AXA Prévention

Guide des bonnes pratiques numériques

Sommaire

Protéger votre ordinateur

Lors de votre navigation sur Internet, des virus ou des logiciels espions peuvent infecter votre tablette ou smartphone. Ils sont susceptibles d'y prélever des informations personnelles à votre insu, voire d'endommager votre matériel informatique.

Certains de ces virus peuvent survivre lorsque vous mettez votre appareil hors tension et l'endommager lors de la remise sous tension, car ils vont se loger dans les mémoires de la machine. Spams, téléchargements non sécurisés, sites douteux, les menaces sont nombreuses : restez vigilant.

Installer un anti-virus

Installer un antivirus est la première étape pour faire face aux risques numériques ! C'est la base de la protection. La fonctionnalité première de ces antivirus est d'analyser votre disque dur interne pour détecter les possibles attaques.

Installer un antispyware

Le spyware est un logiciel malveillant qui a pour but de récupérer vos données et de transférer ces informations sans que vous ne vous en rendiez compte. Le but de cette récolte de données est très souvent commercial. Les spywares ralentissent votre ordinateur et c'est pour cette raison qu'il faut les stopper avec un antispyware.

Effacer les traces de navigation

Un Cookie, c'est quoi ? On ne parle pas de ce bon gâteau rempli de pépites de chocolat, mais d'un fichier déposé sur votre ordinateur qui absorbe des informations clés qu'il transmet à votre navigateur de recherche. En plus clair, c'est un cafeteur invisible ! Il va communiquer à votre navigateur vos goûts et vos préférences de navigation. Vous avez sûrement été confronté aux pouvoirs du cookie : l'autre jour, vous avez acheté une nouvelle paire de chaussures sur Internet et, comme par magie, les jours suivants, vous voyez apparaître des chaussures sur toutes les publicités des sites que vous consultez.

Sécurisez votre smartphone

Le smartphone devient notre troisième main, une extension de nous-mêmes. Il contient des informations précieuses à notre sujet. C'est pour cette raison qu'il faut le sécuriser.

Comment sécuriser votre téléphone ?

+ Pensez à personnaliser votre code PIN dans vos paramètres. Il vous sera demandé à chaque fois que vous allumez votre smartphone.
+ Mettez en place un code de verrouillage afin que votre smartphone, même allumé, soit en permanence sécurisé.
+ Veillez à conserver le code IMEI noté sur la boîte de l'emballage de votre téléphone car il peut vous être très utile. En cas de perte ou de vol, ce code sert à bloquer l'usage du téléphone sur tous les réseaux. Si vous avez perdu votre boîte d'emballage, pas de souci : vous pouvez également l'obtenir en tapant *#06# sur votre téléphone.
+ Chiffrez c'est-à-dire « verrouiller » vos données :

1. Rechargez votre smartphone jusqu'à au moins 80 %.
2. Allez dans les « Paramètres » puis dans « Sécurité » et cliquez sur « chiffrer ».
3. Le mot de passe vous sera demandé à chaque déverrouillage.

Choisir les mots de passe efficaces

Le saviez-vous ?

17 % des internautes utilisent leur date de naissance comme mot de passe. Rien de plus facile pour un pirate du Net !

Choisir un bon mot de passe, c'est-à-dire un mot de passe plus complexe que sa date de naissance, est une des étapes clés pour protéger vos données. Le nombre de comptes piratés (Facebook, Yahoo, Hotmail…) ne cessent d'augmenter. Et ce piratage peut être lourd de conséquences comme l'usurpation d'identité ou la récupération de données. Le mot de passe est donc un outil qui assure la sécurité sur Internet.

À quoi ressemble le mot de passe idéal ?

- Pas trop court (>10 caractères).
- Pas identique à l'identifiant/pseudo.
- Pas de données personnelles : date de naissance, prénom…
- Pas d'uniformité : il faut des minuscules, majuscules, chiffres et caractères spéciaux.

6 commandements du mot de passe

1. Changez régulièrement vos mots de passe.
2. Ne divulguez à personne vos mots de passe.
3. Ne les stockez pas sur un simple fichier Word.
4. N'utilisez pas le même mot de passe pour tous les services.
5. Ne vous envoyez pas vos mots de passe via e-mail.
6. Supprimez les mails de création de compte comportant votre identifiant et mot de passe.

