factures, etc. Comment ne pas les perdre ?

## En les sauvegardant régulièrement






**Le conseil + de la Mission Inclusion Numérique** : Les risques de perte, de vol, de panne, de piratage ou de destruction peuvent également affecter vos sauvegardes. Protégez-les au même titre que vos données originales en effectuant, par exemple, plusieurs sauvegardes de vos données sur différents supports.

Conservez également une sauvegarde dans un lieu différent de celui où sont stockées les données originales pour vous prémunir en cas de sinistre.

La règle pour bien sauvegarder : celle des « 3 – 2 – 1 ». Le principe en est simple : 3 copies des données, dont 2 doivent être stockées sur 2 supports différents dont 1 conservée en dehors du logement.

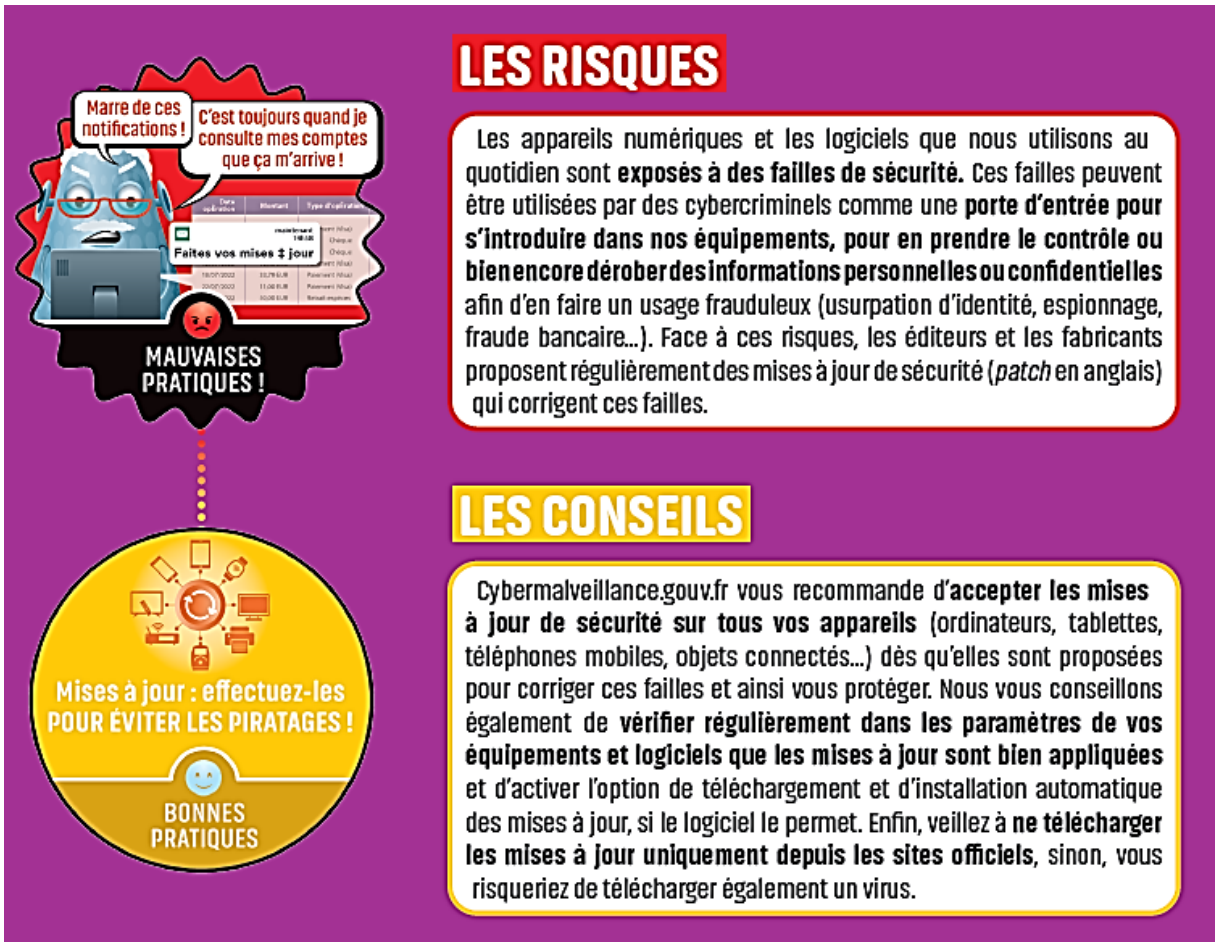
# 03– Procédez aux mises à jour de sécurité sur tous vos appareils

Qui n'a pas « zappé » la dernière notification de mise à jour de son smartphone ? Par manque de temps ou de compréhension, il nous arrive de supprimer les alertes et les notifications de mise à jour sur nos équipements numériques.

