



Digital Security
Progress. Protected.

safer**kid**sonline

Comment protéger et
accompagner nos enfants sur
Internet ?

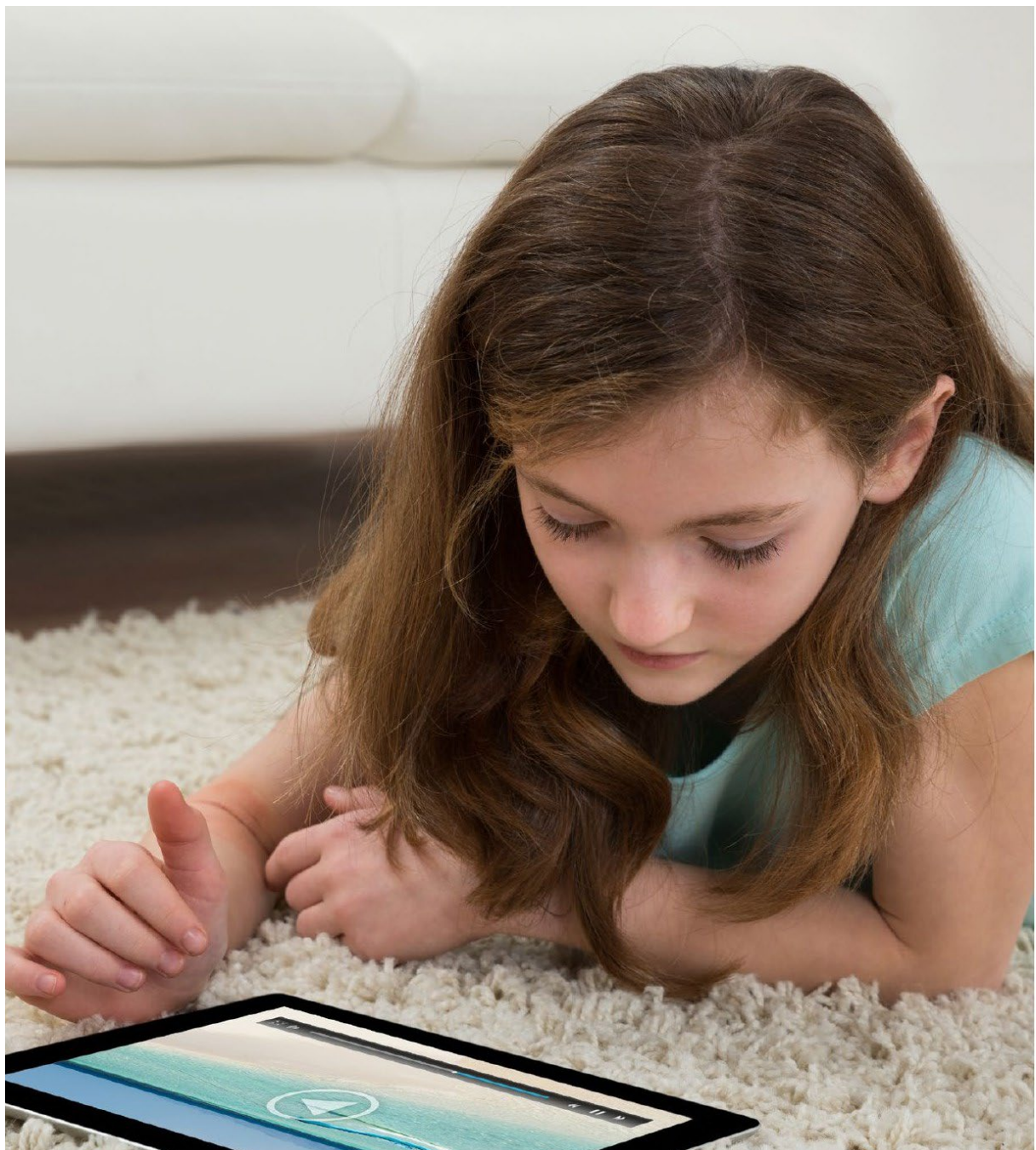
Guide pour les parents

Monde digital

Nous sommes nombreux chez ESET à être des parents, exactement comme vous. Nous ressentons le besoin de guider nos enfants tout au long de leur vie et de les protéger des dangers, mais aujourd'hui, cette responsabilité est un véritable défi.

Avec des appareils mobiles de plus en plus complexes, de nouvelles plateformes de communication et un langage en ligne qui évolue rapidement, les parents ont beaucoup à apprendre pour aider leurs enfants.

Ce guide offre des conseils pour expliquer ce qu'il faut faire pour que vos enfants puissent utiliser Internet en toute sécurité.



Qui devrait leur parler ?

Peu importe si cela vous met mal à l'aise, vous devez le faire.

Vos enfants vont rencontrer de nombreuses personnes qui joueront un rôle très important dans leur vie : leur famille, des amis et des enseignants. Aucune d'entre elles ne peut cependant remplacer votre rôle de parent. Aux yeux d'un enfant, c'est vous qui détenez toutes les réponses et qui êtes en mesure de l'aider lorsqu'il n'est pas sûr de ce qu'il doit faire.

