

Les cahiers de la Mission Inclusion Numérique

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

1



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 ...

2

ERREUR FATALE !!!

The infographic is divided into two main sections: 'MAUVAISES PRATIQUES !' (Bad Practices!) and 'BONNES PRATIQUES' (Good Practices!).

MAUVAISES PRATIQUES ! (Bad Practices!): Illustrated with a woman and a man. A speech bubble from the woman says '0000 ? 1234 ? c'est facile à retenir.' (0000 ? 1234 ? it's easy to remember). A speech bubble from the man says 'Fais comme moi, mets ta date de naissance !' (Do like me, put your date of birth!).

LES RISQUES (RISKS): A red-bordered box containing the text: 'En cas de vol d'un de vos mots de passe, tous les services pour lesquels vous l'utilisez pourraient être piratés. En d'autres termes, vous vous exposeriez alors à une prise de contrôle de l'ensemble de vos comptes par un individu malveillant qui pourrait vous dérober des informations personnelles pour en faire un usage frauduleux : usurpation d'identité, achats ou virements en votre nom, revente de vos données...' (In case of theft of one of your passwords, all the services for which you use them could be hacked. In other words, you would then be exposed to a takeover of all your accounts by a malicious individual who could steal your personal information for fraudulent use: identity theft, purchases or transfers in your name, sale of your data...)

LES CONSEILS (TIPS): A green-bordered box containing the text: 'Pour réduire les risques et éviter un piratage de vos différents comptes en ligne, nous vous recommandons d'utiliser des mots de passe suffisamment longs, complexes et différents pour accéder à chacun de vos équipements et services. Au moindre doute, ou même par prévention, n'hésitez pas à en changer et à activer la double authentification chaque fois que possible pour renforcer votre sécurité. Enfin, utilisez un gestionnaire de mots de passe pour les stocker de manière sécurisée.' (To reduce risks and avoid hacking of your different online accounts, we recommend using sufficiently long, complex and different passwords to access each of your equipment and services. At the slightest doubt, or even as a precaution, do not hesitate to change them and activate double authentication every time possible to strengthen your security. Finally, use a password manager to store them securely.)

BONNES PRATIQUES (GOOD PRACTICES): A green circle containing a smartphone icon and the text: 'Mots de passe : comme vos clés, CHOISISSEZ-EN UN DIFFÉRENT ET ROBUSTE POUR CHAQUE COMPTE.' (Passwords: like your keys, CHOOSE A DIFFERENT AND ROBUST ONE FOR EACH ACCOUNT.)

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, vidéos, contacts téléphoniques, documents bancaires, administratifs, factures, etc. Comment ne pas les perdre ?

En les sauvegardant régulièrement



The infographic is set against a light green background. At the top left, a cartoon illustration shows a woman and a man in a boat. The woman says, 'Oh non ! J'ai tout sur mon smartphone !' and the man asks, 'Tu ne fais pas de sauvegardes ?'. Below them is a black speech bubble with a sad face and the text 'MAUVAISES PRATIQUES !'. To the right, a red-bordered box titled 'LES RISQUES' contains text about the dangers of digital devices. Below that, a blue-bordered box titled 'LES CONSEILS' provides advice on backup methods. At the bottom left, a circular graphic shows a cloud, a USB drive, and a hard drive, with the text 'Sauvegardes : l'unique moyen DE RETROUVER VOS DONNÉES EN CAS DE PROBLÈME !' and 'BONNES PRATIQUES'.

LES RISQUES

Les appareils numériques (ordinateur, téléphone portable, tablette...) sont soumis à des risques qui peuvent entraîner une perte, parfois irréversible, de vos données. Ces situations sont plus nombreuses que vous ne l'imaginez : il peut s'agir d'un piratage, d'une panne, d'un vol ou d'une perte, voire de la destruction de votre appareil... La sauvegarde est alors souvent le seul moyen de retrouver vos données.