Un exemple de faille de sécurité ? aux Etats-Unis, des cybercriminels ont réussi à dérober des données confidentielles d'un casino grâce au thermomètre connecté présent dans un aquarium de l'établissement ☹.



## Protégeons nos données !




**Le conseil de la Mission Inclusion Numérique** : restez vigilants car en naviguant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran : fausses publicités sur des sites Internet ou fenêtres (pop-up en anglais) malveillantes. Restez extrêmement attentif car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

Enfin, pensez à faire aussi les mises à jour de vos applis. Compliqué ? pas si vous suivez nos formations gratuites …

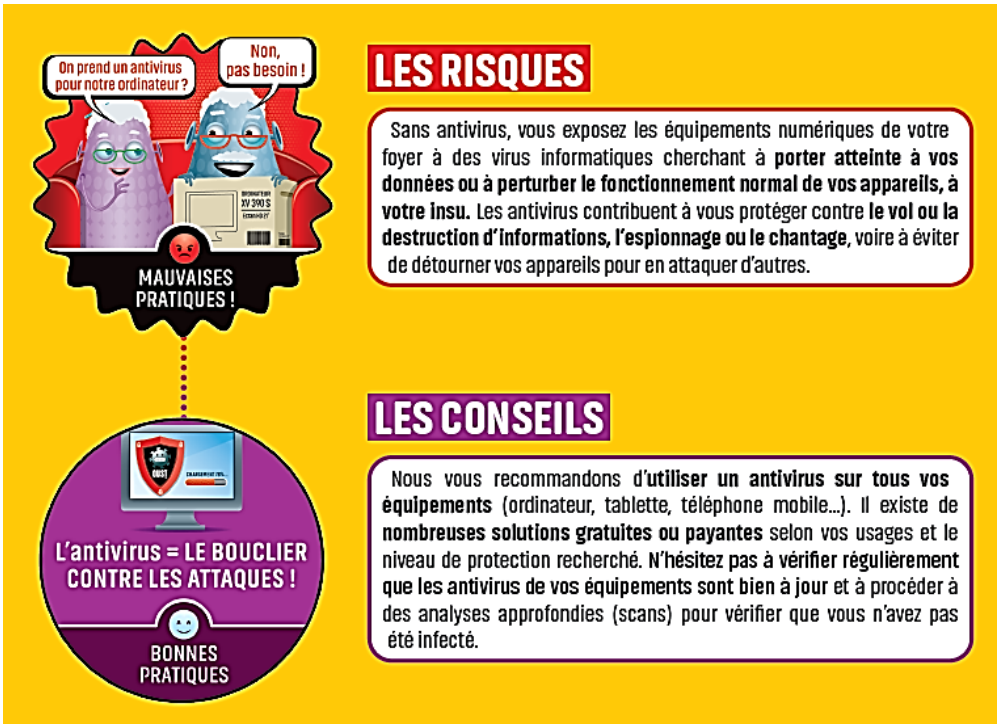
# 04– Importance de l'anti-virus

Un antivirus se greffe sur le système d'exploitation de l'appareil. Il permet de rechercher les virus dans ce qui peut être stocké dans vos équipements numériques, y entrer ou en sortir. Parfois, les anti-virus sont considérés comme une dépense inutile au moment de l'achat d'un équipement informatique. Ou d'autres achètent une licence mais n'activent pas forcément l'anti-virus.

Pourtant il est aussi important que l'alarme incendie de notre domicile. Nos équipements numériques peuvent être infectés par un virus en naviguant sur Internet, en connectant une clé USB, en cliquant sur un lien, ou en ouvrant une pièce jointe d'un courriel.



