Cartable numérique : guide à l'intention des parents pour l'année scolaire

kaspersky

Pourquoi la cybersécurité est-elle importante en cette année scolaire ?

Alors que les enfants se préparent à la nouvelle année scolaire avec des crayons bien taillés et des cahiers neufs, il existe un outil essentiel trop souvent négligé, à savoir la cybersécurité. À une époque où le numérique occupe une place de plus en plus importante dans l'éducation, les élèves dépendent plus que jamais des ordinateurs portables, des tablettes, des applications de messagerie et des plateformes d'apprentissage en ligne. Cependant, le confort de l'apprentissage connecté s'accompagne d'un nombre croissant de menaces en ligne, allant du phishing, des escroqueries et des violations de données au cyberharcèlement et à l'usurpation d'identité.

Pour les parents, cela signifie que la cybersécurité n'est plus une option, mais un élément essentiel de la préparation à la rentrée scolaire. De la même manière que vous apprenez à votre enfant à traverser la rue en toute sécurité ou à préparer un déjeuner équilibré, vous devez lui fournir les outils et les connaissances nécessaires pour naviguer dans le monde en ligne avec confiance et prudence.

Dans ce guide, nous vous présenterons les principaux risques en matière de cybersécurité auxquels votre enfant pourrait être confronté au cours de cette année scolaire, ainsi que les mesures que vous pouvez prendre pour les prévenir. Depuis la configuration de mots de passe forts et de contrôles parentaux jusqu'à l'identification des escroqueries et aux discussions sur les comportements en ligne, le cartable numérique est là pour vous aider à garder une longueur d'avance et à assurer la sécurité numérique de votre enfant.

Monde en ligne

Les élèves d'aujourd'hui sont plus connectés que jamais : ils discutent avec leurs amis par le biais d'applications de messagerie, rejoignent des groupes de discussion entre élèves, utilisent des outils d'IA pour faire leurs devoirs et explorent le vaste monde d'Internet pour leurs études et pour le plaisir. Cependant, les opportunités d'apprentissage s'accompagnent de risques réels. Le monde en ligne, bien que fascinant et riche en possibilités, peut également constituer un lieu où les enfants sont exposés à des contenus dangereux, se retrouvent victimes d'escroqueries, ou deviennent la cible de cyberharcèlement.

Il ne s'agit plus seulement de contrôler le temps d'utilisation des écrans, mais également de savoir ce qui se passe pendant ce temps. Sans le savoir, les enfants peuvent télécharger des programmes malveillants déguisés en outils éducatifs, entrer en contact avec des inconnus se faisant passer pour des camarades de classe, ou partager trop d'informations personnelles susceptibles d'être exploitées. Même les plateformes conçues à des fins pédagogiques et coopératives ne sont pas à l'abri des menaces.

Comprendre ces dangers constitue la première étape pour pouvoir protéger votre enfant. Dans cette section, nous allons aborder les menaces en ligne les plus courantes auxquelles sont aujourd'hui confrontés les enfants en âge d'aller à l'école, du phishing aux fausses applications en passant par l'ingénierie sociale et les contenus inappropriés. Nous allons voir comment ces menaces fonctionnent, pourquoi les enfants sont vulnérables, et ce que vous pouvez faire pour les aider à rester en sécurité.

Recherche sécurisée

Les moteurs de recherche ne font pas toujours la différence entre les contenus adaptés à une certaine tranche d'âge et les contenus réservés aux adultes. C'est pourquoi les enfants ont besoin à la fois de mesures de protection techniques et d'un esprit critique pour naviguer en toute confiance dans le monde numérique. Lorsque les enfants acquièrent dès le plus jeune âge des habitudes de recherche sûres, ils évitent non seulement les risques liés à Internet, mais ils deviennent également des apprenants plus réfléchis, plus curieux et plus indépendants.

1. Utiliser des filtres de contenu et des outils de contrôle parental

Commencez par activer le contrôle parental sur tous les appareils utilisés par votre enfant : smartphones, tablettes, ordinateurs et téléviseurs intelligents. La plupart des systèmes d'exploitation (comme iOS, Android, Windows et macOS) proposent des fonctionnalités intégrées qui vous permettent de bloquer les sites Internet explicites, de restreindre certains types d'applications et de filtrer les résultats de recherche. Par ailleurs, des plateformes comme YouTube, Netflix et TikTok vous permettent d'activer des modes « restreint » ou « enfants », qui limitent l'accès aux contenus réservés aux adultes. Pour encore plus de contrôle, envisagez d'utiliser des outils comme Kaspersky Safe Kids, qui offre un filtrage du contenu en temps réel, une gestion du temps d'utilisation des écrans et une surveillance des applications. Cet outil permet de détecter les contenus inappropriés qui pourraient échapper aux filtres standard, en particulier dans les navigateurs.

2. Désactiver les fonctionnalités de lecture automatique

La lecture automatique est l'un des principaux moyens par lesquels les enfants sont involontairement exposés à des contenus inappropriés. Sur des plateformes comme YouTube ou Netflix, une vidéo peut en entraîner une autre, et avant même que vous ne vous en rendiez compte, votre enfant regarde un contenu qui n'est pas du tout adapté à son âge. Désactivez la lecture automatique dans la mesure du possible, à la fois dans les paramètres et dans les extensions de navigateur si nécessaire. Lorsque la lecture automatique est désactivée, votre enfant doit choisir consciemment de cliquer sur la vidéo suivante. Cela ralentit sa consommation de contenu, vous donne plus de chances de pouvoir intervenir, et encourage globalement des habitudes de visionnage plus réfléchies.

