Assurance & Protection
Épargne & Retraite

abeille ASSURANCES

Notre guide pour assurer la sécurité de votre famille en ligne

Sommaire

Top 10
des questions les plus posées

Afin de mieux garantir la sécurité de votre famille en ligne, consultez nos conseils en cliquant sur le lien de chaque question. Il s'agit des questions les plus récurrentes sur le sujet.

- Que faire en cas de perte ou vol de mon smartphone ?
- Je m'occupe actuellement d'une personne vulnérable. Comment puis-je l'aider à naviguer sur Internet en toute sécurité ?
- Les mots de passe sont essentiels pour aider ma famille à rester en sécurité. Quels conseils pouvez-vous me donner ?
- J'ai un certain nombre d'appareils connectés à Internet dans ma maison, y compris des caméras de vidéosurveillance. Comment puis-je m'assurer qu'ils sont tous sécurisés ?
- Comment savoir si mon adresse e-mail est impliquée dans une violation de données ? Que puis-je faire pour me protéger ?
- Les réseaux Wi-Fi publics sont-ils sécurisés ?
- Comment éviter la diffusion en ligne de contenus préjudiciables me concernant ?
- Mon enfant subit un harcèlement en ligne. Que puis-je faire pour le protéger ?
  - 8-10 ans
  - 11-13 ans
- Mon enfant joue à des jeux en ligne. Comment le protéger ?
  - 4-7 ans
  - 8-10 ans
  - 11-13 ans
- Comment empêcher mes enfants de voir des contenus choquants en ligne ?
  - 4-7 ans
  - 8-10 ans
  - 11-13 ans

1 Bienvenue dans notre guide

À l'ère du numérique, la plupart d'entre nous utilisent de nombreux outils en ligne dans le cadre de notre vie quotidienne. Nous utilisons Internet pour travailler, apprendre et nous divertir. Nous nous tournons vers le Web lorsque nous avons besoin de payer des factures, de faire des achats, de rester en contact avec nos amis ou de trouver l'amour. Il n'y aucun aspect de notre vie qui n'est pas touché d'une manière ou d'une autre par la technologie numérique.

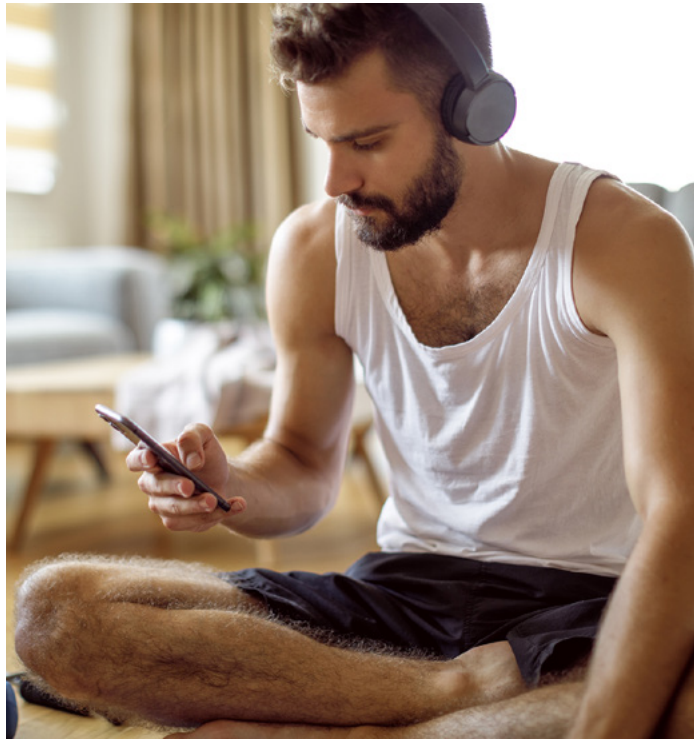
Notre monde s'est ouvert, notre accès à l'information s'est élargi et, bien que cela apporte d'énormes avantages, cela n'est pas non plus sans risque.

Ce guide nous permet de vous aider, ainsi que vos proches, à rester en sécurité dans le monde du numérique, que vous soyez à la maison ou au travail. Pensez à l'utiliser pour aborder ce sujet au plus tôt avec les jeunes enfants et établir un dialogue continu avec eux sur leur vie en ligne. Vous trouverez également de nombreuses recommandations pour les personnes âgées et les adultes vulnérables. Nous avons rassemblé des conseils d'experts de confiance afin que vous soyez sûr de faire tout ce qui est en votre pouvoir pour vous protéger, vous et votre famille.

Ce guide a été conçu pour créer des discussions entre les parents et leurs jeunes enfants et donc entamer un dialogue continu sur tous les sujets liés au numérique dès le plus jeune âge. À mesure que vos enfants avancent en âge et gagnent en indépendance, nous vous suggérons de leur transmettre ce guide afin qu'ils puissent parcourir ces conseils par eux-mêmes. Partagez ce guide avec votre famille et vos amis afin qu'ils puissent explorer le monde numérique en toute confiance.