## Utilisez un anti-virus et ... mettez-le à jour !




**Le rappel de la Mission Inclusion Numérique** : des milliers de nouveaux virus sont créés chaque jour. Pour rester protégés face aux menaces, les éditeurs de logiciels réalisent des mises à jour régulières de leurs produits. Il est donc important de ne pas les différer.

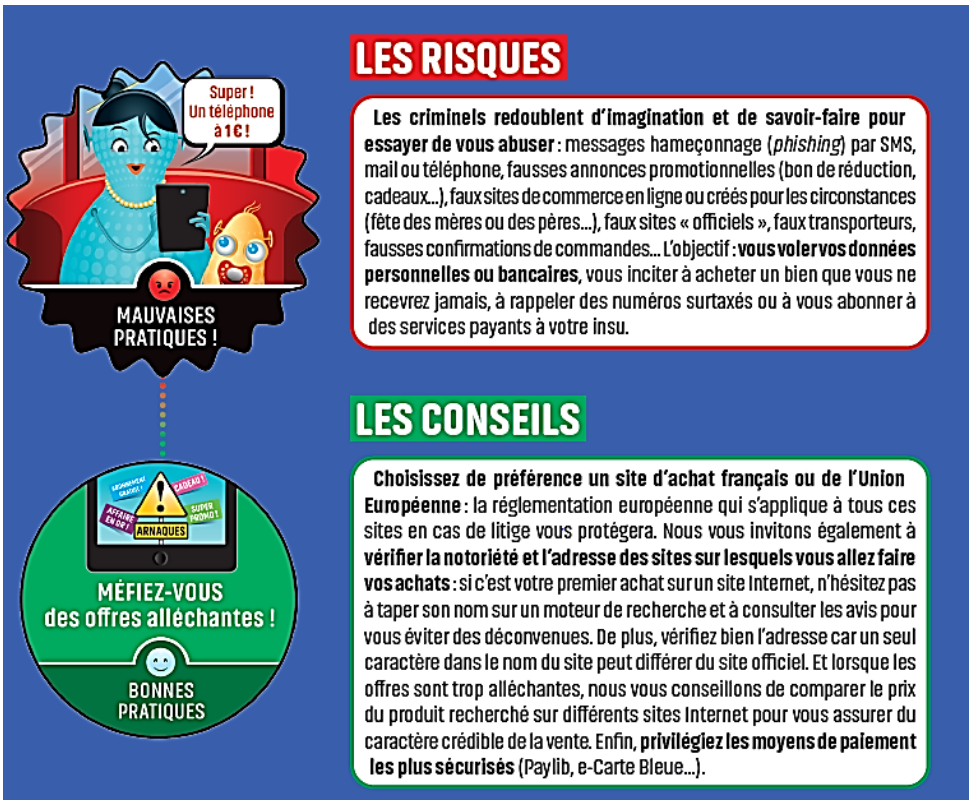
Si malgré tout, vous avez été victime d'une attaque virale, il est conseillé de déconnecter l'appareil d'Internet et de lancer une analyse « scan » approfondie pour vous assurer qu'aucune trace de virus ne subsiste. Si vous ne pouvez supprimer un virus en quarantaine, il est recommandé une réinstallation complète de l'appareil et un changement des mots de passe ou de faire appel à un professionnel.

Souvenez-vous qu'un antivirus est très souvent fourni gratuitement par l'éditeur de votre logiciel.

# 05– Acheter en ligne en toute sécurité

Internet a révolutionné notre façon de consommer et le confinement dû au COVID a accéléré le recours au numérique pour nos achats. Tout est accessible en un clic. Le bon comme le mauvais.