Quand devriez-vous leur parler ?

Maintenant !

Dès qu'un enfant montre un intérêt pour votre tablette, votre smartphone ou votre ordinateur, vous devez commencer à lui expliquer certaines choses. Nous enseignons de nombreuses règles aux enfants pour leur sécurité dans le monde physique. Il en existe tout autant pour le monde en ligne. Si les menaces immédiates pour la sécurité peuvent prendre une forme différente, le danger potentiel est tout aussi réel.

Au fur et à mesure que votre enfant grandira, de nouveaux problèmes apparaîtront et les conseils appropriés changeront. Un accompagnement bienveillant dans ces situations nouvelles sera l'étape décisive qui poussera votre enfant dans la bonne direction.

L'éducation – Une voie à double sens

Avez-vous l'impression que vos enfants en savent plus que vous sur l'informatique ? Vous n'êtes pas seul(e).

Les enfants d'aujourd'hui sont nés avec les nouvelles technologies et sont capables de les utiliser pleinement. Pour de nombreux adultes, ces compétences doivent être acquises. Cependant, savoir comment accéder à Internet ne signifie pas nécessairement savoir l'utiliser en toute sécurité.

En tant que parent, vous n'avez pas besoin d'en savoir plus que vos enfants sur ce qui se passe dans le monde virtuel. Mais vous devriez être en mesure de réagir au cas où vos enfants rencontreraient quelque chose d'inhabituel et auraient besoin d'en discuter avec quelqu'un de plus expérimenté.

L'important est d'intégrer l'enfant : créez un environnement où il peut poser librement des questions et avoir le temps d'absorber de nouvelles informations.

Nos conseils selon l'âge de vos enfants

Utilisez des outils de contrôle parental

Quel que soit l'âge de vos enfants, il existe des technologies que vous pouvez utiliser. Les outils de contrôle parental d'ESET permettent de bloquer des sites ou même des catégories de pages au contenu potentiellement choquant. Vous pouvez limiter le temps passé à surfer sur Internet ou à jouer. Ces technologies permettent également à votre enfant de vous demander la permission de consulter certaines pages ou d'avoir plus de temps pour jouer, par exemple lorsque leurs devoirs sont terminés.

En plus des outils de contrôle, nous proposons quelques conseils pour différentes tranches d'âge qui rendront les activités en ligne des enfants plus sécurisées.

JUSQU'À 10 ANS

1. Accompagnez-les pour leurs premiers pas sur le web

Veillez à être présent lorsque vos enfants font leurs premiers pas dans le monde digital. Le premier contact d'un enfant avec Internet est une bonne occasion de prendre le temps de le guider dans sa nouvelle aventure.

2. Fixez les conditions d'utilisation d'Internet

Délimitez des règles de base pour l'utilisation d'internet. Une bonne pratique consiste à superviser le nombre d'heures passées en ligne et à définir les horaires pendant lesquels l'accès au web est autorisé.

3. Soyez un bon exemple

Les enfants prennent généralement pour exemple le comportement de leurs parents, que ce soit dans la vie réelle ou en ligne. Si les membres de la famille ont un comportement positif, l'enfant est susceptible de faire de même.



DE 11 À 14 ANS

1. Apprenez-leur à ne pas communiquer d'information qui pourraient les identifier

Il est important de faire comprendre aux enfants que dans le monde virtuel, tout le monde n'est pas un ami, et que certaines personnes peuvent même leur vouloir du mal. Expliquez pourquoi il ne faut pas communiquer d'informations telles que l'adresse ou le numéro de téléphone du domicile, le nom de l'école ou les activités extrascolaires auxquelles ils participent. L'enfant doit également vous demander l'autorisation avant de communiquer des photos potentiellement sensibles sur Internet.

2. Gardez un dialogue ouvert

Encouragez vos enfants à être ouverts avec vous et à vous poser librement des questions sur ce qu'ils voient sur Internet. Si vous utilisez un ordinateur de bureau, essayez de l'installer dans une pièce où toute la famille passe du temps et où vous pouvez le surveiller, et non dans leur chambre.



DE 15 À 18 ANS

1. Personne d'autre ne doit connaître leurs mots de passe

Nous savons que les adolescents peuvent être difficiles, mais veillez à ce qu'ils comprennent les bonnes pratiques en matière de mots de passe et les appliquent. Respectez la vie privée de vos adolescents, mais veillez également à ce qu'ils ne communiquent jamais leurs mots de passe à quiconque directement ou sur Internet.

2. Signalez immédiatement les cas de cyberharcèlement

Vous souvenez-vous du petit « dur » de votre école, celui qui harcelait les autres enfants ? De nos jours, de nombreux harceleurs sont passés à la technologie et se cachent derrière leur clavier. Ce qui n'a pas changé, c'est qu'ils essaient toujours de nuire psychologiquement aux autres. Vous devez donc dire à vos enfants de vous informer immédiatement s'ils sont victimes de harcèlement.