Les réseaux sociaux

Les réseaux sociaux sont des outils de communication conçus pour des adultes et des adolescents de plus de 13 ans (c'est l'âge minimum requis pour pouvoir créer un compte sur n'importe quel réseau social, y compris Snapchat et Tik Tok - anciemment Musically).
Il est important de respecter ces limites d'âge, car ces réseaux ont de très nombreux utilisateurs.

2,2 milliards
sur Facebook

1 milliard
sur Instagram

255 millions
sur Snapchat

Protégez votre compte

Désactivez l'option qui permet de publier un contenu directement sur votre compte. Allez dans l'étoile en haut à droite de votre page d'accueil, puis sur compte, puis « journal et identification » et « qui peut ajouter des contenus dans mon journal » et choisissez : « moi uniquement ».

Bien paramétrer ses comptes

Il est indispensable de prendre le temps de se plonger dans les paramètres de confidentialité de vos profils sur les réseaux sociaux afin de les utiliser en toute sécurité.

Les réseaux sociaux (suite)

Facebook

Si aucun paramètre de confidentialité n'est réglé sur le site, le profil est public, tout le monde peut donc voir vos publications, notamment les photos, et vous envoyer des messages.

Choisissez les photos dans lesquelles vous apparaissez

Détaguez vous d'une photo en cliquant sur elle, puis en cliquant sur « options » et « retirer l'identification ». Cliquez sur le cadenas en haut à gauche de votre page d'accueil, puis « afficher plus de paramètres », allez ensuite dans « Journal et identification » et dans la section « Examiner les publications dans lesquelles vos amis vous identifient avant qu'elles n'apparaissent sur votre journal ». Une fois cette option activée, à chaque fois que vous serez tagué sur une photo ou un statut, une autorisation sera nécessaire.

Choisissez avec qui vous partagez vos infos.

Allez dans confidentialité et choisissez « qui peut voir vos futures publications ? » : public, amis, moi uniquement, personnalisé, etc. Cette dernière option permet de restreindre la visibilité des contenus à une ou plusieurs listes de contacts (amis proches, connaissances, travail…) ou à certaines personnes individuellement. Pratique pour diffuser ses photos de vacances à la plage aux amis proches mais pas à ses connaissances du travail ! Sélectionnez qui peut voir vos amis : vous pouvez configurer qui peut aller voir avec qui vous êtes amis sur Facebook. Cliquez sur le bloc « Amis » sur votre profil puis sur « Modifier », et choisissez l'option que vous préférez.

Rangez vos « amis » Facebook

Listes d'amis proches, famille, réseau professionnel…
Pour ce faire, allez sur le profil de chaque ami puis passez la souris sur « Amis » (sous la photo de couverture) et ajoutez-le à « Nouvelle liste » que vous créerez directement. Facebook propose déjà une liste « Amis proches ».

Contrôler sa e-réputation

Les outils pour veiller sur mon e-réputation

Google : tapez vos « **prénom nom** » entre guillemets et lancez la recherche. Quels liens apparaissent dans les premiers résultats ? Vous conviennent-ils ? Sont-ils toujours d'actualité ?

Google Alerts : en paramétrant **une alerte sur vos noms et prénoms**, Google vous enverra automatiquement un mail à chaque fois qu'il détectera une nouvelle publication vous mentionnant. Pratique pour ne rien manquer.

Tweetdeck : relié à votre compte Twitter, cet outil vous permet de **suivre ce qui se dit sur Twitter**. Vous pouvez suivre votre nom + prénom et votre handle.

Comment réagir si je suis cité sur une page web et que cela me gêne ?

Je **contacte l'administrateur du site** pour lui demander sa modification/sa suppression (le site whois.net vous aide à retrouver son nom et ses coordonnées). Je peux également faire une **demande de déréférencement à Google.**

https://support.google.com/legal/contact/lr_eudpa?product=websearch

En cas de refus ou d'absence de réponse sous 2 mois, je peux **saisir la CNIL par courrier** (des modèles sont disponibles sur leur site) qui **étudiera alors le dossier** et délibèrera en faveur ou non d'une suppression du contenu.

Si après toutes ces démarches, je n'obtiens pas gain de cause, je peux également **faire une demande de Droit à l'Oubli** auprès de Google.

Les pratiques pour garder une bonne e-réputation

- Bien régler mes **paramètres de confidentialité** afin de protéger ma vie privée.
- Veiller à toujours **être courtois et bienveillant** dans mes échanges.
- Me **Googler régulièrement**.
- Rester **vigilant à la qualité** de ce que je partage (source, pas de photos compromettantes, ...).