2 Des conseils pour tous les usagers d'Internet

Aujourd'hui, nous sommes tous des citoyens numériques. Même les personnes qui choisissent de ne pas être présentes sur les réseaux sociaux ont sans doute un smartphone ou une télévision. Voici quelques conseils pour vous garantir une sécurité maximale dans ce nouveau monde plein de possibilités.



L'Internet des objets (IdO)

L'Internet des objets est le terme utilisé pour décrire les produits et appareils qui étaient auparavant hors ligne et qui peuvent désormais être connectés à un réseau pour collecter et échanger des données. Cela englobe toutes sortes d'objets, des baby-phones aux compteurs d'électricité intelligents, en passant par les dispositifs de suivi de santé portables et les assistants personnels intelligents (comme Alexa). Même les ampoules, les brosses à dents électriques, les serrures de porte et les lave-linges sont actuellement adaptés pour pouvoir rejoindre l'IdO.

S'il présente des avantages comme vous faire économiser de l'énergie en allumant votre chauffage depuis votre téléphone alors que vous êtes dans le bus, il comporte aussi certains risques. C'est un domaine entièrement nouveau qui comprend encore quelques faiblesses. C'est pourquoi le gouvernement et le secteur collaborent pour développer des lois et politiques qui renforcent la sécurité de l'IdO et protègent les consommateurs.

Voici les conseils pour utiliser des appareils connectés en toute sécurité :

1. **Faites vos recherches**
   Avant d'acheter un produit, prenez le temps de lire des avis d'experts et de consommateurs.

2. **Lisez le manuel**
   Le fabricant doit expliquer clairement comment fonctionnent les paramètres de confidentialité et indiquer s'il est nécessaire d'utiliser une application pour utiliser l'appareil en toute sécurité.

3. **Modifiez votre mot de passe**
   Ne vous contentez pas de conserver le mot de passe paramétré par défaut sur l'appareil. Créez-en un nouveau suffisamment fort. Pour plus d'informations, consultez ce guide sur les mots de passe.

4. **Paramétrez le Bluetooth sur « non détectable »**
   Si un périphérique est compatible Bluetooth, il peut se connecter aux appareils à proximité sans avoir à se connecter à Internet. La modification des paramètres l'empêchera de partager des données ou de s'appairer avec un autre appareil.

5. **Réinitialiser**
   Si vous décidez de vous débarrasser d'un périphérique IdO, assurez-vous de réinitialiser les paramètres d'usine et de supprimer toutes les données stockées sur l'appareil afin que les futurs propriétaires ne puissent pas y accéder.

Des conseils pour tous les usagers d'Internet

Le Wi-Fi public

Tous types de lieux publics, des transports en commun aux cafés, proposent désormais le Wi-Fi, mais il n'est pas toujours judicieux de se connecter. Les réseaux publics permettent aux cybercriminels d'obtenir facilement vos informations car les mots de passe publics sont accessibles à tous. Restez prudent…

- Désactivez la connexion automatique pour que votre téléphone ne se connecte qu'à des réseaux de confiance.
- N'effectuez JAMAIS de transactions financières sur un réseau Wi-Fi public.
- Utilisez un VPN (réseau privé virtuel) lorsque vous vous connectez à un réseau Wi-Fi public. Il s'agit d'un « tunnel privé » qui crypte toutes vos données transitant sur le réseau. Si vous avez besoin d'un VPN sur votre appareil personnel, effectuez une rapide recherche sur Google pour identifier les fournisseurs recommandés.

Notre conseil

Pour accéder aux réseaux d'Abeille Assurances en toute sécurité, utilisez le VPN d'Abeille Assurances.

Logiciel antivirus et mises à jour d'applications

La mise à jour de votre logiciel antivirus contribue à protéger vos appareils et vos données. Ces logiciels sont conçus pour détecter et supprimer les virus et autres types de logiciels malveillants (ou programmes malveillants). Les produits antivirus modernes se mettent automatiquement à jour pour lutter contre les derniers virus, vous garantissant ainsi une tranquillité d'esprit et une protection optimale.

Pour prévenir toute infection par un virus, ne cliquez pas sur des liens ou n'ouvrez pas de pièces jointes provenant d'une source inconnue ou suspecte, (exemple : dans des e-mails suspects ou des clés USB). Le meilleur conseil que nous pouvons vous donner reste de « réfléchir avant de cliquer ».

Les applications mobiles sont également ciblées par les cybercriminels. Il est donc important de mettre à jour vos applications. Les nouvelles versions sont fournies avec des correctifs intégrés pour assurer la sécurité de votre appareil et de vos données.

Des conseils pour tous les usagers d'Internet

La fraude en ligne

Un e-mail d'hameçonnage est un e-mail utilisé par les cybercriminels pour tenter d'accéder à des informations personnelles telles que les noms d'utilisateur, les mots de passe et même les coordonnées bancaires. Ces e-mails peuvent également contenir des pièces jointes malveillantes ou des liens vers des sites Web pour tenter d'infecter vos appareils. Si une communication similaire est établie par SMS, on parle alors de smishing.