3. Apprendre à votre enfant ce qu'il doit faire lorsqu'il voit quelque chose qu'il ne devrait pas voir

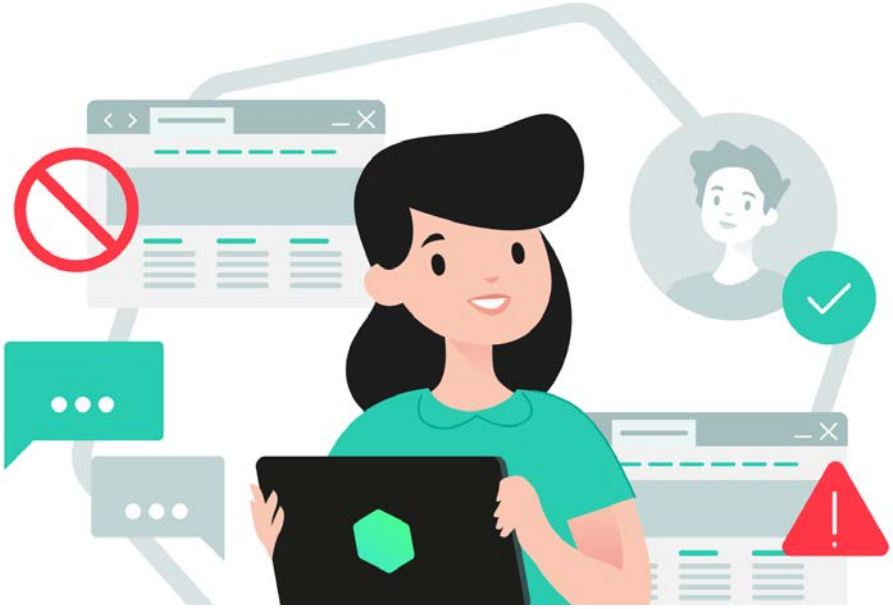
Aucun filtre n'est infaillible. C'est pourquoi il est essentiel de donner à votre enfant les moyens de réagir lorsque quelque chose ne lui semble pas approprié. Enseignez-lui la réponse en trois étapes : **s'arrêter, fermer le contenu, prévenir un adulte.** Expliquez-lui qu'il ne sera pas puni s'il vous en parle, même s'il a cliqué sur quelque chose par erreur ou par curiosité. Encouragez l'honnêteté et la franchise. Vous pouvez même convenir d'un « mot de sécurité numérique » que votre enfant peut prononcer lorsqu'il a vu quelque chose dont il a du mal à parler immédiatement.

4. Regarder et discuter ensemble

Le filtre le plus efficace n'est pas un logiciel, mais **vous**. Prenez le temps de regarder des émissions, de jouer à des jeux vidéo ou de parcourir du contenu ensemble de temps en temps. Cela vous permet non seulement de contrôler ce que votre enfant voit, mais également de discuter de valeurs, de sentiments et de situations de la vie réelle. Pour en découvrir plus à propos des recherches des enfants en ligne, consultez notre dernier rapport sur les centres d'intérêt des enfants.

5. Vérifier les historiques des appareils, et rester à l'écoute

Gardez l'historique du navigateur, l'historique de visionnage sur YouTube et les journaux d'utilisation des applications activés. Ne considérez pas cela comme de l'espionnage, mais comme une responsabilité partagée. Plus important encore, si vous découvrez quelque chose qui ne vous plaît pas, ne faites pas immédiatement un scandale et ne grondez pas votre enfant. Essayez de prendre du recul et de comprendre pourquoi cela s'est produit. Votre enfant peut avoir entendu un nouveau mot et voulu en apprendre davantage. Au fil du temps, à mesure que votre enfant grandit, fait constamment des choix sûrs en ligne et est capable d'expliquer avec assurance dans quelle mesure certains contenus sont sûrs ou dangereux, vous pouvez progressivement réduire ces contrôles. L'objectif est de l'aider à acquérir de solides habitudes numériques, afin que la surveillance devienne inutile et soit remplacée par la confiance, une communication ouverte, et sa propre capacité à gérer les risques en ligne.



Phishing et liens malveillants

Le phishing constitue l'une des cybermenaces les plus courantes auxquelles les enfants sont confrontés en ligne. Il s'agit généralement d'un faux message, d'un faux site Internet ou d'une fausse annonce qui incite les utilisateurs à cliquer sur un lien malveillant, à saisir des données personnelles ou à télécharger un logiciel dangereux. Étant donné que le phishing semble souvent « normal », comme une notification liée à un prix, un fichier pour les devoirs ou une offre relative à un jeu, les enfants y sont particulièrement vulnérables.

1. Enseigner à votre enfant la règle d'or : « Ne clique pas sur ce qui te paraît suspect. »

Les enfants cliquent souvent rapidement, surtout lorsqu'ils sont enthousiasmés par un message comme « Tu as gagné un prix ! » ou « Des skins gratuits pour Roblox ! » Expliquez à votre enfant que les cybercriminels se font souvent passer pour quelqu'un ou quelque chose de familier afin de tromper les gens, tout comme dans les escroqueries de la vie réelle.

Donnez-lui des exemples : de faux messages provenant de « professeurs » lui demandant ses informations de connexion, des fenêtres contextuelles affirmant que son appareil est infecté, ou des annonces offrant des « V-Bucks gratuits ». Incitez-le à prendre du recul et à se dire : **« Est-ce que je connais cette personne ? Est-ce que cela me paraît trop beau pour être vrai ?** Si oui, je ne clique pas. Je dois toujours en parler d'abord à un adulte. »

2. Montrer à votre enfant à quoi ressemble le phishing (sans prendre de risques)

Plutôt que de simplement le mettre en garde, montrez-lui des exemples réels (ou des simulations sûres) d'emails de phishing, de fausses pages de connexion ou de fenêtres contextuelles liées à des escroqueries. Soulignez les signes révélateurs :
– les fautes d'orthographe – les URL étranges – le ton urgent (« Vous devez agir immédiatement ! »)
– les demandes de mots de passe ou de paiement

En vous prêtant ensemble à un exercice consistant à « repérer l'escroquerie », vous développez la conscience visuelle de votre enfant et vous lui apprenez ce qu'il doit éviter, comme il éviterait un inconnu dans la vie réelle.

3. Utiliser des filtres anti-spam puissants et des paramètres de navigation sécurisés

Configurez la messagerie électronique et le navigateur de votre enfant avec des filtres anti-spam puissants et une protection efficace contre le phishing. Installez une solution de sécurité fiable, comme Kaspersky Premium, qui offre une protection en temps réel contre les tentatives de phishing, les annonces malveillantes et les téléchargements dangereux. Ce type d'outil bloque souvent les pages dangereuses avant même que votre enfant ne puisse les voir.

4. Maintenir les applications et les systèmes à jour

De nombreuses attaques de phishing exploitent les failles de sécurité des navigateurs, des applications ou des systèmes d'exploitation obsolètes. Assurez-vous que les mises à jour automatiques sont activées pour les appareils, les applications de messagerie et les navigateurs de votre enfant. Cela permet de corriger les vulnérabilités avant que des pirates informatiques ne puissent en tirer parti.