LES CONSEILS

Afin de prévenir de tels risques, Cybermalveillance.gouv.fr vous recommande fortement de réaliser des **sauvegardes régulières** de l'ensemble de vos appareils en ayant au préalable identifié les données que vous estimez importantes. Pensez à en conserver une **copie sur un support externe** (clé USB, DVD ou disque dur externe), que vous débranchez une fois la sauvegarde effectuée, pour éviter qu'elle ne soit détruite également en cas de piratage ou d'infection de votre appareil par un virus. Il existe par ailleurs des **services en ligne**, appelés « Cloud », qui offrent des fonctionnalités de sauvegarde de données. Ces solutions peuvent être gratuites ou payantes en fonction de la capacité de stockage dont vous avez besoin.

Sauvegardes : l'unique moyen DE RETROUVER VOS DONNÉES EN CAS DE PROBLÈME !

BONNES PRATIQUES

3

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.

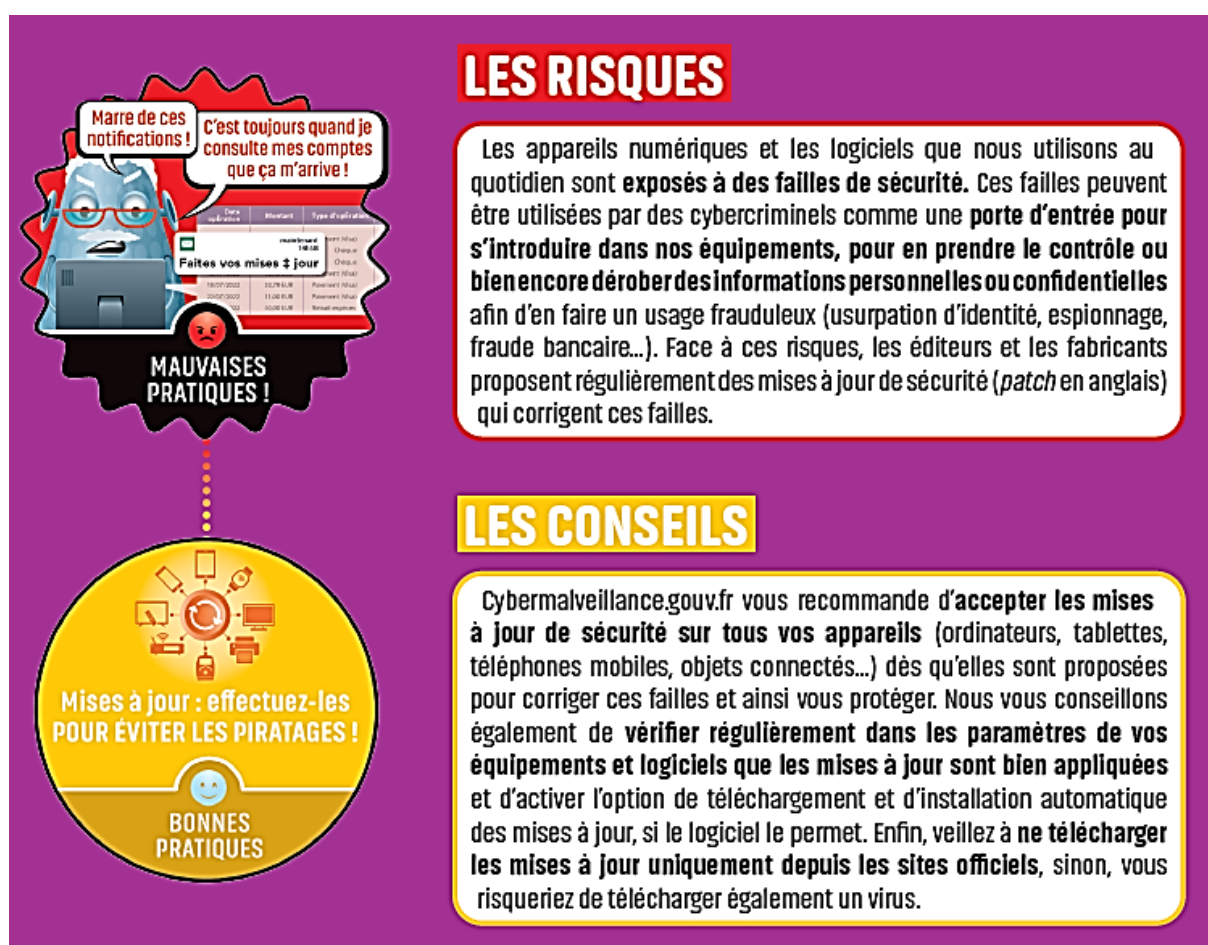
03– Procédez aux mises à jour de sécurité sur tous vos appareils

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 😞.