L'hameçonnage ciblé est un message de type similaire, mais cette fois, le criminel utilisera certaines informations personnelles de la victime ciblée pour tenter de gagner sa confiance et de lui faire baisser sa garde.

Les messages d'hameçonnage, de smishing et d'hameçonnage ciblé sont conçus pour ressembler à des messages provenant d'une source fiable, mais certains éléments clés les trahissent souvent.

- Votre banque ne vous demandera jamais votre mot de passe ou d'autres informations personnelles.
- Vérifiez l'adresse e-mail dans le champ « De » de l'e-mail. Attendiez-vous cet e-mail ? A-t-il l'air authentique ou suspect ?
- L'e-mail concerne-t-il une affaire urgente pour vous inciter à agir ? Il s'agit d'un subterfuge délibéré imaginé par les cybercriminels pour installer des logiciels malveillants ou voler des informations.

Cinq conseils : Mots de passe

1. N'utilisez pas le même mot de passe pour différents comptes.
2. Utilisez trois mots au hasard (par exemple, cafétrainpoisson), puis ajoutez des caractères spéciaux et des lettres majuscules (par exemple, caFétrain!poisson5).
3. Évitez d'utiliser des mots de passe qui pourraient être facilement devinés par des personnes qui vous connaissent ou par toute personne pouvant consulter vos comptes sur les réseaux sociaux (par exemple, le nom de votre animal de compagnie ou votre anniversaire).
4. Modifiez régulièrement vos mots de passe, mais ne les « recyclez » pas en changeant simplement un chiffre, par exemple.
5. Différenciez vos mots de passe selon le service utilisé, changez-les régulièrement et choisissez les avec soin. Evitez les dates de naissance par exemple. Ne les enregistrez pas et ne les notez pas. Servez-vous d'outils de génération de mot de passe tels que Keepass, outil certifié par l'ANSSI.

Protégez bien l'accès à votre compte **en utilisant des mots de passe différents et suffisamment robustes**.
Si le service le propose, activez également la double authentification.

Si vous recevez un e-mail, un SMS ou un appel téléphonique suspect sur vos appareils personnels, vous pouvez le signaler à Signal spam ou Stop aux spams vocaux et SMS.

Des conseils pour tous les usagers d'Internet

Attention

Il est important de vérifier si vos informations personnelles ont été compromises par une violation de données. Rendez-vous sur ce site pour savoir si votre adresse mail personnel a été compromise.

Notre conseil

Sauvegardez les données de votre téléphone ! Pensez à sauvegarder vos données et photos sur le cloud et/ou hors ligne en toute sécurité. Cela vous aidera à conserver vos informations en cas de perte, de vol ou de bris de votre appareil.

Cookies : le saviez-vous…?

Tous les sites Web envoient des « cookies » à votre appareil. Cela permet de suivre vos visites et votre activité. Les cookies mémorisent vos informations de connexion et permettent aux vendeurs en ligne de conserver les articles dans votre panier, par exemple.

Cependant, certains virus et programmes malveillants peuvent être déguisés en cookies : il est donc recommandé de les gérer avec précaution. Ouvrez votre navigateur Internet et recherchez le stockage des cookies dans vos paramètres ou fichiers. Chrome, Firefox, Safari et Microsoft Edge intègrent tous des commandes légèrement différentes, il faudra donc chercher comment gérer les cookies sur le navigateur que vous utilisez.

C'est vous qui décidez des informations auxquelles les sites en ligne peuvent accéder. Si vous ne reconnaissez pas un site ou si vous avez changé d'avis, supprimez le cookie.

Attention

Si quelque chose semble trop beau pour être vrai, c'est probablement le cas ! De rapides recherches en ligne peuvent vous éviter toutes sortes d'embarras. Faites vos propres vérifications (et plutôt deux fois qu'une !) avant d'effectuer des achats ou de partager de fausses informations.

Attention : vous avez perdu votre téléphone !

Veillez à utiliser les fonctions de sécurité intégrées aux appareils mobiles tels que les téléphones, les ordinateurs portables et les tablettes. L'identification par empreinte digitale ou un mot de passe à l'écran de verrouillage peut protéger vos données des cybercriminels en cas de perte ou de vol de votre appareil.