5. Inculquer à votre enfant des habitudes de téléchargement sûres

Le phishing se présente souvent sous la forme de téléchargements de fichiers malveillants, en particulier dans les domaines de l'éducation et des jeux vidéo. Par exemple :
– un « fichier de devoirs » envoyé sur Discord – un « mod » pour Minecraft provenant d'un site aléatoire – un PDF envoyé par un inconnu sur WhatsApp

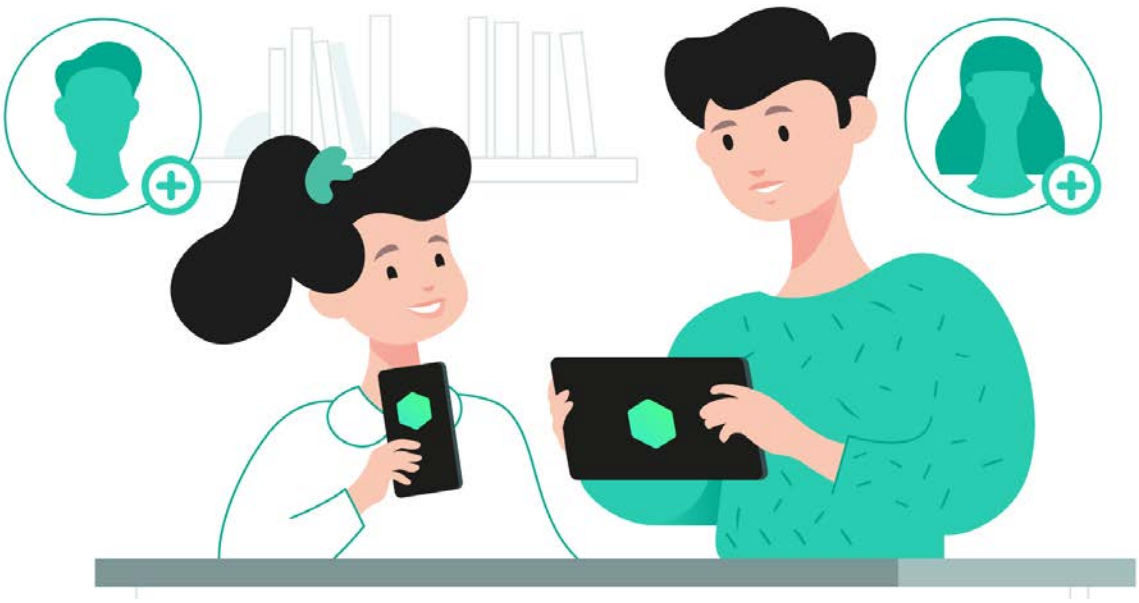
Expliquez à votre enfant qu'il ne doit télécharger que des fichiers provenant de sources fiables, comme ses professeurs, des sites Internet officiels ou des boutiques d'applications vérifiées. Établissez une règle : en cas de doute, il doit demander l'avis d'un adulte avant de télécharger quoi que ce soit.

6. Protéger les comptes de paiement et de boutiques d'applications

De nombreuses escroqueries incitent les enfants à dépenser accidentellement de l'argent réel, soit en leur demandant des informations de carte de crédit « pour recevoir un prix », soit en déclenchant des achats au moyen de l'application non désirés. Assurez-vous que toutes les boutiques d'applications et tous les dispositifs de paiement exigent des mots de passe, des données biométriques ou un accord parental avant toute transaction. Vérifiez également quels jeux et quelles plateformes ont enregistré vos informations de paiement, et supprimez ces dernières ou limitez-les dans la mesure du possible.

7. Signaler et bloquer les messages et les comptes suspects

Montrez à votre enfant comment signaler les fausses annonces, les messages liés à des escroqueries ou les comptes usurpés sur toutes les plateformes qu'il utilise. Qu'il s'agisse de TikTok, de YouTube, de Roblox ou d'Instagram, tous les services les plus connus disposent d'outils de signalement. Encouragez votre enfant à les utiliser, même si le message « est drôle » ou « n'est sans doute pas sérieux ». Apprenez-lui également à bloquer les utilisateurs qui envoient des offres ou des liens suspects et à ne jamais interagir avec eux. Même le fait de répondre « non merci » peut indiquer aux escrocs que le compte est actif et vulnérable.



Partage excessif

De nos jours, les enfants et les adolescents grandissent dans un monde où le partage est une seconde nature, qu'il s'agisse de publier des selfies et des vidéos ou de commenter chaque instant de leur vie. Ce qui paraît anodin et amusant pour un enfant peut néanmoins poser un risque sérieux pour la vie privée lorsque des informations confidentielles sont divulguées aux mauvaises personnes.

Le partage excessif n'a pas toujours l'air dangereux. Parfois, il s'agit simplement d'une photo d'anniversaire, d'un uniforme scolaire, d'une balise de localisation ou d'une discussion informelle sur ses projets pour le week-end. Cependant, les petits détails s'additionnent, et des cybercriminels, des cyberharceleurs ou des inconnus peuvent utiliser ces informations pour suivre, manipuler ou blesser un enfant.

1. Créer les comptes à deux, et vérifier régulièrement les paramètres de confidentialité

La création d'un compte sur les réseaux sociaux ou sur une messagerie doit toujours se faire à deux, en particulier pour les enfants de moins de 16 ans. Asseyez-vous avec votre enfant et parcourez ensemble le formulaire d'inscription. Cela vous aidera à comprendre la plateforme, à définir vos attentes et à configurer les paramètres de sécurité dès le départ.

- Utilisez uniquement le surnom ou le prénom de votre enfant. Évitez d'utiliser son nom complet, qui peut être associé à d'autres données personnelles.
- Ne mentionnez pas sa date de naissance, le nom de son école et sa ville de résidence dans les biographies et les profils publics. Ces informations peuvent être utilisées par des inconnus pour localiser votre enfant ou usurper son identité.
- Désactivez la géolocalisation dans les paramètres et dites à votre enfant de ne jamais indiquer sa position dans ses publications (par exemple : « Je suis à Montmartre en ce moment ! »).
- Limitez les commentaires ou les messages aux « amis uniquement » ou aux personnes que vous connaissez tous les deux dans la vie réelle.