Comment réagir en cas de... ?

Il arrive parfois que nous ne sachions pas comment réagir face à une situation nouvelle. Elle peut être d'autant plus perturbante alors que l'on commence à peine à se familiariser avec ce nouvel environnement. Pas de panique, voici les principaux réflexes à adopter.

Quelques conseils d'usage des réseaux sociaux en cas de situations d'urgence

(attentats, sinistres d'ampleur, inondations...).

- Ne relayez pas **de fausses informations** et appuyez-vous sur les informations fournies par les **comptes officiels** (gendarmerie nationale, ministère de l'Intérieur).
- Signalez toute **atteinte à la dignité** : création et diffusion de contenus explicitement choquants (photos, vidéos post événements).
- Par respect pour les familles et les victimes, ne relayez pas de photos montrant des **scènes choquantes**.
- Sur Twitter, lorsque vous parcourez votre flux d'actualité les vidéos se **lancent automatiquement**, sans que vous puissiez contrôler le contenu qui va être visualisé. Si vous le souhaitez, vous pouvez **désactiver cette fonctionnalité** : Cliquez sur votre photo de profil → Paramètres et confidentialité → Dans la rubrique « Contenu » décochez la case « Lecture automatique des vidéos ».

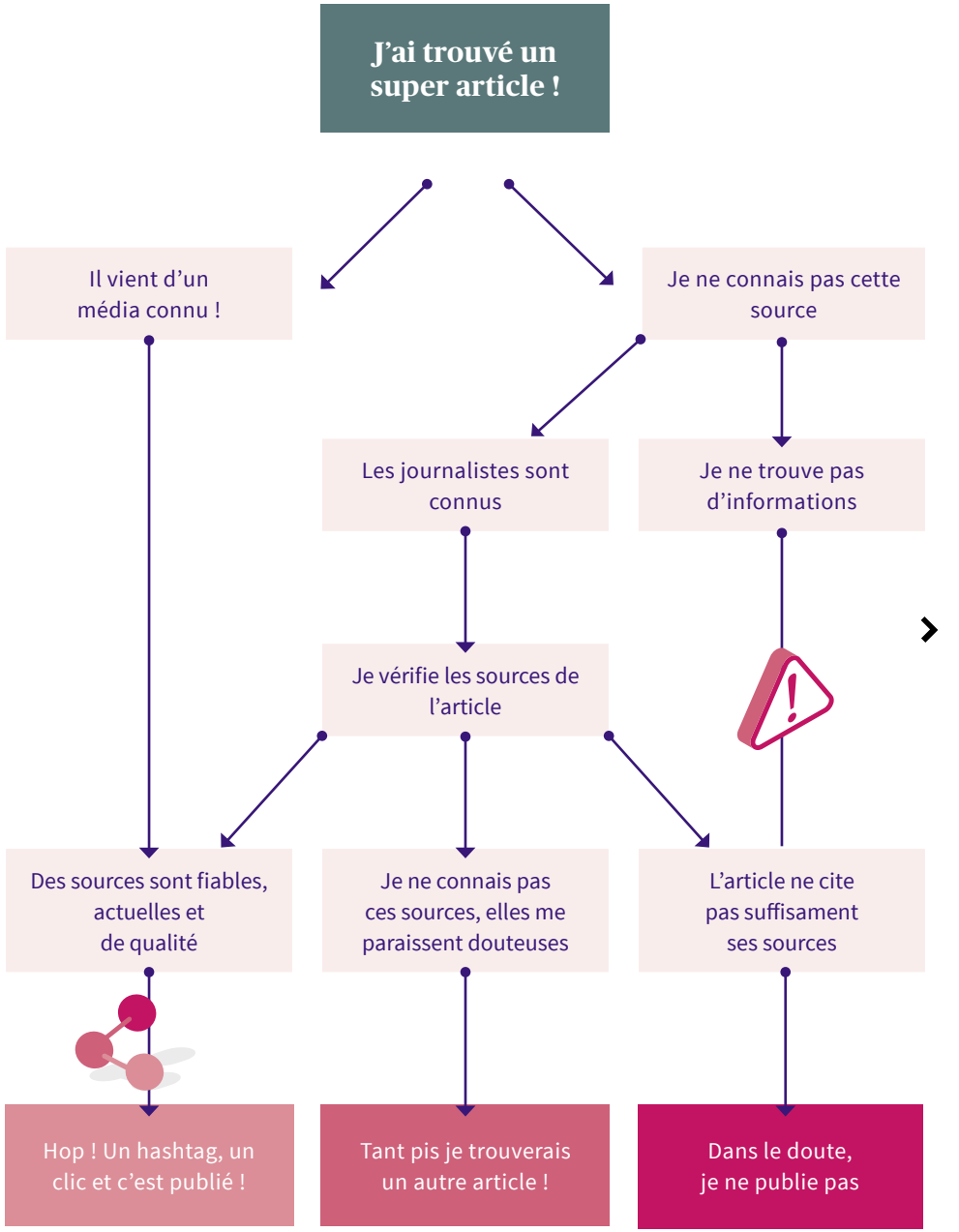
Je constate des contenus illicites

(appel à la haine raciale, diffusion images choquantes...).

- Vous pouvez saisir directement les **administrateurs** de la plateforme à l'aide d'un bouton dédié.
- Vous pouvez saisir les autorités via **la plateforme Pharos**. Les signalements envoyés sont traités par des policiers et gendarmes.
- Attention : ne faites **jamais une capture écran** d'un contenu choquant impliquant un mineur, transmettez simplement l'URL aux autorités concernées.

Comment éviter les fake news ?

Les fausses informations... on n'arrête pas d'en entendre parler. Facebook et Google leur ont même ouvertement déclaré la guerre ! Mais comment les éviter ?



Hyper connecté(e) : comment rester zen ?