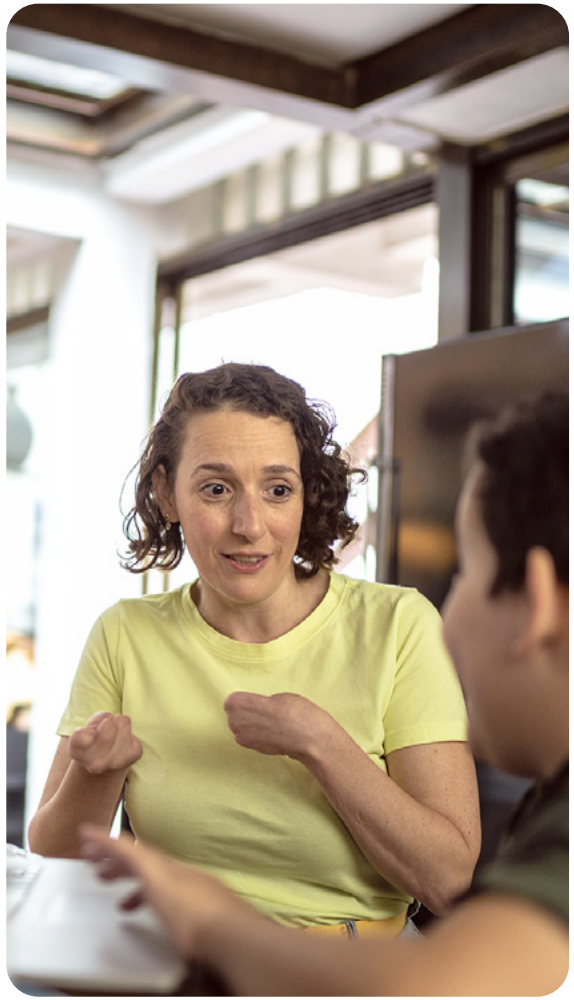
3 Conseils aux parents de jeunes enfants (4 à 7 ans)

Quoi qu'on en pense, Internet a une influence considérable sur nos enfants. En tant que parents ou tuteurs, il est de notre devoir de les aider à faire les bons choix afin qu'ils puissent tirer le meilleur parti de la technologie numérique et de tout ce qu'elle a à offrir. Voici quelques conseils et outils qui vous aideront à donner à votre enfant les moyens d'utiliser Internet en toute sécurité et en toute confiance.

Cinq conseils : Contrôler ce que voient vos enfants

1. Pour cela, le contrôle parental est votre meilleur allié. Visitez le site **e-Enfance**. pour découvrir comment l'utiliser.
2. Assurez-vous que votre enfant n'utilise des appareils numériques que dans les parties communes de votre domicile. La vie en ligne doit être une activité sociale, et non solitaire.
3. Limitez sa durée d'exposition aux écrans et assurez-vous que votre enfant n'utilise pas d'appareil à l'approche de l'heure du coucher.
4. Faites des recherches sur les jeux ou applications que votre enfant utilise. **e-Enfance** contient des informations très utiles sur les jeux les plus populaires.
5. Intéressez-vous à ce que fait votre enfant. Habituez votre enfant à vous raconter ce qu'il fait en ligne.

Conseils aux parents de jeunes enfants (4 à 7 ans)



Parlons-en

Internet représente un nouveau défi pour les parents. Tout cela n'existait tout simplement pas quand nous étions petits. C'est pourquoi, il peut être difficile pour nous de savoir par où commencer lorsqu'il s'agit de guider nos propres enfants. Heureusement, de nombreuses ressources sont disponibles pour nous aider.

Il s'agit d'un excellent moyen d'entamer un dialogue sur ce qu'il faut faire pour explorer Internet en toute sécurité. Il est important que vous parliez régulièrement avec votre enfant pour veiller à ce que ses activités en ligne restent sûres et saines.

Le site e-Enfance propose du contenu pour vous aider, vous et votre enfant. Parler de la sécurité en ligne et savoir réagir s'il voit quelque chose de dérangeant, constitue un très bon point de départ.

Que faire si quelque chose ne va pas

Si votre enfant vous dit que quelque chose l'a mis mal à l'aise et que vous n'êtes pas sûr de savoir quoi faire, vous pouvez appeler les conseillers de Net Ecoute au **0 800 200 000** (numéro gratuit, anonyme, confidentiel, ouvert du lundi au vendredi de 9h à 19h) ou sur le site internet www.netecoute.fr.

Attention

Votre enfant possède-t-il des appareils ou jouets connectés qui fonctionnent en écoutant les commandes vocales de l'enfant ? N'oubliez pas que ces appareils pourraient enregistrer des conversations personnelles entre vous et votre enfant, soyez prudent. Lisez le manuel pour savoir comment consulter et supprimer les fichiers audio enregistrés et désactivez le microphone pour qu'aucun enregistrement audio ne soit effectué.

4 Conseils aux parents d'enfants plus âgés (8-10 ans)

À mesure que nos enfants avancent en âge et gagnent en indépendance, nous devons être sûrs qu'ils sont capables de prendre les bonnes décisions pour rester en sécurité en ligne, tout comme dans le monde réel. Il est important de continuer à discuter avec votre enfant et de vous assurer que vous savez ce qu'il fait en ligne.