2. Expliquer à votre enfant ce qu'il ne doit pas publier

Les enfants sous-estiment souvent tout ce qu'ils révèlent dans ce qui leur semble être une simple publication, histoire ou discussion. Classez les informations dans des catégories et expliquez à votre enfant **pourquoi** chaque catégorie présente un risque, pas seulement « parce que je le dis », mais car ces informations sont susceptibles d'être détournées, mal comprises ou manipulées.

Informations personnelles

Ne jamais mentionner dans une publication ou un message :
- Nom complet
- adresse du domicile ou nom de la rue
- numéro de téléphone, adresse email ou coordonnées des parents
- nom de l'école, numéro de la classe ou itinéraire du bus
- identifiant de l'élève, notes, résultats d'examens ou mots de passe

Ces informations peuvent être utilisées pour deviner les réponses aux questions de sécurité de votre enfant, trouver où il habite ou se faire passer pour lui en ligne.

Informations générales

Éviter de partager :
– où il se trouve actuellement
– où il se rend tous les jours
– ses projets de voyage à venir

Ces informations peuvent permettre à des inconnus de suivre les déplacements de votre enfant et de savoir lorsqu'il est seul ou sans surveillance.

Informations sensibles

Faire attention aux photos et vidéos :
– en uniforme scolaire présentant des écussons ou des insignes
– à l'intérieur du domicile, montrant l'aménagement, des objets de valeur ou des effets personnels
– en sous-vêtements, maillot de bain ou pyjama, même pour plaisanter
– d'autres enfants, partagées sans leur autorisation

Une fois partagées, ces photos et vidéos peuvent être copiées, partagées à nouveau ou utilisées à des fins de harcèlement, souvent sans que l'enfant s'en rende compte.

3. Discuter de l'empreinte numérique et de ses conséquences à long terme

Même si une publication disparaît, Internet n'oublie jamais. Les photos supprimées peuvent faire l'objet d'une capture d'écran, d'une copie ou d'un archivage. De futurs employeurs, écoles ou équipes sportives pourraient un jour examiner la présence en ligne de votre enfant, ou quelqu'un pourrait essayer de lui causer du tort des années plus tard à l'aide d'une ancienne publication.

Formulez-le de manière positive : **« Tu construis ta réputation numérique chaque jour. Essaie d'en faire quelque chose dont tu es fier. »** Incitez votre enfant à partager ses passe-temps, ses accomplissements, ses œuvres d'art ou des messages gentils, c'est-à-dire des choses qui reflètent ses valeurs et sa personnalité d'une manière saine.

Blogging et streaming

Plus de 30 % des enfants déclarent aspirer à devenir créateurs de contenu sur les réseaux sociaux, et des études montrent qu'environ 32 % des jeunes de 12 à 15 ans citent le métier de « youtubeur » comme le métier de leurs rêves. Pour les enfants, les créateurs de contenu sont des modèles, et leur désir de briller en ligne apparaît avant même l'adolescence. Dans un tel contexte, l'implication des parents n'est pas seulement utile, elle est vitale. Lorsque les parents jouent un rôle actif, en apprenant comment fonctionnent les plateformes, en configurant avec leurs enfants les paramètres de sécurité et de confidentialité et en discutant ouvertement des limites à respecter, ce voyage numérique partagé transforme les risques potentiels en opportunités d'apprentissage et aide les enfants à explorer leur créativité en toute confiance.

1. Faire preuve de curiosité, sans se montrer critique. Votre ouverture d'esprit constitue le filet de sécurité de votre enfant.

Lorsqu'un enfant dit « Je veux créer un blog » ou « Je veux devenir youtubeur », cela peut susciter des inquiétudes, surtout si les parents pensent aux trolls, aux escrocs ou au partage excessif. Cependant, la première mesure la plus sûre ne consiste pas à couper le dialogue, mais à l'ouvrir. Demandez à votre enfant pourquoi il souhaite tenir un blog et ce qu'il veut y publier. Cette approche permet deux choses importantes : premièrement, elle montre à votre enfant que vous prenez ses centres d'intérêt au sérieux, ce qui permet d'instaurer un climat de confiance. Deuxièmement, cela vous donne l'occasion d'aborder naturellement des sujets liés à la sécurité, comme les paramètres de confidentialité, les limites en matière de contenu et la gestion de l'attention en ligne.

Pour rendre ces conversations plus faciles et plus intéressantes, commencez par utiliser des ressources adaptées à l'âge de votre enfant. Par exemple, l'abécédaire de la cybersécurité de Kaspersky, un manuel téléchargeable gratuitement, aide les enfants à apprendre les bases de l'hygiène numérique d'une manière simple et amusante. Il présente les concepts clés de la cybersécurité dans un langage accessible et au moyen d'illustrations colorées, ce qui permet aux enfants de comprendre comment repérer les escroqueries, protéger leurs données et rester en sécurité tout en explorant leur créativité en ligne.

2. Rechercher régulièrement le pseudonyme de votre enfant sur Google

Une fois que votre enfant commence à publier sous un pseudonyme, il est important de faire preuve de vigilance quant à sa visibilité et à la possibilité de le trouver en ligne. Une manière simple d'y parvenir consiste à rechercher régulièrement son pseudonyme sur Google. Recherchez son nom d'utilisateur, le nom de son blog ou son pseudo sur les réseaux sociaux, et voyez ce qui apparaît. Y a-t-il des photos personnelles, des balises de localisation ou des commentaires qui en révèlent plus qu'ils ne le devraient ? Quelqu'un a-t-il copié son contenu ou tenté de se faire passer pour lui ?

3. Mettre votre enfant en garde contre les collaborations frauduleuses ou les offres douteuses

À mesure que les jeunes blogueurs gagnent en visibilité, ils peuvent commencer à recevoir des messages provenant de prétendus marques ou comptes leur offrant des produits gratuits, des parrainages ou des opportunités de collaboration. Pour un enfant, cela peut sembler être un rêve qui devient réalité, mais dans de nombreux cas, il s'agit d'une escroquerie. Apprenez à votre enfant à traiter chaque offre inattendue avec prudence. Les demandes de fausses « collaborations » sont souvent envoyées par message privé ou par email et peuvent inclure des liens vers des sites de phishing conçus pour voler des identifiants de connexion, des données personnelles, ou même des informations bancaires. Certains escrocs demandent également de payer une avance pour les « frais d'expédition » pour de faux cadeaux ou tentent d'inciter les enfants à installer des applications malveillantes.