Un tweet par-ci, un partage par-là, vous **multipliez les connexions** sur les réseaux sociaux, mais à partir de quand cela peut-il **devenir problématique** ?

Avez-vous déjà entendu parler du **syndrome FOMO** (fear of missing out) ? Hyper connectées, certaines personnes souffrent d'angoisse à l'idée de rater quelque chose.

Il peut s'agir d'une actualité ou la peur de passer à côté d'un événement relayé sur les réseaux sociaux (une soirée ou un anniversaire) plus intéressant que ce que nous sommes en train de faire. Il s'agit souvent des premiers pas vers une **addiction aux écrans**. Voici **3 conseils pour souffler un coup** et que tout se passe pour le mieux :

CONSEIL N°1

Pas d'écrans une heure avant le coucher

La lumière bleue émise par les tablettes et les smartphones **affecte la mélatonine** (l'hormone du sommeil) ainsi que votre **horloge biologique**, ce qui provoque des troubles du sommeil. Alors **le soir, évitez les écrans** au moins 1 h avant l'heure du coucher. Vous aurez moins de mal à vous endormir et votre sommeil sera plus récupérateur.

CONSEIL N°2

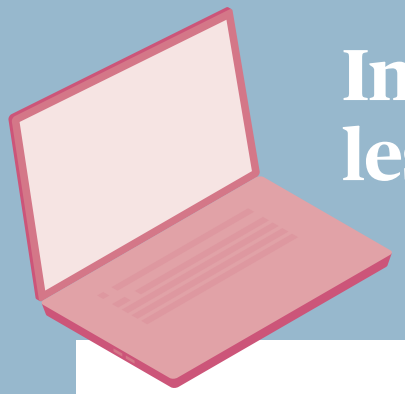
Déconnectez-vous

Désactivez les notifications de votre smartphone afin de ne pas recevoir d'alertes sonores en continu.
La « **Digital Detox** » vous connaissez ? N'hésitez pas durant vos vacances à vous **détacher des nouvelles technologies** et de profiter de l'instant présent.

CONSEIL N°3

Soyez cool

Vous n'avez **pas vu cette info ou cette publication ?** Ce n'est pas grave ! Ménager une **distance avec les réseaux sociaux**, c'est aussi ne pas se sentir coupable de ne pas être au courant ou de ne pas avoir vu !



Internet et les enfants

Sur Internet

De la même façon que vous savez où votre enfant va dans la rue, vous devez savoir où il va sur Internet : quels sites il fréquente. Il en va de même pour ses amis : vous connaissez ses amis dans la vie, il est souhaitable de connaître ceux avec qui il discute sur Internet. Il est important de connaître l'identité de votre enfant sur Internet.

Pour garantir sa sécurité et la vôtre, vous devez l'aider à construire des pseudos et mots de passe sûrs.