4

Protégeons nos données !



The infographic is set against a purple background. On the left, a cartoon character with a blue face and glasses looks frustrated. A speech bubble above it says "Marre de ces notifications!" and another says "C'est toujours quand je consulte mes comptes que ça m'arrive!". Below the character is a table of update notifications with columns for "Date", "Mise à jour", and "Type d'update". The table contains several rows of data. Below the table is a red speech bubble that says "Faites vos mises à jour" and a black speech bubble that says "MAUVAISES PRATIQUES!". A dotted line connects this to a yellow circle on the right. The yellow circle contains icons of various devices and a central refresh icon. Below the icons is the text "Mises à jour : effectuez-les POUR ÉVITER LES PIRATAGES !" and "BONNES PRATIQUES" with a smiley face icon.

LES RISQUES

Les appareils numériques et les logiciels que nous utilisons au quotidien sont **exposés à des failles de sécurité**. Ces failles peuvent être utilisées par des cybercriminels comme une **porte d’entrée pour s’introduire dans nos équipements, pour en prendre le contrôle ou bien encore dérober des informations personnelles ou confidentielles** afin d’en faire un usage frauduleux (usurpation d’identité, espionnage, fraude bancaire...). Face à ces risques, les éditeurs et les fabricants proposent régulièrement des mises à jour de sécurité (*patch* en anglais) qui corrigent ces failles.

LES CONSEILS

Cybermalveillance.gouv.fr vous recommande d’**accepter les mises à jour de sécurité sur tous vos appareils** (ordinateurs, tablettes, téléphones mobiles, objets connectés...) dès qu’elles sont proposées pour corriger ces failles et ainsi vous protéger. Nous vous conseillons également de **vérifier régulièrement dans les paramètres de vos équipements et logiciels que les mises à jour sont bien appliquées** et d’activer l’option de téléchargement et d’installation automatique des mises à jour, si le logiciel le permet. Enfin, veuillez à **ne télécharger les mises à jour uniquement depuis les sites officiels**, sinon, vous risqueriez de télécharger également un virus.

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.

5

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

On prend un antivirus pour notre ordinateur? **Non, pas besoin!**

MAUVAISES PRATIQUES!

LES RISQUES

Sans antivirus, vous exposez les équipements numériques de votre foyer à des virus informatiques cherchant à **porter atteinte à vos données** ou à **perturber le fonctionnement normal de vos appareils, à votre insu**. Les antivirus contribuent à vous protéger contre **le vol ou la destruction d’informations, l’espionnage ou le chantage**, voire à éviter de détourner vos appareils pour en attaquer d’autres.

LES CONSEILS

Nous vous recommandons d’utiliser un antivirus sur **tous vos équipements** (ordinateur, tablette, téléphone mobile...). Il existe de **nombreuses solutions gratuites ou payantes** selon vos usages et le niveau de protection recherché. N’hésitez pas à **vérifier régulièrement** que les antivirus de vos équipements sont bien à jour et à procéder à des analyses approfondies (scans) pour vérifier que vous n’avez pas été infecté.

L’antivirus = LE BOUCLIER CONTRE LES ATTAQUES!

BONNES PRATIQUES

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 ?



The infographic is set against a dark blue background. At the top left, a cartoon woman with blue skin and a black headscarf is shown in a red car-like shape, holding a smartphone. A speech bubble above her says 'Super! Un téléphone à 1€!'. Below her is a black speech bubble with a red sad face and the text 'MAUVAISES PRATIQUES !'. To the right, a white box with a red border contains the text 'LES RISQUES'. Below this, another white box with a green border contains 'LES CONSEILS'. At the bottom left, a green circular graphic shows a smartphone with a warning icon and the text 'MÉFIEZ-VOUS des offres alléchantes !' and 'BONNES PRATIQUES'.