Aidez votre enfant à repérer les signaux d'alerte, comme une grammaire incorrecte ou un ton urgent (« Agissez immédiatement ! »), des demandes d'informations personnelles ou de mots de passe, des liens suspects ou des sites Internet douteux, des comptes non vérifiés se faisant passer pour de vraies marques.

Pour les enfants plus jeunes, il est préférable que toutes les interactions liées aux activités commerciales, notamment la lecture des messages privés, l'analyse des offres provenant de marques et les réponses aux demandes de collaboration, soient gérées par les parents. Discutez ensemble des marques avec lesquelles il est approprié de travailler et expliquez à votre enfant pourquoi certaines offres ne sont pas aussi inoffensives qu'il n'y paraît.

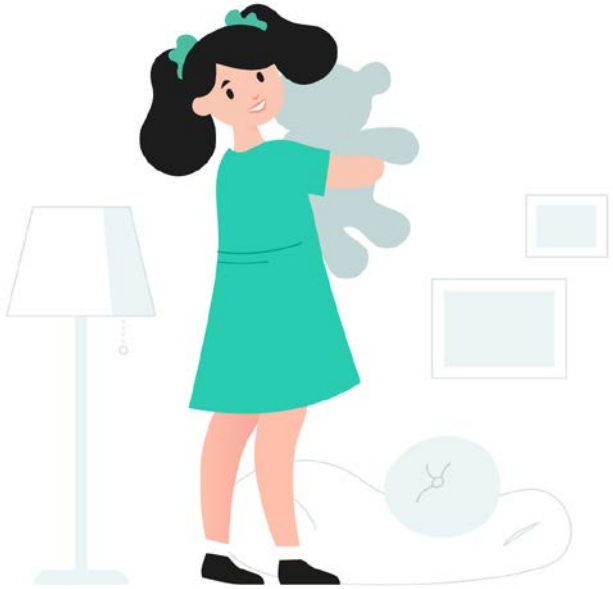
4. Parler à votre enfant des inconnus en ligne

À mesure que votre enfant développe son audience, il risque d'attirer non seulement des fans, mais également des personnes au comportement inapproprié ou manipulateur. Malheureusement, le grooming en ligne est une menace réelle, en particulier pour les jeunes créateurs ouverts et confiants qui partagent des détails sur leur vie. Expliquez à votre enfant que toutes les personnes qui paraissent gentilles en ligne n'ont pas forcément de bonnes intentions. Les groomers agissent souvent comme des « amis qui soutiennent » : ils font l'éloge du contenu de votre enfant, lui proposent leur aide, ou prétendent avoir les mêmes centres d'intérêt que lui. Au fil du temps, ils peuvent lui demander des informations personnelles et des photos privées ou essayer de rediriger la conversation vers des supports moins sûrs, comme des chats privés, des appels vidéo ou des messageries chiffrées.

Apprenez à votre enfant à reconnaître les signaux d'alerte :

- Un inconnu qui lui envoie des messages fréquents ou trop personnels
- Quelqu'un qui insiste sur le fait de garder le secret (« N'en parle pas à tes parents »)
- Des pressions pour l'inciter à partager des informations ou des images privées
- Une manipulation émotionnelle : culpabilisation, flatteries ou menaces

Plus important encore, veillez à faire savoir à votre enfant qu'il peut se tourner vers vous sans craindre une punition.



IA et enfants

L'intelligence artificielle prend de plus en plus de place dans l'univers numérique de votre enfant, qu'il s'agisse de chatbots et d'outils d'écriture alimentés par l'IA, de jouets intelligents, de moteurs de recommandations ou de professeurs virtuels. D'après le rapport de Kaspersky, la curiosité des enfants pour l'IA a plus que doublé en 2025. Si ces technologies peuvent favoriser l'apprentissage et la créativité, elles soulèvent également d'importantes questions en matière de confidentialité, de sécurité et d'éthique. En tant que parent, vous jouez un rôle clé dans l'accompagnement de votre enfant dans cette nouvelle réalité.

1. Expliquer à votre enfant ce qu'est l'IA, et ce qu'elle n'est pas

Les enfants pensent souvent que l'IA est « juste un robot intelligent » ou un ami qui sait tout. Expliquez-lui que l'IA ne « pense » pas et ne « ressent » pas. Elle génère des réponses basées sur des modèles de données, et non sur des émotions ou des intentions. Cela s'avère particulièrement important pour les jeunes enfants qui pourraient tisser des liens affectifs avec des avatars d'IA, des chatbots ou des « amis IA ». Aidez votre enfant à comprendre les limites de l'IA : celle-ci peut être utile à des fins de réflexion ou de recherche, mais elle peut également commettre des erreurs, partager des contenus biaisés ou paraître sûre d'elle-même lorsqu'elle se trompe. Incitez votre enfant à vérifier les informations générées par des IA et à ne jamais les considérer comme automatiquement vraies.

2. Parler de la protection de la vie privée lors de l'utilisation d'outils d'IA

Les outils d'IA collectent souvent de grandes quantités de données personnelles, notamment ce que votre enfant tape, demande ou télécharge. Expliquez-lui clairement qu'il ne doit jamais partager son vrai nom, des informations sur son école, des photos ou des informations confidentielles avec des plateformes d'IA, en particulier celles connectées à Internet. Examinez les politiques de confidentialité de toutes les applications ou de tous les sites Internet basés sur l'IA que votre enfant utilise. Si la collecte de données n'est pas transparente ou est excessive, renoncez complètement à cet outil, ou trouvez une alternative sûre pour les enfants.

3. Fixer des limites à l'utilisation non supervisée de l'IA

Bien qu'une utilisation non supervisée de l'IA puisse sembler sans danger, elle peut exposer les enfants à des contenus dangereux ou à des informations erronées, en particulier par le biais d'outils libres d'utilisation comme ChatGPT, les bots de personnages ou les générateurs d'images basés sur l'IA. Fixez des règles claires :

- Demander l'autorisation avant d'utiliser de nouveaux outils d'IA
- Utiliser l'IA dans les pièces communes
- Éviter les plateformes d'IA qui permettent des interactions anonymes entre utilisateurs

Expliquez à votre enfant que certains modèles d'IA sont formés à partir de l'ensemble du contenu disponible sur Internet, y compris du contenu nocif ou dangereux, de sorte que même des questions innocentes peuvent parfois donner des réponses dérangeantes.