Un pseudo fiable ne doit donner aucune indication sur le nom, le prénom, la localisation géographique ou encore l'âge de votre enfant. Un mot de passe fiable doit comporter des lettres, des chiffres, des caractères spéciaux en évitant les mots de passe évidents comme ceux reprenant le prénom ou la date de naissance de votre enfant.

Il est également important de contrôler le temps passé sur Internet et les réseaux sociaux.

Enfin, la loi s'applique aussi sur Internet : les parents sont responsables de ce que leurs enfants publient. Il faut donc leur expliquer de ne rien publier qui puisse nuire à quelqu'un d'autre. Un « cyberharceleur » de 13 à 15 ans risque jusqu'à 18 mois de placement en centre éducatif fermé et 7 500 € d'amende.

AXA Prévention accompagne les plus jeunes depuis 2013, en partenariat avec les Forces de l'ordre, avec le programme Permis Internet, programme national de responsabilisation des élèves de CM2 pour un usage vigilant, sûr et responsable d'Internet et des réseaux sociaux.

Retrouvez toutes les informations utiles sur : permisinternet.fr

PERMIS INTERNET pour les enfants

Les réseaux sociaux

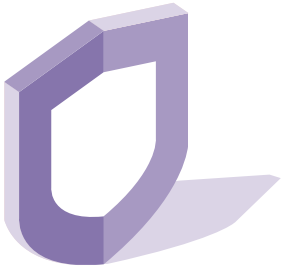
Afin que votre enfant soit bien protégé sur les réseaux sociaux, accompagnez-le lors de son inscription, notamment lorsque vient l'étape de configuration des paramètres de confidentialité.

Rappelez-lui les règles fondamentales d'utilisation :

1. S'assurer de connaître personnellement chacun des contacts. Ne jamais accepter d'invitation d'un inconnu.
2. Paramétrer avec l'aide d'un adulte les options de confidentialité de son profil… et vérifier tous les 2 mois.
3. Avant de publier quelque chose sur un réseau social, une photo par exemple, toujours se demander si on montrerait la même chose à tout le monde dans la cour du collège ? Si la réponse est « non », ne pas publier : tout ce qui est pubié sur un réseau social (même en « privé ») peut toujours devenir PUBLIC. Sur Snapchat, la disparition des photos est une illusion : toute photo peut être « screenée » (capturée) et rediffusée. Toutes les photos sont conservées sur les serveurs de Snapchat pour une durée indéterminée.

En cas d'abus sur un réseau social, ou de cyber-harcèlement

Il n'est jamais acceptable d'être moqué, injurié ou diffamé. Encore moins sur Internet, car la diffusion est massive et incontrôlable. Si votre enfant est victime d'un abus, conseillez-lui d'en parler tout de suite à un adulte. En cas de problème, on peut contacter gratuitement Net Ecoute au 0800 200 000 ou le 30 20 (Non au harcèlement) et consulter des conseils sur : www.nonauharcelement.education.gouv.fr



Se protéger de la délinquance numérique

Ne pas publier sur un site sa date et son lieu de naissance, ni son adresse **personnelle.** Ce sont des éléments d'identification forts.

Ne pas se vanter de son **patrimoine** ou du dernier luxe qu'on s'est offert en postant des photos, par exemple.

Ne jamais envoyer **d'argent** quand un internaute en réclame !

Vérifier à deux fois le téléchargement ou l'exécution des pièces jointes signalées comme suspectes par votre ordinateur. Idem pour les fichiers d'un site web sur lequel vous avez atterri après avoir cliqué sur un lien d'origine incertaine.

Rester **méfiant** avec les mails personnalisés envoyés par un tiers de confiance, sollicitant mots de passe ou codes de **carte bleue.**

Ne pas crier sur les toits que l'on part en vacances, en déplacement ou en week-end pour ne pas faciliter le travail des **cambrioleurs.**

Être **vigilant** sur les mails que l'on reçoit, en vérifiant le nom et l'adresse de l'expéditeur.

AXA Prévention

Ce guide vous est offert par AXA Prévention dans le cadre de ses actions d'éducation aux risques.

Association à but non lucratif, **AXA Prévention** contribue au développement de **comportements responsables face aux risques du quotidien** (santé, accidents de la route, dangers du web) et intervient sur l'ensemble du territoire français avec de nombreuses actions de prévention.
Retrouvez tous les conseils et services de prévention sur **axaprevention.fr** et sur **@AXAprevention**.

Réf. 973747 03 2019 SGI - crédits photos : Shutterstock