LES RISQUES

Les criminels redoublent d'imagination et de savoir-faire pour essayer de vous abuser : messages hameçonnage (*phishing*) par SMS, mail ou téléphone, fausses annonces promotionnelles (bon de réduction, cadeaux...), faux sites de commerce en ligne ou créés pour les circonstances (fête des mères ou des pères...), faux sites « officiels », faux transporteurs, fausses confirmations de commandes... L'objectif : **vous voler vos données personnelles ou bancaires**, vous inciter à acheter un bien que vous ne recevrez jamais, à rappeler des numéros surtaxés ou à vous abonner à des services payants à votre insu.

LES CONSEILS

Choisissez de préférence un site d'achat français ou de l'Union Européenne : la réglementation européenne qui s'applique à tous ces sites en cas de litige vous protégera. Nous vous invitons également à **vérifier la notoriété et l'adresse des sites sur lesquels vous allez faire vos achats** : si c'est votre premier achat sur un site Internet, n'hésitez pas à taper son nom sur un moteur de recherche et à consulter les avis pour vous éviter des déconvenues. De plus, vérifiez bien l'adresse car un seul caractère dans le nom du site peut différer du site officiel. Et lorsque les offres sont trop alléchantes, nous vous conseillons de comparer le prix du produit recherché sur différents sites Internet pour vous assurer du caractère crédible de la vente. Enfin, **privilégiez les moyens de paiement les plus sécurisés** (Paylib, e-Carte Bleue...).

6

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

7

The infographic is set against a green background. At the top left, a purple cartoon character with glasses looks at a smartphone. A speech bubble above it says 'Tiens, un remboursement des impôts ?' and another below it says 'Allez, je force !'. To the right, a white envelope icon with a red 'X' is shown. Below the character, a black speech bubble contains the text 'MAUVAISES PRATIQUES !'. To the right of this is a red-bordered box titled 'LES RISQUES' containing text about stolen information being used by scammers. Below the character is a blue circular area with icons for an envelope, '@', a telephone, and a speech bubble. It contains the text 'Au moindre doute, CONTACTEZ L'ORGANISME CONCERNÉ.' and 'BONNES PRATIQUES' at the bottom. To the right of this is another white-bordered box titled 'LES CONSEILS' with advice on not clicking links and contacting the relevant organization.

LES RISQUES

Les informations dérobées (mots de passe, informations d'identité ou bancaires) seront ensuite **directement utilisées par les escrocs ou bien revendues** à d'autres cybercriminels pour mener diverses actions frauduleuses : piratage de compte en ligne, fraude à la carte bancaire, usurpation d'identité, hameçonnage ciblé sur la victime ou ses proches...

LES CONSEILS

Premier réflexe : **ne pas cliquer sur le lien qui vous est proposé. Au moindre doute, lors de la réception d'un message inattendu ou alarmiste, nous vous recommandons de contacter directement l'organisme concerné par un autre moyen** (exemple : par téléphone ou en se connectant par soi-même à son compte en ligne). Il peut en effet s'agir d'un message d'hameçonnage (phishing) visant à vous piéger.

Au moindre doute, CONTACTEZ L'ORGANISME CONCERNÉ.

BONNES PRATIQUES

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

8

The infographic is set against an orange background. At the top left, a cartoon girl with black hair and a red headband is holding a smartphone. A speech bubble above her says, 'Chouette, je vais pouvoir publier toutes les photos de la fête !'. Below her is a red jagged shape with a sad face icon and the text 'MAUVAISES PRATIQUES !'. To the right, a red box titled 'LES RISQUES' contains text about various threats like identity theft and fraud. Below that, a purple box titled 'LES CONSEILS' provides advice on strong passwords and privacy settings. At the bottom left, a purple circle with a smartphone icon and a smiley face is titled 'BONNES PRATIQUES' and contains text about checking security parameters.

LES RISQUES

Les réseaux sociaux n'échappent pas aux activités malveillantes : escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation... Les techniques frauduleuses ne manquent pas. **Certaines malveillances ciblent expressément les enfants et les adolescents sur les réseaux sociaux** : les jeux morbides ou dangereux déguisés en challenges, jeu-concours frauduleux, messages privés à caractère pornographique ou incitant à la prostitution...