Cinq conseils : Contrôler ce que voient vos enfants

1. Le contrôle parental n'empêche pas votre enfant de voir tout ce que vous aimeriez éviter qu'il voie, en particulier lorsqu'il se familiarise avec le Web. Mais il vaut toujours la peine d'être utilisé. Visitez le site **e-Enfance** pour découvrir comment le contrôle parental fonctionne sur différentes plates-formes de jeu, sites Web et applications TV à la demande.

2. Redoublez d'attention lorsqu'il s'agit de relier des plates-formes de jeu ou des applications à votre carte bancaire. Les frais liés aux achats dans les applications et aux renouvellements d'abonnements (souvent après un essai gratuit) peuvent réellement s'accumuler sans que vous ou votre enfant ne le réalisiez.

3. Limitez sa durée d'exposition aux écrans et assurez-vous que votre enfant n'utilise pas d'appareil à l'approche de l'heure du coucher. Cela risquerait de perturber ses habitudes de sommeil.

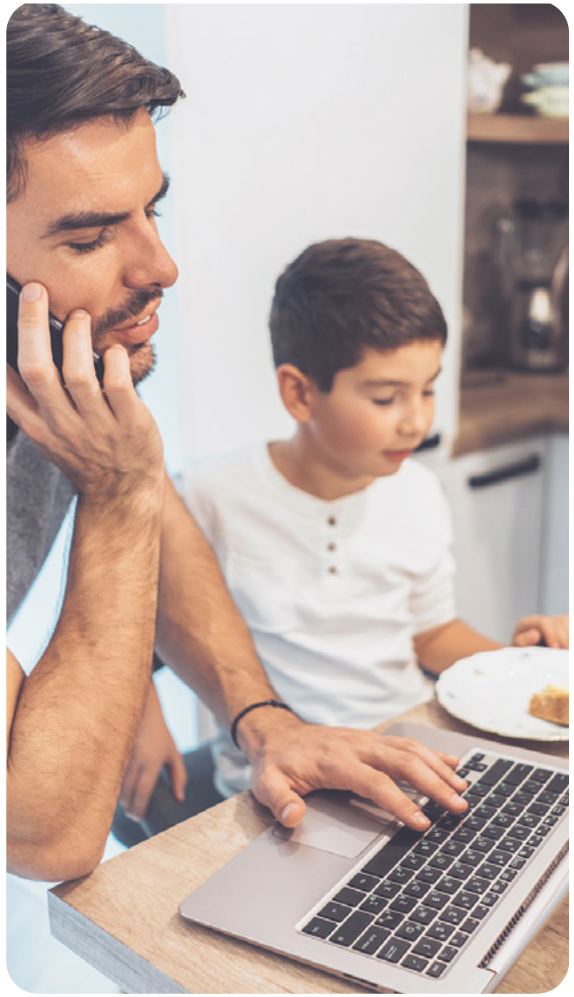
4. Faites des recherches sur les jeux ou applications que votre enfant utilise. contient **e-Enfance** informations très utiles sur les jeux les plus populaires.

5. Intéressez-vous à ce que votre enfant fait en ligne. Discutez régulièrement de ce qu'il fait sur différents appareils et de ce qu'il regarde.

Attention

La mise en place de limites concernant l'usage des appareils électroniques pour votre enfant ne fonctionnera que si vous montrez vous-même l'exemple ! Si vous attendez que votre enfant passe moins de temps sur ses appareils, mieux vaut éviter de rester toute la journée sur votre téléphone ou d'utiliser votre tablette à table.

Conseils aux parents d'enfants plus âgés (8-10 ans)



Devenir indépendant en ligne

À mesure que votre enfant devient plus indépendant, vous allez l'encourager à gérer son propre temps en trouvant un équilibre entre son travail scolaire, ses activités sociales et ses passe-temps. Comprendre que les appareils numériques ne représentent qu'une infime partie de sa vie est un élément majeur dans ce processus. Pour cette raison, certaines familles ont établi une sorte de contrat régissant les droits et responsabilités numériques de leurs enfants. Il peut couvrir :

- la quantité de temps qu'ils ont le droit de passer devant les écrans chaque jour ;
- des directives claires sur les applications et les jeux appropriés ;
- un accord prévoyant de montrer ce qu'il fait en ligne à un adulte de confiance ;
- le fait de convenir d'une heure d'extinction des appareils le soir ;
- le fait d'indiquer le forum et les applications de messagerie qu'ils utilisent.

Si vous pensez que ce type d'accord pourrait fonctionner dans votre famille, il est important d'inclure votre enfant dans sa définition. Vous trouverez quelques conseils très utiles pour vous aider sur le site Web **Internetsanscrainte**.

Savoir prendre les bonnes décisions est une compétence essentielle pour devenir un citoyen numérique responsable.

Parlez à votre enfant, demandez-lui ce qu'il pense des différents sites et s'ils sont adaptés ou non à différents âges. Prenez le temps de bien expliquer les risques encourus sur les réseaux sociaux et leur apprendre ce qu'ils peuvent faire et ne pas faire sur ces réseaux comme de divulguer trop d'informations à caractère personnel sur Internet.