## Derrière le caddy virtuel, y-a-t-il un escroc ?




**7 petits conseils pour éviter les escroqueries en ligne**

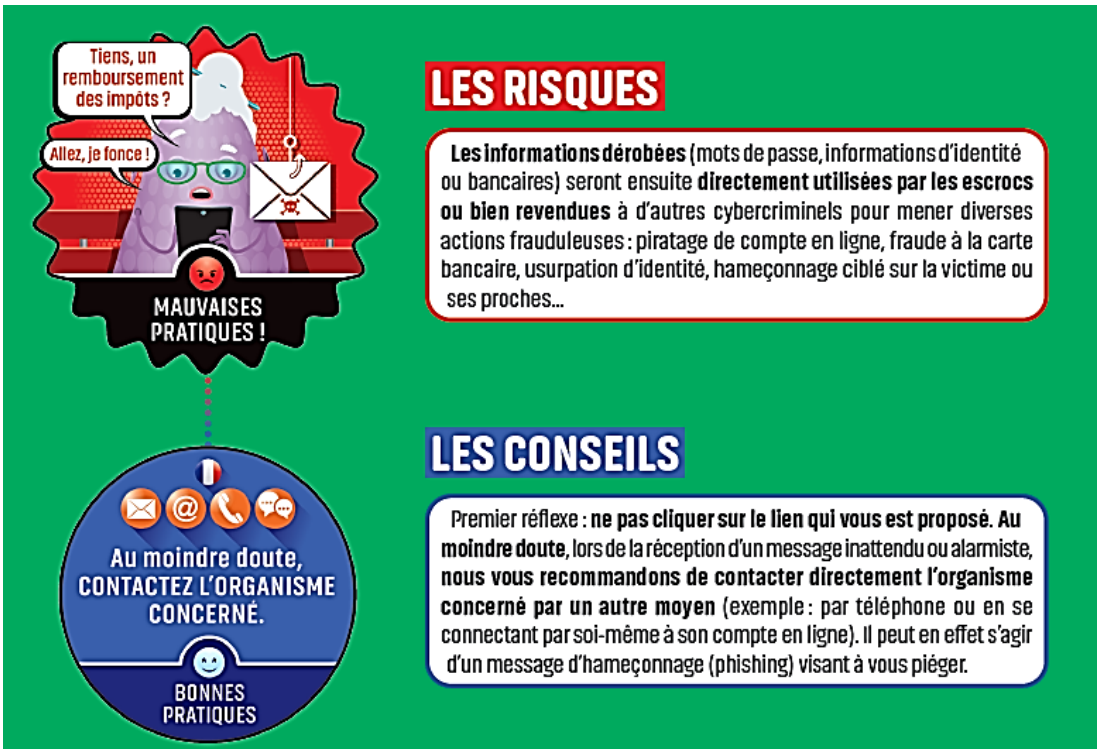
- Méfiez-vous des offres trop généreuses. Faites un minimum de vérification
- Un vendeur vous propose l'affaire du siècle si vous achetez immédiatement ? Il est surtout urgent de prendre son temps et de vérifier l'existence réelle du vendeur, la réalité de la promotion. Ne donnez pas le numéro de votre carte bancaire !
- Vous venez de recevoir un sms énigmatique (un colis à débloquer, une amende à payer) ? ne cliquez sur aucun lien. Préférez rappeler le numéro officiel du vendeur ou du service concerné.
- Un mail vous demande de cliquer sur un lien pour bénéficier d'une promotion ? vous risquez le vol de vos codes d'accès, de vos données personnelles ou l'achat d'une contre-façon. Vérifiez le site officiel.
- Attention aux faux sites officiels ; certains imitent presque parfaitement l'original. Soyez attentifs et curieux !
- Ne fournissez jamais vos données personnelles ou bancaires. Utilisez la double autorisation de votre banque.
- Utilisez un mot de passe solide et différent pour chaque application ou site Internet.

# 06– Méfiez-vous des messages suspects

Il ne se passe pas un jour sans que nous recevions un sms ou un mail frauduleux, imitant parfaitement le logo d'une institution connue ou de l'entreprise du coin de la rue. Le but ? chercher à nous induire en erreur et à nous inciter à donner nos informations personnelles ou à ouvrir une pièce jointe qui nous dirige vers un site frauduleux.

**Tout est bon pour nous contraindre : la peur, l'urgence, la crédulité**






**Les conseils de la Mission Inclusion Numérique**

- Au moindre doute, contactez l'organisme concerné
- Faites opposition immédiatement
- Conservez les preuves
- Déposez plainte
- Changez immédiatement de mot de passe
- Signalez tout message ou site frauduleux à « Signal Spam », associé à la CNIL (https://www.signal-spam.fr/ )
- Signalez l'adresse d'un site d'hameçonnage à « Phishing Initiative » qui bloquera l'accès à ce site https://phishing-initiative.eu/contrib/
- Pour être bien conseillé dans ces démarches, prenez contact avec « Info Escroqueries » du ministère de l'intérieur au 0 805 805 817 (appel gratuit de 9h à 18h30 du lundi au vendredi)

**La règle numéro 1** : ne **JAMAIS** cliquer sur un lien fourni dans un message (sms ou mail). Vous devez toujours vérifier l'information sur le site web officiel. Notre formation en cybersécurité vous donnera toutes les astuces et conseils.