LES CONSEILS

Pour utiliser les réseaux sociaux en toute sécurité et protéger l'accès à vos comptes, nous vous recommandons d'utiliser à la fois **des mots de passe robustes et systématiquement différents pour chaque service** mais aussi d'**activer la double authentification** lorsque cela est possible. Par ailleurs, nous vous recommandons de **vérifier régulièrement les paramètres de confidentialité de vos comptes** pour définir les options de visibilité de vos publications. Enfin, ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire et bien sûr, **faites attention à qui vous parlez sur les réseaux**.

MAUVAISES PRATIQUES !

Chouette, je vais pouvoir publier toutes les photos de la fête !

BONNES PRATIQUES

VÉRIFIEZ VOS PARAMÈTRES DE SÉCURITÉ pour contrôler vos données.

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](https://www.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



The infographic is set against a purple background. At the top left, a green cartoon character with a speech bubble says, 'Cheuette, j'ai du réseau! Je vais pouvoir consulter mes comptes bancaires!'. Below this is a red cloud with the text 'MAUVAISES PRATIQUES!' and a sad face icon. To the right, a red box titled 'LES RISQUES' contains text about security risks. Below that, an orange box titled 'LES CONSEILS' provides advice on using mobile networks instead of public WiFi. At the bottom left, a circular graphic shows a crossed-out Wi-Fi symbol and a Euro symbol, with the text 'Wi-Fi public : NE RÉALISEZ PAS D'OPÉRATIONS SENSIBLES!' and 'BONNES PRATIQUES!' below it.

LES RISQUES

En effet, les réseaux Wi-Fi publics ne sont pas toujours sécurisés et peuvent être contrôlés ou usurpés par des cybercriminels. Des pirates pourraient ainsi capturer vos informations personnelles : mots de passe, numéro de carte bancaire par exemple, pour les utiliser à des fins frauduleuses.

LES CONSEILS

En dehors de votre domicile, nous vous suggérons de privilégier la connexion de votre abonnement téléphonique (3G, 4G ou 5G) aux réseaux Wi-Fi publics. Si vous ne pouvez faire autrement, nous vous conseillons de vérifier scrupuleusement le nom du réseau proposé et celui affiché sur votre appareil et de ne jamais y réaliser d'opérations sensibles (paiement par CB, consultation de compte bancaire, renseignement d'informations confidentielles...).

Wi-Fi public :
NE RÉALISEZ PAS
D'OPÉRATIONS SENSIBLES !

BONNES PRATIQUES

9

3 précautions à prendre

- Évitez 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



The infographic is set against an orange background. At the top left, a cartoon illustration shows a green alien-like character with a speech bubble saying 'Non, pas besoin !' (No, no need!) and a blue character asking 'Tu as paramétré le babyphone ?' (Did you set up the baby monitor?). Below them is a baby's crib with a teddy bear and a red angry face icon, with the text 'MAUVAISES PRATIQUES !' (BAD PRACTICES!). To the right, a red box titled 'LES RISQUES' (THE RISKS) contains the text: 'Parce qu'ils ne sont pas toujours correctement sécurisés ou bien paramétrés, ces objets représentent de véritables menaces de piratage ou de vol d'informations personnelles. Ils peuvent donc constituer le « maillon faible » de notre environnement numérique.' (Because they are not always correctly secured or well configured, these objects represent real threats of hacking or theft of personal information. They can therefore constitute the « weak link » of our digital environment.) Below this, a teal box titled 'LES CONSEILS' (THE ADVICE) contains the text: 'Dès la première utilisation de votre objet connecté, changez le mot de passe par défaut et utilisez un mot de passe suffisamment long et complexe pour sécuriser chacun de vos équipements. Nous vous conseillons également de réaliser les mises à jour de sécurité et celles de leurs applications dès qu'elles vous sont proposées. Veillez aussi à vérifier leurs paramètres de sécurité en fonction de vos usages et à désactiver les fonctionnalités que vous n'utilisez pas. Enfin, nous vous conseillons d'éteindre systématiquement vos objets connectés lorsque vous ne les utilisez pas.' (From the first use of your smart object, change the default password and use a sufficiently long and complex password to secure each of your devices. We also advise you to carry out security updates and those of their applications as soon as they are proposed to you. Also be sure to check their security parameters according to your usage and to deactivate the features that you do not use. Finally, we advise you to turn off your smart objects systematically when you do not use them.) At the bottom left, a teal circle with a house icon and a smiley face contains the text: 'Objets connectés : MODIFIEZ LE MOT DE PASSE PAR DÉFAUT pour éviter les intrusions !' (Smart objects: CHANGE THE DEFAULT PASSWORD to avoid intrusions!) and 'BONNES PRATIQUES' (GOOD PRACTICES).