3. Les transactions financières en ligne sont réservées aux adultes

Acheter quelque chose sur Internet ne devrait pas poser de problème, tant que cela est fait avec précaution. Néanmoins, tant que vos enfants ne sont pas familiers des bonnes pratiques d'achat en ligne notamment sur le partage d'informations financières personnelles, nous vous conseillons d'encadrer et de superviser leurs emplettes sur le web.



Quelles sont les principales menaces en ligne ?

Malwares

Les malwares désignent des logiciels malveillants. Ce type de programme tente d'endommager un appareil de différentes manières. Certains d'entre eux chiffrent les fichiers de votre ordinateur, tandis que d'autres essaient de vous espionner ou de télécharger d'autres applications dangereuses sur votre ordinateur.

Dans la plupart des cas, l'infection se produit à cause des « erreurs » commises par les utilisateurs après avoir été trompés par un malfaiteur. L'utilisation de solutions de sécurité réputées et de bonnes pratiques réduit le risque d'être infecté par des malwares.

Spam

Vous avez certainement déjà rencontré du spam. Il s'agit de tous ces emails non sollicités qui apparaissent dans votre boîte de messagerie. Ils comprennent généralement des publicités qui vous invitent à consulter certaines pages proposant des offres incroyables, mais qui abritent le plus souvent des contenus potentiellement dangereux.

Escroqueries

Ce sont des actes frauduleux commis sur Internet. Elles peuvent prendre différentes formes, notamment le spam et les techniques d'ingénierie sociale. Dans ce cas précis, les cyberattaquants proposent de vendre quelque chose, se font passer pour vos collègues ou même votre banque, afin d'obtenir des informations confidentielles. Les faux messages demandant des noms d'utilisateur et des mots de passe d'accès à des comptes sur des réseaux sociaux sont un exemple fréquent d'escroquerie.

Cyberharcèlement

Ce comportement hostile est généralement dirigé contre les enfants. La victime peut être menacée et humiliée par d'autres enfants en ligne, une pratique fréquente chez les adolescents. Cela peut potentiellement nuire à l'enfant en lui causant un traumatisme émotionnel. Le cyberharcèlement emprunte différentes voies, utilisant même les fonctions de chat des jeux sur console.

Manipulation en vue d'abus sexuels

Cela se produit lorsqu'un adulte tente de persuader un enfant de se livrer à des activités sexuelles, en créant un environnement de confiance et en établissant un lien émotionnel avec l'enfant. Les adultes se font souvent passer pour des enfants afin d'établir une relation étroite, puis tentent d'organiser une rencontre en "vrai". Pour un parent, il est important d'avoir une bonne visibilité sur les personnes avec lesquelles votre enfant interagit en ligne.

Sexting

Le « sexting », dérivé de « sexe » et de « texting », existe depuis un certain temps. Si la fonction SMS était initialement utilisée sur les téléphones mobiles pour échanger des messages ou "textos", différents services de messagerie permettent désormais d'envoyer couramment des photos et des vidéos, car la plupart des adolescents et des enfants ont leurs appareils mobiles sur eux à tout moment.

Vol d'informations

Les informations envoyées sur le web, sans les précautions nécessaires, peuvent être interceptées par des tiers et utilisées à des fins d'usurpation d'identité ou de chantage.



Dernières suggestions

Utilisez des outils de contrôle parental

Le contrôle parental peut être utilisé dans les navigateurs web et les logiciels antivirus. Il est intégré à la dernière version d'[ESET Internet Security](#) et est disponible sous forme d'application distincte [ESET Parental Control pour Android](#). Ce type d'outils est également disponible pour les consoles de jeux.

Ne laissez pas votre enfant envoyer des informations confidentielles sur Internet

Des informations sensibles ne devraient jamais être demandées par email ou par chat. Les banques ne demandent pas les données de votre compte ni votre code PIN de cette manière. Il est également important de ne pas fournir ces informations précieuses à vos enfants.

Ne répondez pas aux messages de harcèlement et ne les supprimez pas

Si votre enfant est victime de cyberharcèlement, il ne doit pas répliquer. Expliquez que l'harceleur veut provoquer une réaction car cela nourrit son désir de nuire aux autres. Si ce genre de situation se reproduit, prévenez les autorités compétentes. N'effacez pas les messages reçus car ils pourraient être utilisés comme preuves.



Restez à jour

Aujourd'hui, refuser à votre enfant l'accès aux technologies n'est pas une solution. Les appareils digitaux font partie de leur vie quotidienne et sont de plus en plus importants pour leur développement. Au lieu de mettre en place des restrictions, aidez vos enfants à les utiliser en toute sécurité et participez à l'interaction entre l'enfant et l'appareil. Il convient également de souligner que nombre de ces risques peuvent également toucher les adultes, et que beaucoup des précautions décrites ici devraient être prises à tout âge.

La sécurité des enfants est la responsabilité de tous, et les conseils fournis dans ce guide ne sont que des bases. Pour plus d'informations, consultez nos sites web et nos pages sur les réseaux sociaux

www.eset.com/fr

<http://www.welivesecurity.com/fr>

Suivez-nous sur www.facebook.com/ESETFrance

et sur https://twitter.com/ezet_france