# 07– Maîtrisez vos réseaux sociaux

FaceBook, Instagram, LinkedIn, TikTok, Twitter, Snapchat … les réseaux sociaux sont devenus notre quotidien et celui de nos enfants. On y publie tout, on y partage nos opinions, nos photos et … rien ne s'efface, rien ne nous appartient plus. Tout circule.

## Comment garder la maîtrise de nos informations personnelles ?

*identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance*




**Le savez-vous ?** 28% des enfants de 9 – 11 ans ont déjà un compte sur les réseaux sociaux. 78% des parents ne savent pas ce que leurs enfants font sur les réseaux sociaux et sur Internet alors que l'autorisation parentale est obligatoire jusqu'à 15 ans !

**Que faire en cas de problème ?**

- Demander la suppression d'une publication gênante ou compromettante : https://www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer
- En cas de situation de cyberharcèlement, contactez le **3018**, ligne d'écoute nationale anonyme et confidentielle destinée aux internautes confrontés à ce problème
- Signaler un contenu illicite sur les réseaux sociaux : Internet-signalement.gouv.fr
- N'oubliez pas de séparer compte personnel et compte professionnel.

# 08– WiFi publics ou inconnus

Aujourd'hui, chacun souhaite se connecter où qu'il soit, partout et à tout moment. En voyage ou en déplacement professionnel. Les communes, les lieux touristiques proposent une connexion WiFi publique. C'est un service pratique mais est-ce sans danger ?

## Parfois, c'est une aubaine pour les pirates informatiques




**3 précautions à prendre**

- Evitez de vous connecter à des réseaux sans fil, inconnus : demandez le nom du réseau au commerçant ou au propriétaire de l'établissement
- Ne confiez pas trop d'information à un portail d'accès Wi-Fi : si celui-ci vous demande des informations personnelles en échange d'un accès à internet et évitez d'utiliser votre adresse mail principale, remplissez le moins d'informations possibles, et ne cochez pas la case « *communiquer mes données à des tiers* ».
- Désactivez la fonction Wi-Fi de votre appareil lorsqu'il n'est pas utilisé. Désactivez l'option « *recherche toujours disponible* » si votre téléphone vous le permet.

Ces conseils sont valables pour les connexions BlueTooth. Attention aussi aux clés USB « trouvées » ou données sur les foires expos ; elles présentent souvent un danger

**LE SAVIEZ-VOUS ?** Les organismes (restaurant, aéroports…) qui proposent un accès au réseau internet au public, à titre payant ou gratuit, sont tenus de conserver les données de trafic de leurs clients (sauf les informations relatives au contenu des communications, comme le corps ou l'objet d'un courrier électronique ou les URL des sites web consultés).

# 09– Sécurisez vos objets connectés

Depuis votre montre ou votre smartphone, vous pouvez suivre vos performances sportives, régler à distance le thermostat de votre domicile ? C'est très pratique d'être connecté à tout !

## Mais cela décuple votre exposition aux risques


Alexa ? Siri ? Echo ? Non, vous n'appelez pas votre animal de compagnie : vous demandez l'aide d'un assistant vocal pour effectuer diverses tâches (recherche d'information sur le Net, commande de produits, gestion de vos appareils intelligents). Mais nos données personnelles sont-elles en sécurité ?

Les assistants vocaux peuvent, et peuvent être programmés, pour influencer les choix et les comportements des utilisateurs, ce qui soulève des préoccupations éthiques quant à la manipulation des utilisateurs, notamment mineurs.

Soyez vigilants et conscients de l'utilisation de l'assistant vocal en limitant les autorisations si nécessaires, en renforçant les mots de passe et en évitant de s'appuyer sur lui pour toutes les tâches.