Signaler les contenus choquants

Il est important que vous et votre enfant sachiez tous les deux comment signaler et bloquer des contenus sur tous les sites, jeux et applications qu'il utilise. Vous pouvez signalez du contenu sur **Internet-signalement.gouv.fr** . Assurez-vous que votre enfant sait que vous l'aiderez à signaler tout contenu perturbant qu'il pourrait voir.

Vous devez également apprendre à votre enfant que le harcèlement et le cyber harcèlement sont inacceptables.
Le site **e-Enfance** a de très bons conseils pour les parents et les enfants sur la façon de gérer ce problème.

5 Conseils aux 11-13 ans

À mesure que les enfants grandissent, ils deviennent plus susceptibles de naviguer en toute indépendance. Ainsi, plutôt que de se contenter de conseiller les parents, cette section est conçue pour être lue par les enfants et les adolescents afin qu'ils apprennent eux-mêmes comment rester en sécurité en ligne.

Maintenant que tu es au collège, tu vas sans doute passer une bonne partie de ta vie en ligne.

Tu utiliseras le Web pour effectuer des recherches et réviser, et tu seras peut- être également très actif sur les réseaux sociaux et les sites de jeux. Comme dans la vie réelle, il est important de savoir te protéger en ligne et de traiter les autres avec respect.

Cinq conseils : Rester prudent et intelligent en ligne

1. Utilise tes paramètres de confidentialité pour garder le contrôle. Désactive les fonctions de localisation sur les applications de réseaux sociaux mais n'oublie pas de les garder activées sur toutes les applications que tes parents utilisent pour ta sécurité.

2. Réfléchis bien avant de partager quoi que ce soit, en ligne ou en envoyant des messages. Une fois que tu auras appuyé sur « Envoyer », tu n'auras plus aucune prise sur les images ou les mots partagés, et tu ne peux pas contrôler la façon dont les autres personnes les utiliseront.

3. Veille sur tes amis. S'ils sont dans une mauvaise passe ou semblent avoir des problèmes en ligne, parles-en à une personne de confiance ou lis des conseils utiles sur ce que tu peux faire pour les aider, comme les informations disponibles sur le site **e-Enfance**.

4. Sur Internet, les gens ne sont pas toujours ceux qu'ils prétendent être. Fais très attention quand tu envoies des messages à quelqu'un que tu ne connais pas ou à des personnes qui prétendent connaître tes amis. Ne partage jamais d'informations personnelles ou de photos avec des personnes que tu ne connais pas ou que tu as uniquement rencontrées sur un forum.

5. Si quelque chose que tu as vu en ligne ou ce que quelqu'un t'a dit sur un forum, dans un jeu, sur un site Web ou sur une application te met mal à l'aise, il faut que tu parles à un adulte de confiance. Si tu as du mal à parler à quelqu'un que tu connais, appelle Net Ecoute au **0 800 200 000.**

Conseils aux 11-13 ans

Les écrans, une question de temps

Internet, c'est génial pour toutes sortes de choses, du travail scolaire aux discussions entre amis, mais n'oublie pas de faire régulièrement des pauses. Si tu trouves que tu passes beaucoup de temps en ligne (ton téléphone peut probablement te dire exactement combien de temps tu passes sur les sites et applications), et si tu y penses même quand tu n'es pas en ligne, il est probablement temps d'agir. Il y a des tas de choses à faire dans le monde réel, alors n'oublie pas de t'aérer un peu !

Attention

Fais attention aux achats que tu peux faire dans les applications ou dans les jeux. Il est très facile d'accumuler une dette réelle en achetant des produits en ligne. Demande conseil à un adulte pour éviter de te retrouver dans le piège des dépenses en ligne.

6 Conseils aux adolescents et aux jeunes adultes

Tout le monde sait que les adolescents peuvent défendre leur indépendance avec acharnement. Ainsi, si vous êtes un adolescent ou un jeune adulte qui navigue sur le Web, cette section est conçue pour vous aider à rester en sécurité en ligne et vous avertir des dangers potentiels.

Être indépendant signifie que vous allez prendre toutes sortes de décisions seul, y compris celles qui concernent votre identité en ligne. Il est très important de rester prudent en ligne et de ne pas sous-estimer les connexions que vous établissez. Vous devez également vous rappeler que tout ce que vous mettez en ligne y restera quasiment pour l'éternité. C'est ce que l'on appelle votre empreinte numérique, et si vous ne vous en souciez pas, vous courez le risque de voir une image peu reluisante, une opinion mal formulée ou une plaisanterie déplacée se retourner contre vous.

Attention

Des études montrent que passer beaucoup de temps à regarder les profils d'autres personnes sur les réseaux sociaux peut te laisser penser que ta vie est moins intéressante ou moins drôle, ou que tu es toi-même moins beau, intelligent ou drôle que les autres, mais cette comparaison n'a pas lieu d'être. C'est une version exagérée et modifiée de la vie réelle. Les photos et les publications sélectionnées avec soin par les autres ne sont pas représentatives.