4. Encourager une utilisation éthique, sans raccourcis

L'IA peut être un raccourci tentant pour les devoirs, les dissertations ou les travaux créatifs. Cependant, le fait de trop en dépendre peut nuire à l'esprit critique et à la créativité. Discutez avec votre enfant de ce qui est honnête et de ce qui constitue une tricherie en matière d'utilisation de l'IA. Voici une bonne règle à lui enseigner : **« Utilise l'IA pour soutenir ta réflexion, pas pour la remplacer. »** Par exemple, il est acceptable de chercher des idées, des définitions ou des résumés, mais pas de copier des réponses entières ou de présenter un travail rédigé par une IA comme étant le sien. Cette règle permet de développer une intégrité numérique dès le plus jeune âge.

5. Mettre votre enfant en garde contre le téléchargement de logiciels provenant de sources non officielles

Cela est particulièrement valable pour les programmes qui prétendent offrir des outils « exclusifs » pour les travaux scolaires et qui promettent de « résoudre instantanément n'importe quel problème lié aux devoirs ». Les cybercriminels déguisent souvent leurs programmes malveillants en outils d'étude utiles, en utilisant des noms attrayants et de fausses marques éducatives pour inciter les élèves à cliquer sur des liens suspects.

Expliquez à votre enfant que les téléchargements à partir de sites Internet non vérifiés, de plateformes de partage de fichiers ou de liens aléatoires dans des groupes de discussion peuvent compromettre son appareil, permettre de voler ses données personnelles, ou même bloquer ses comptes.

6. Faire attention aux deepfakes et aux supercheries générées par IA

L'IA est désormais capable de créer de fausses images, vidéos ou voix hyperréalistes, appelées deepfakes. Les enfants peuvent tomber dessus sur TikTok, YouTube ou dans des discussions de groupe sans se rendre compte qu'il s'agit de faux.

Apprenez à votre enfant à repérer les signaux d'alerte :

- Des mouvements d'yeux étranges ou des lèvres mal synchronisées dans les vidéos
- Des visages trop parfaits ou à l'apparence robotique
- Une manipulation émotionnelle (par exemple, de fausses actualités ou des escroqueries impliquant des célébrités)

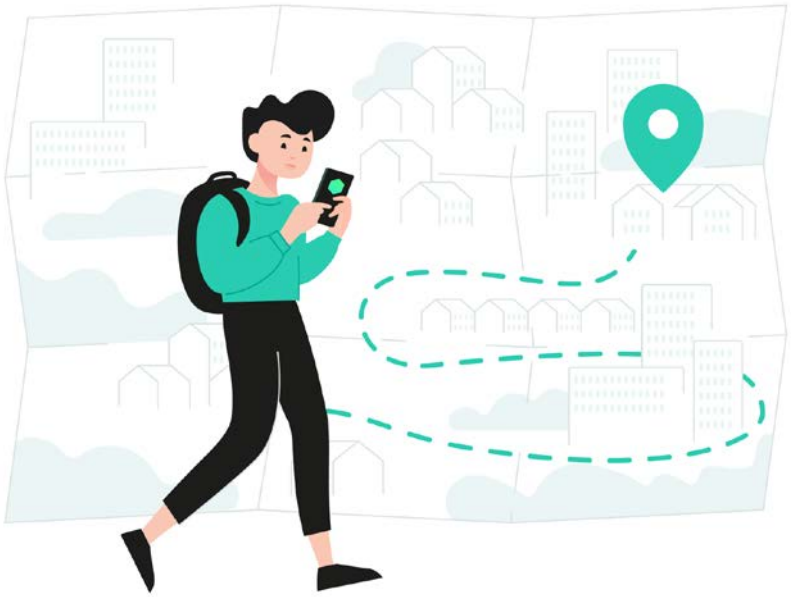
Encouragez un scepticisme sain : **« Ce n'est pas parce que tu le vois que cela est réel. »** Montrez des exemples et démystifiez-les ensemble. Faites-en un exercice de réflexion critique.

Monde hors ligne

Dès lors qu'une nouvelle année scolaire commence, les enfants passent souvent plus de temps seuls : ils vont à l'école à pied, prennent les transports en commun, participent à des activités extrascolaires ou étudient à la bibliothèque. Cette indépendance croissante constitue une étape passionnante et importante : elle les aide à prendre confiance en eux, à développer leur capacité à prendre des décisions et à apprendre à évoluer dans le monde qui les entoure.

Cependant, à mesure que les enfants gagnent en autonomie, ils sont de plus en plus exposés aux risques du monde réel, dont beaucoup ont des conséquences numériques. La cybersécurité ne se limite pas au monde en ligne : elle commence par des choix opérés au quotidien dans le monde hors ligne. Dans cette section, nous allons découvrir comment les parents peuvent aider leurs enfants à adopter des habitudes sûres dans les lieux publics, à protéger leur vie numérique lorsqu'ils se déplacent et à prendre conscience que la vigilance dans le monde réel est tout aussi importante que les règles relatives au temps d'utilisation des écrans.

De la sécurité physique sur le chemin de l'école à l'utilisation intelligente du Wi-Fi public, en passant par le fait de garder ses appareils en sécurité dans son sac à dos, ces leçons préparent les enfants à évoluer dans le monde avec confiance et prudence.



Sécurité physique

Si la cybersécurité se concentre souvent sur les applications, les appareils et les réseaux, la sécurité dans le monde réel joue un rôle tout aussi important dans la protection de votre enfant. Les enfants en âge d'aller à l'école sont de plus en plus mobiles : ils se rendent seuls à l'école à pied, prennent les transports en commun, ou passent du temps dehors sans la surveillance d'un adulte. Ces moments de la vie quotidienne ont également des implications numériques : un appareil perdu, un mot de passe entendu par hasard ou une montre intelligente non protégée peut ouvrir la porte à des menaces en ligne.

1. Apprendre à votre enfant les règles de sécurité pour se déplacer à pied et effectuer son trajet domicile-école

Veillez à ce que votre enfant connaisse les règles de sécurité fondamentales à appliquer dans la rue : toujours traverser aux passages piétons, respecter les feux de signalisation, marcher sur les trottoirs, et ne jamais prendre de raccourcis en empruntant des ruelles ou des endroits inconnus. Si ces règles peuvent sembler évidentes, les enfants de moins de 12 ans peuvent facilement se laisser distraire, surtout s'ils portent des écouteurs ou regardent un écran en marchant.