# 10 – Cyberharcèlement, on en parle ?

Certains harceleurs le prennent comme un jeu, les victimes en souffrent durablement. Le harcèlement peut être le fait d'une ou plusieurs personnes et toucher aussi bien les adultes que les plus jeunes. Avec l'avènement des nouvelles technologies et des réseaux sociaux, le harcèlement s'est également développé en ligne : intimidations, insultes, rumeurs, publication de photos ou vidéos compromettantes…

## Evitez de rester seul/seule face au cyberharcèlement




**Que faire en cas de cyberharcèlement ?**

- Ne répondez pas aux commentaires ; vous risqueriez d'empirer la situation en y montrant de l'intérêt
- Parlez-en à un tiers de confiance (membre de la famille, ami, frère, ou à un adulte de votre établissement scolaire)
- Conservez des preuves : captures d'écran, les messages pour pouvoir déposer plainte.
- Verrouillez au plus vite les comptes de réseaux sociaux en modifiant les paramètres de confidentialité. Vous pouvez bannir les contacts indésirables et bloquer les auteurs des messages harcelants.
- Signalez les contenus et comportements illicites auprès des plateformes sur lesquelles les harceleurs sont présents
- Demandez à ce que les contenus harcelants ne soient plus référencés par les moteurs de recherche (déréférencement) et déposez plainte.

**Un numéro utile : le 3018 ou 3020 (Education Nationale)**

# COMMENT PARLER DE CYBERSÉCURITÉ AVEC SES ENFANTS ?

Quotidiennement exposés aux outils numériques, mais souvent peu conscients des risques encourus dans leurs pratiques, les jeunes représentent des cibles faciles (cyberharcèlement, vol de données personnelles, piratage de comptes en ligne...). D'où l'importance de les sensibiliser et de les aider à acquérir des « réflexes » avec les bonnes pratiques, et ce, dès le plus jeune âge.

## QUE FAIRE FACE AUX CONTENUS ILLICITES SUR INTERNET ?

### DES MINEURS VICTIMES...

Au même titre que les adultes, les enfants peuvent être confrontés à des contenus choquants, parfois illicites : incitation à la haine, propagande terroriste, pédopornographie, etc. L'encadrement des mineurs dans leur navigation sur Internet reste donc un enjeu majeur. Cyberharcèlement, injure, diffamation, corruption de mineur, incitation à commettre un crime ou un délit... Pour signaler un contenu illicite sur Internet, rendez-vous sur le site du ministère de l'Intérieur www.internet-signalement.gouv.fr. Le 3018 propose également des informations sur ces dangers.

### ...OU AUTEURS DE CONTENUS ET DE COMPORTEMENTS ILLICITES

Il arrive également que les jeunes soient tentés de se rendre visibles sur les réseaux sociaux ou Internet, avec un fort sentiment d'impunité. Or, Internet n'est pas un espace de non-droit et contrairement à certaines légendes, l'anonymat absolu n'y existe pas. Sur le web, tout comme le monde « réel », des lois existent dont les mineurs et les familles ne sont pas toujours conscients. Selon la nature des infractions, les auteurs de propos illicites tenus sur Internet encourent des peines qui peuvent aller jusqu'à plusieurs milliers d'euros d'amende et même dans certains cas des peines d'emprisonnement.