Conseils aux adolescents et jeunes adultes

Cinq conseils : En ligne, montrez votre meilleur profil

1. Internet est éternel, alors pensez à quelqu'un que vous aimez et que vous respectez : que penserait-il ou elle du message ou de la photo que vous êtes sur le point de publier ?
2. De nombreuses amitiés et relations se vivent en partie dans des discussions en ligne. Restez respectueux et, si quelqu'un vous contrarie, assurez-vous de savoir comment le bloquer ou le signaler. Consultez internet pour vous aider à gérer cela. Et si vous craignez que l'un de vos amis ait rencontré quelqu'un d'étrange en ligne, n'hésitez jamais à agir. **e-Enfance** être d'une grande aide.
3. N'oubliez pas que les gens ne sont pas forcément ceux qu'ils prétendent être. Ne partagez pas d'images avec des personnes que vous ne connaissez pas et soyez également très prudent lorsque vous en partagez avec vos amis. Une fois que vous avez envoyé une image, elle n'est plus sous votre contrôle.
4. Les autres personnes aussi ont des sentiments. Même si vous le dites juste pour rire, un commentaire irréfléchi peut blesser quelqu'un. Réfléchissez bien à la façon dont vous traitez les autres en ligne et restez respectueux. Vous ne pouvez pas savoir ce qu'ils traversent dans la vie réelle. Pensez également à votre propre comportement. Si vous exagérez des problèmes émotionnels pour recevoir de la compassion, vous empêchez quelqu'un qui a de véritables problèmes d'obtenir toute l'aide dont il a besoin. C'est ce que l'on appelle le « sadfishing » (pêche à la tristesse) et c'est un véritable problème sur les réseaux sociaux.
5. Ne laissez pas vos appareils vous empêcher de faire d'autres choses ! Des études montrent que la lumière émise par les téléphones et les tablettes peut sérieusement perturber nos habitudes de sommeil, et nous savons tous que les sites de réseaux sociaux sont conçus pour devenir addictifs. Définir des limites de temps et utiliser des applications de productivité peut vous aider à rester concentré sur les autres aspects de votre vie.

Attention

Il est important de savoir que la pornographie exagère beaucoup la réalité. Elle peut avoir pour but de choquer, de divertir et de faire de l'argent. Elle ne représente pas forcément la réalité ou des relations consenties.

7 Rendre internet plus inclusif

Le monde numérique a beaucoup à offrir à tous, et il aide de nombreuses personnes vulnérables de notre société à se sentir connectées et indépendantes. Il peut nous aider à nous sentir moins isolés en nous connectant à nos amis et à notre famille via les réseaux sociaux et les appels vocaux et vidéo en ligne. Il offre également des opportunités exceptionnelles en termes de passe-temps et d'apprentissage : apprendre une nouvelle langue, prendre des cours en ligne sur divers sujets ou faire des recherches généalogiques. Les possibilités sont infinies.

Pour toutes sortes de raisons différentes, nous pouvons tous parfois nous sentir vulnérables. Nous pouvons tous rencontrer des problèmes de santé physique ou mentale, ou encore des difficultés d'apprentissage ou d'expression. Si vous pensez que vous n'êtes pas aussi sûr de vous que vous aimeriez l'être dans le monde numérique, de nombreuses aides sont à votre disposition.

Cinq conseils : apprendre à explorer Internet

1. Si vous connaissez une personne âgée qui souhaite en savoir plus mais qui ne sait pas par où commencer, pourquoi ne pas regarder sur internet si un organisme propose une formation en informatique dans sa région ? Elle recevra des conseils pratiques qui lui permettront de se connecter en toute sécurité.

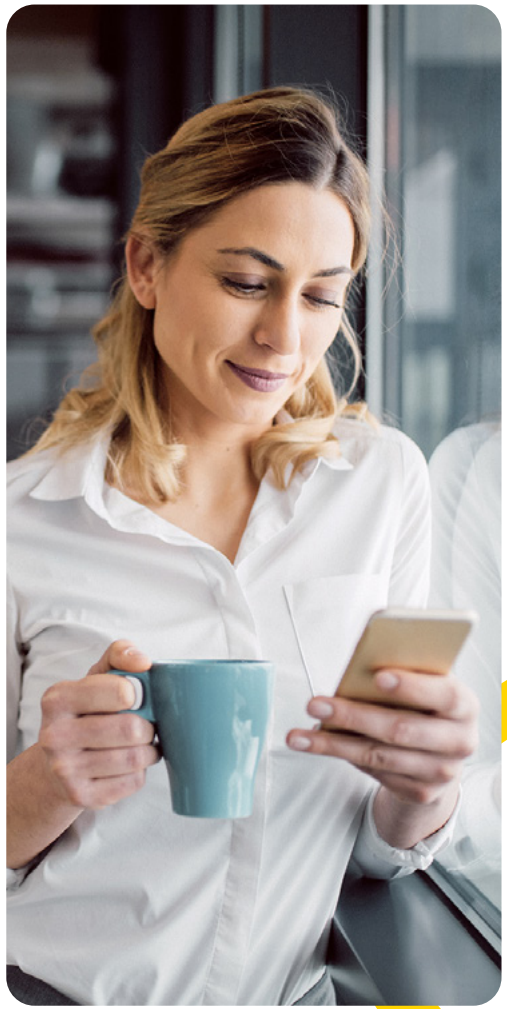
2. Pour certains, les termes du monde numérique peuvent ressembler à du chinois. Si le mot « navigateur » vous déboussole ou que le terme « spam » vous donne du vague à l'âme, jetez un coup d'œil à cet **excellent glossaire** pour vous aider à les comprendre.