Expliquez à votre enfant l'importance de faire preuve de vigilance et de ne pas utiliser d'appareils électroniques à proximité de routes ou dans les lieux publics. Adoptez le même comportement : rangez votre téléphone aux intersections, regardez à gauche et à droite, et retirez vos écouteurs lorsque vous marchez avec votre enfant. Lorsque les enfants voient les adultes adopter des habitudes sûres, ils sont plus enclins à les imiter.

2. Utiliser des systèmes de suivi et d'enregistrement par GPS

Envisagez d'utiliser des outils de sécurité équipés d'un GPS comme Kaspersky Safe Kids afin de surveiller le trajet de votre enfant en temps réel. De nombreuses applications vous permettent de configurer des alertes de géolocalisation : vous recevrez alors une notification si votre enfant quitte une zone donnée ou fait un détour inattendu.

Il n'est pas question d'espionnage, mais de tranquillité d'esprit. Faites preuve de transparence : expliquez à votre enfant pourquoi cet outil est mis en place et convenez de vérifications régulières par téléphone ou par message. Apprenez-lui à vous contacter rapidement en cas d'urgence et répétez ce qu'il doit faire s'il se sent en danger pendant son trajet.

Pour les parents, il est tout aussi important de sécuriser le compte de suivi : activez l'authentification à deux facteurs, utilisez un mot de passe unique et fort, et vérifiez régulièrement les appareils connectés afin de garantir la confidentialité des données de localisation.

3. Sécuriser les appareils transportés en dehors du domicile

Les enfants transportent souvent avec eux des smartphones, des montres intelligentes, des tablettes ou des ordinateurs portables. Il s'agit de cibles de grande valeur pour le vol et l'exposition des données. Apprenez à votre enfant à garder ses appareils dans un sac fermé et hors de vue lorsqu'il ne les utilise pas et à ne jamais les laisser sans surveillance, même « juste une seconde ». Configurez des codes de verrouillage pour ses appareils, activez les fonctionnalités d'effacement à distance (comme « Localiser mon iPhone » ou « Localiser mon appareil ») et sauvegardez ses travaux scolaires dans un cloud. Ainsi, même en cas de perte ou de vol d'un appareil, les informations de votre enfant resteront protégées.

4. Faire preuve de prudence avec le Wi-Fi public

Si les réseaux Wi-Fi publics (dans les écoles, les cafés, les aéroports ou les transports publics) peuvent sembler pratiques, ils présentent souvent de sérieux risques en matière de sécurité. Ces réseaux sont rarement chiffrés, ce qui implique que les cybercriminels peuvent intercepter les données que votre enfant envoie et reçoit, y compris ses identifiants de connexion, ses messages, et même ses photos.

Apprenez à votre enfant une règle simple : ne jamais se connecter à des comptes personnels (comme une messagerie électronique, une banque ou un espace de stockage dans le cloud) par le biais d'un réseau Wi-Fi public, à moins d'utiliser un VPN de confiance. Un VPN chiffre les données transférées, ce qui rend leur espionnage par des tiers beaucoup plus difficile.

5. Mettre en place des alertes en cas de connexions ou d'activités suspectes

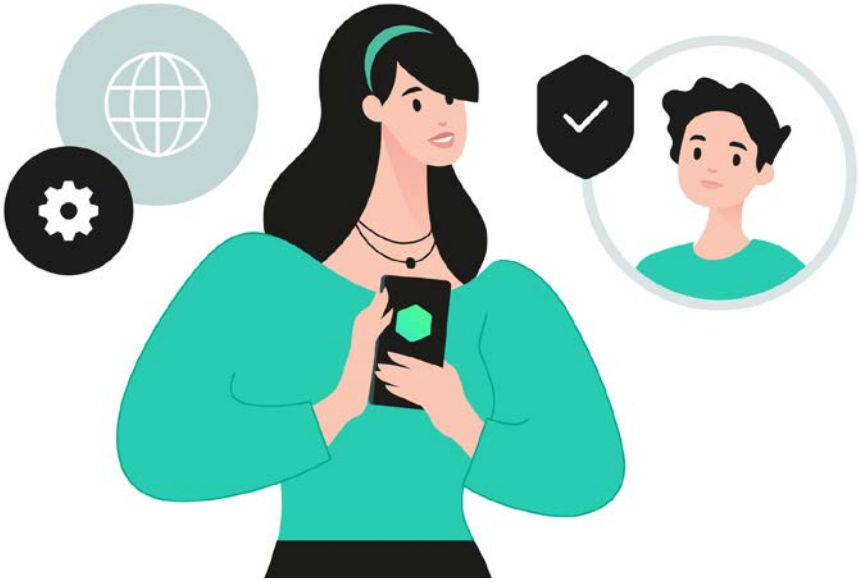
Activez les **alertes de connexion** afin d'être averti en cas d'accès au compte de votre enfant à partir d'un emplacement ou d'un appareil inhabituel. Ces alertes peuvent aider à détecter si quelqu'un a eu accès à ses identifiants par le biais d'une session Wi-Fi non sécurisée. Encouragez votre enfant à signaler tout événement inhabituel, comme une déconnexion inattendue ou l'apparition de fenêtres contextuelles étranges, même s'il n'est pas sûr de ce qui se passe. Mieux vaut prévenir que guérir.

6. Entraîner votre enfant à avoir des conversations sûres en public

Rappelez à votre enfant de ne pas divulguer à voix haute des informations personnelles (comme son adresse, ses mots de passe ou ses projets de voyage) dans des lieux publics. S'il utilise un téléphone ou une application de messagerie, assurez-vous qu'il ne partage pas d'informations privées là où d'autres personnes pourraient facilement l'entendre ou jeter un coup d'œil à son écran. Cela s'avère particulièrement important lorsque les enfants se retrouvent seuls dans le bus, dans des centres commerciaux ou lors d'activités extrascolaires. La confidentialité numérique commence par la conscience de son environnement.