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

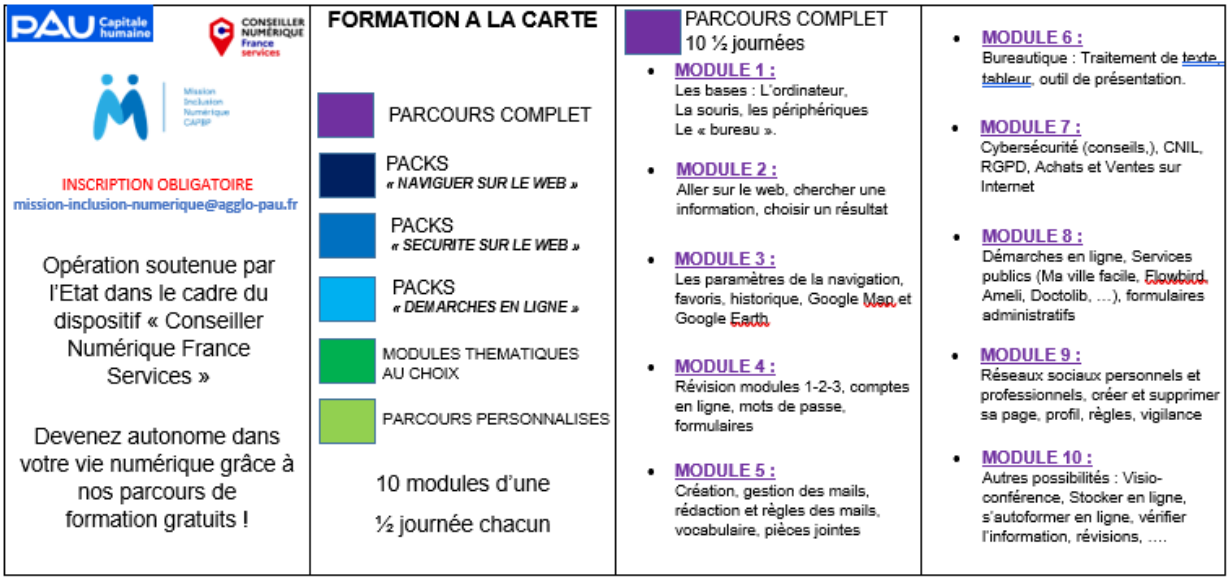
WWW.CYBERMALVEILLANCE.GOUV.FR

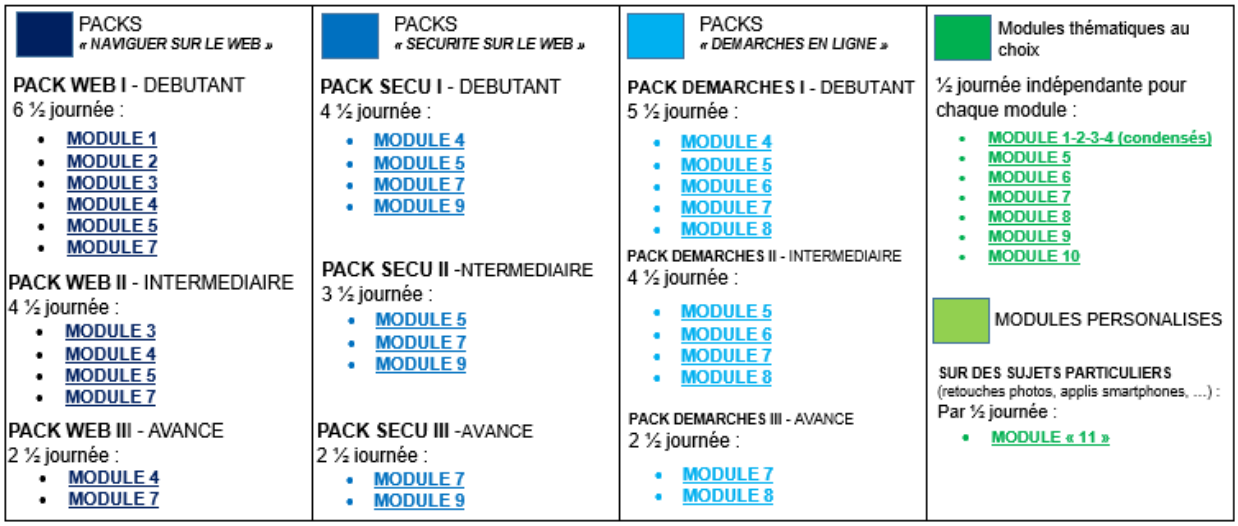
# Nos ateliers numériques gratuits

Vous souhaitez mieux maîtriser les outils numériques dans votre quotidien ou pour avoir accès à vos droits ou approfondir les conseils donnés dans ce cahier sur la cybersécurité ? n'hésitez pas à nous solliciter. Nous avons imaginé plein de modules pour vous aider !

Nous travaillons en partenariat étroit avec votre mairie, les Maisons France Services, les CCAS et d'autres acteurs de l'inclusion numérique.






Une petite video pour vous décider ? https://www.youtube.com/watch?v=MxWVBeSWdrE

# La Mission Inclusion Numérique, proche de vous

Le numérique, ce n'est pas si compliqué : nos ateliers sont proches de chez vous, gratuits et tout s'apprend facilement dans la bonne humeur, à votre rythme. Venez en confiance : nous sommes un service public au sein de la Communauté d'agglomération Pau Béarn Pyrénées.


**Formulaires d'inscription disponibles à l'accueil de votre mairie ou sur demande à :**

mission-inclusion-numerique@agglo-pau.fr