3. Tout comme dans la vie réelle, vous devez utiliser votre instinct pour savoir si quelqu'un ou quelque chose est authentique ou non. Derrière un écran, il est très facile de prétendre être ce que l'on n'est pas, alors faites vos recherches et ne confiez jamais vos informations personnelles à quiconque, sauf si vous êtes absolument certain que votre interlocuteur est fiable.

4. **Infos Arnaques** donne quelques conseils utiles pour reconnaître les escroqueries en ligne.

5. Si quelque chose que vous avez vu en ligne vous inquiète ou si vous pensez avoir été victime d'une escroquerie, vous devez le signaler. Rassemblez toutes les informations nécessaires (site Web ou adresse e-mail, date, noms, etc.) et rendez vous sur le site Web **internet-signalement.**

Rendre internet plus inclusif



Gérer les situations difficiles

Malheureusement, outre toutes les expériences positives qu'il offre, Internet est utilisé à des fins malveillantes par certaines personnes. L'abus et le harcèlement ne doivent pas être tolérés en ligne, pas plus que dans la vie réelle. Nous avons tous le droit de vivre une expérience numérique sans intimidation ni peur. Si vous pensez que vous ou l'un de vos proches êtes visé d'une manière ou d'une autre, vous ne devez pas vous laisser faire.

Attention !

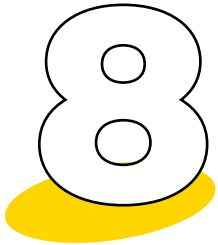
Si vous vous sentez mal à l'aise ou menacé sur un site Web, un jeu ou une application, voici ce qu'il faut faire :

- désactivez la discussion avec le harceleur ou bloquez-le (sur les réseaux sociaux et les jeux) ;
- enregistrez les preuves ;
- signalez-le aux responsables du site ou aux modérateurs ;
- si vous pensez que votre intégrité physique est menacée, contactez la police.

Harcèlement en ligne : le saviez-vous…?

Le harcèlement sur les réseaux sociaux ou d'autres sites Web est également connu sous le nom de « cyber harcèlement ». Si vous êtes victime de ce genre d'abus, vous ne devez pas vous laisser faire.

Visitez **e-Enfance** pour obtenir des conseils utiles sur la marche à suivre, quel que soit votre âge.



En savoir plus

Il est important de se rappeler que les risques en ligne évoluent et se développent aussi rapidement que les nouvelles opportunités qu'offre le monde numérique. C'est pourquoi nous ne pouvons pas nous reposer sur nos lauriers. Nous devons prendre l'habitude de tester régulièrement la sécurité que nous avons mise en place et de rester au courant des nouvelles menaces et alertes. Il est recommandé de consulter régulièrement les actualités d'une source fiable pour obtenir les conseils les plus récents.

Sites Web utiles

Pour tous les citoyens numériques

L'ANNSI (agence nationale de la sécurité des systèmes d'informations) prodigue les conseils les plus récents pour les particuliers, les entreprises et les organismes du secteur public.

Pour les victimes de criminalité en ligne

Internet signalement pour signaler des faits de cybercriminalité.

Si vous vous retrouvez face à une situation de « Revenge Porn », contacter directement sur **NET ECOUTE** **0800 200 000 NET ECOUTE** ou pour toute personne dont des images intimes ont été partagées en ligne sans son consentement.

Cette plateforme téléphonique s'adresse à toutes les victimes d'infractions, quelle que soit la forme de l'agression ou le préjudice subi. Le 116 VICTIMES (soit le 116006) est un numéro non surtaxé, disponible 7 jours sur 7. Deux autres numéros sont à votre disposition : **SOS Enfants disparus : 116 000 - Enfance en danger : 119**

Pour les enfants, les jeunes et leurs parents/tuteurs

e-Enfance : informations et ressources pour assurer la sécurité des enfants en ligne.

Document non contractuel d'information générale à jour le 01/06/2022.
Crédit photo : Getty Images

Abeille Assurances Holding
Société anonyme au capital de 1 678 702 329 €
Siège social : 80 avenue de l'Europe - 92270 Bois-Colombes
331 309 120 RCS Nanterre