10

Alexa ? Siri ? Echo ? Non, vous n'appellez 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

11

The infographic is divided into two main sections: 'LES RISQUES' (Risks) and 'LES CONSEILS' (Advice). On the left, there are two circular icons. The top one, labeled 'MAUVAISES PRATIQUES !' (Bad Practices!), shows a cartoon character with a sad face and a speech bubble saying 'Oh la honte ! Je vais garder ça pour moi...' (Oh shame! I'll keep this for myself...). It is surrounded by various cyberbullying scenarios like 'RECEVOIR DES LIKES' (Receiving likes), 'Être à son adresse en direct' (Being at one's address live), 'Mettre un lien sur son profil' (Putting a link on one's profile), and 'Séparer tu fais trop PTTT' (Separating you do too much PTTT). The bottom icon, labeled 'BONNES PRATIQUES' (Good Practices!), shows a hand holding a lifebuoy with the text 'HELP HELP' and 'Victime ou témoin, PARLEZ-EN !' (Victim or witness, talk about it!).

LES RISQUES

Les conséquences du cyberharcèlement sur la santé physique ou morale de ceux qui en sont victimes ne doivent pas être minimisées. Elles **peuvent s'avérer importantes voire dramatiques** : sentiment d'insécurité, dépression, décrochage scolaire ou professionnel, troubles psychologiques ou émotionnels, violence en tout genre... Et peuvent même parfois conduire au suicide.

LES CONSEILS

Il est important de ne pas rester seul face au cyberharcèlement et de libérer la parole dans un cadre apaisé. Aussi **nous vous conseillons d'aborder le sujet du cyberharcèlement en famille avec vos enfants pour expliquer de quoi il peut s'agir et de les encourager à vous en parler s'ils sont témoins, victimes ou susceptibles d'être contributeurs.**

Voici un exemple de questions pour engager la discussion : *Tu sais ce que c'est que le cyberharcèlement ? As-tu déjà vu des situations de cyberharcèlement ? Que ferais-tu si tu voyais ou subissais un cyberharcèlement ?*

Si un cyberharcèlement se produit dans le cadre scolaire, informez-en la direction de l'établissement pour qu'elle puisse prendre les mesures nécessaires.

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 encourrent des peines qui peuvent aller jusqu'à plusieurs milliers d'euros d'amende et même dans certains cas des peines d'emprisonnement.

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.

  <p>INSCRIPTION OBLIGATOIRE mission-inclusion-numerique@agglo-pau.fr</p> <p>Opération soutenue par l'Etat dans le cadre du dispositif « Conseiller Numérique France Services »</p> <p>Devenez autonome dans votre vie numérique grâce à nos parcours de formation gratuits !</p>	<p>FORMATION A LA CARTE</p> <ul style="list-style-type: none">  PARCOURS COMPLET  PACKS « NAVIGUER SUR LE WEB »  PACKS « SECURITE SUR LE WEB »  PACKS « DEMARCHES EN LIGNE »  MODULES THEMATIQUES AU CHOIX  PARCOURS PERSONNALISES <p>10 modules d'une ½ journée chacun</p>	<p>PARCOURS COMPLET 10 ½ journées</p> <ul style="list-style-type: none"> • MODULE 1 : Les bases : L'ordinateur, La souris, les périphériques Le « bureau ». • MODULE 2 : Aller sur le web, chercher une information, choisir un résultat • MODULE 3 : Les paramètres de la navigation, favoris, historique, Google Map, et Google Earth • MODULE 4 : Révision modules 1-2-3, comptes en ligne, mots de passe, formulaires • MODULE 5 : Création, gestion des mails, rédaction et règles des mails, vocabulaire, pièces jointes 	<ul style="list-style-type: none"> • MODULE 6 : Bureautique : Traitement de texte, tableur, outil de présentation. • MODULE 7 : Cybersécurité (conseils), CNIL, RGPD, Achats et Ventes sur Internet • MODULE 8 : Démarches en ligne, Services publics (Ma ville facile, Flowbird, Ameli, Doctolib, ...), formulaires administratifs • MODULE 9 : Réseaux sociaux personnels et professionnels, créer et supprimer sa page, profil, règles, vigilance • MODULE 10 : Autres possibilités : Visio-conférence, Stocker en ligne, s'autoformer en ligne, vérifier l'information, révisions, ...
--	--	---	--

<p> PACKS « NAVIGUER SUR LE WEB »</p> <p>PACK WEB I - DEBUTANT 6 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 1 • MODULE 2 • MODULE 3 • MODULE 4 • MODULE 5 • MODULE 7 <p>PACK WEB II - INTERMEDIAIRE 4 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 3 • MODULE 4 • MODULE 5 • MODULE 7 <p>PACK WEB III - AVANCE 2 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 4 • MODULE 7 	<p> PACKS « SECURITE SUR LE WEB »</p> <p>PACK SECU I - DEBUTANT 4 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 4 • MODULE 5 • MODULE 7 • MODULE 9 <p>PACK SECU II - INTERMEDIAIRE 3 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 5 • MODULE 7 • MODULE 9 <p>PACK SECU III - AVANCE 2 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 7 • MODULE 9 	<p> PACKS « DEMARCHES EN LIGNE »</p> <p>PACK DEMARCHES I - DEBUTANT 5 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 4 • MODULE 5 • MODULE 6 • MODULE 7 • MODULE 8 <p>PACK DEMARCHES II - INTERMEDIAIRE 4 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 5 • MODULE 6 • MODULE 7 • MODULE 8 <p>PACK DEMARCHES III - AVANCE 2 ½ journée :</p> <ul style="list-style-type: none"> • MODULE 7 • MODULE 8 	<p> Modules thématiques au choix</p> <p>½ journée indépendante pour chaque module :</p> <ul style="list-style-type: none"> • MODULE 1-2-3-4 (condensés) • MODULE 5 • MODULE 6 • MODULE 7 • MODULE 8 • MODULE 9 • MODULE 10 <p> MODULES PERSONALISES</p> <p>SUR DES SUJETS PARTICULIERS (retouches photos, applis smartphones, ...): Par ½ journée :</p> <ul style="list-style-type: none"> • MODULE « 11 »
---	--	--	---

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.



Un atelier
chaque semaine
proche de chez vous

Par groupe
de 6 personnes

C'est GRATUIT

N'hésitez plus :
Inscrivez-vous maintenant !

2023

Ateliers numériques gratuits

Ne laissez pas une souris vous gâcher la vie, apprivoisez-la !

Un parcours complet ou des modules ciblés, gratuits et animés par un professionnel certifié !

Vous êtes un peu perdus dans les outils et les usages numériques ?
Du 1er clic aux fonctions avancées des outils numériques et d'Internet, **devenez autonome dans vos démarches** : formulaires administratifs en ligne, se prémunir contre la cybermalveillance, mieux connaître les réseaux sociaux, créer et gérer sa messagerie, les outils bureautiques, naviguer facilement sur Internet, installer des applis...



INFORMATIONS ET INSCRIPTIONS OBLIGATOIRES

A l'accueil de votre Mairie
ou par courriel :
mission-inclusion-numerique@agglo-pau.fr

LIEUX DES ATELIERS

GAN
Tous les mardis de 9h00 à 12h00

OUSSE
Tous les mardis de 14h15 à 17h15

LESCAR
Les mercredis de 9h00 à 12h00
et de 14h15 à 17h15

POEY DE LESCAR
Tous les lundis de 9h15 à 12h15

PAU BEARN
PYRÉNÉES
Communauté d'Agglomération



Mission
Inclusion
Numérique
CA 2017



**CONSEILLER
NUMÉRIQUE
France
services**

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

mission-inclusion-numerique@agglo-pau.fr