7. Planifier les situations d'urgence, et répéter les étapes à suivre

Donnez à votre enfant les coordonnées des personnes à contacter en cas d'urgence et veillez à ce qu'il sache comment agir en cas de crise. Qui doit-il appeler ? Où doit-il aller s'il ne se sent pas en sécurité ou s'il se perd ? Jouez des scénarios simples : perte de téléphone, porte claquée, bus manqué ou comportement suspect. Entraînez votre enfant à réagir calmement, sans paniquer. L'objectif est de renforcer sa confiance et son degré de préparation, et non sa peur.



Sécurité des informations financières

Au fur et à mesure que les enfants gagnent en indépendance, leurs habitudes financières commencent souvent à se former en même temps que leurs habitudes numériques. Qu'il s'agisse d'acheter leur déjeuner ou d'effectuer des achats dans un jeu vidéo, les enfants d'aujourd'hui gèrent de l'argent réel par le biais d'applications, de cartes et de plateformes en ligne, souvent avant d'en comprendre pleinement les risques.

1. Fixer des limites de dépenses claires

Commencez par établir une structure budgétaire de base pour les dépenses courantes de votre enfant :
– les fournitures scolaires – la nourriture ou l'argent pour le déjeuner – les achats liés au sport ou aux loisirs – le divertissement (applications, jeux, abonnements)

Plutôt que de contrôler minutieusement chaque achat, parlez de pourcentages. Par exemple : « 70 % pour les dépenses scolaires, 20 % pour le divertissement, 10 % pour l'épargne. » Profitez de cette occasion pour lui enseigner les bases de l'argent numérique : expliquez-lui comment les achats au moyen d'applications, les microtransactions ou les frais cachés peuvent épuiser son solde s'il ne fait pas attention.

2. Utiliser des modes de paiement sécurisés

Au lieu de donner à votre enfant de l'argent liquide, qui peut être perdu ou volé, optez pour des cartes bancaires adaptées aux enfants ou pour des portefeuilles numériques dotés d'un contrôle parental. De nombreuses applications bancaires offrent des fonctionnalités comme :
– limites de dépenses – notifications d'achat – historique des transactions en temps réel – blocage de certaines catégories (par exemple, jeux ou places de marché en ligne)

En parallèle, installez une solution de cybersécurité qui comprend une navigation sécurisée et une protection sécurisée des paiements. Ainsi, lorsque votre enfant effectue des achats en ligne pour des fournitures scolaires, des jeux ou des abonnements, ses données bancaires sont chiffrées et protégées contre les enregistreurs de frappe, les fausses pages de paiement et les attaques de l'homme du milieu.

3. Sécuriser les appareils et les comptes bancaires

Si les enfants ne comprennent peut-être pas complètement l'importance de la sécurité des comptes, un mot de passe faible ou un appareil volé peut exposer tous leurs outils financiers. En tant que parent, vous pouvez apporter votre aide en :
– activant l'authentification à deux facteurs (2FA) pour chaque application impliquant de l'argent – utilisant un gestionnaire de mots de passe, qui stocke les identifiants en toute sécurité et permet aux autres membres de la famille d'y accéder en cas de problème – lui enseignant les principes de base des mots de passe forts, à savoir utiliser au moins 12 caractères, éviter les noms ou les dates de naissance et ne pas réutiliser les mêmes mots de passe sur plusieurs plateformes

4. Discuter des cybermenaces qui ciblent les jeunes utilisateurs

Si les enfants peuvent penser que les escroqueries ne touchent que les adultes, en réalité, les cybercriminels ciblent souvent les enfants et les adolescents, qui sont plus confiants et moins expérimentés.

Expliquez à votre enfant les formes courantes d'escroqueries financières :
– emails de phishing prétendant provenir de sa banque ou de son magasin préféré – faux cadeaux demandant des informations bancaires – escroqueries de type « ami dans le besoin », dans lesquelles quelqu'un demande de l'argent par le biais d'un compte piraté – escroqueries dans les jeux vidéo proposant des objets « gratuits » en échange d'informations de connexion

Apprenez à votre enfant à se méfier des liens, des offres et des messages privés qui créent un sentiment d'urgence (« Faites-le maintenant ou vous perdrez votre compte ! »). Incitez-le à vous consulter avant de saisir des informations bancaires en ligne.

5. Garder un œil sur les abonnements et les frais récurrents

De nombreuses applications et plateformes, en particulier les jeux, les outils d'apprentissage et les services de streaming, proposent désormais des modèles d'abonnement plutôt que des achats ponctuels. Les enfants peuvent facilement s'inscrire à un « essai gratuit », qui se transforme ensuite en frais mensuels sans qu'ils s'en aperçoivent.

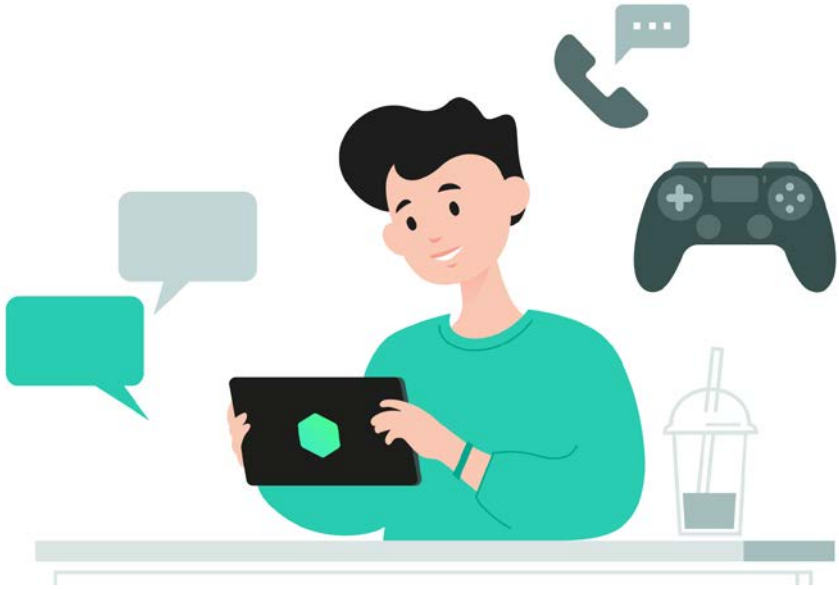
Apprenez à votre enfant à :
– toujours demander avant de commencer un essai gratuit – rechercher les paramètres de « renouvellement automatique » et annuler ce dernier – définir des rappels dans le calendrier pour les dates de fin d'essai

En tant que parent, consultez chaque mois l'historique des achats effectués dans la boutique d'applications, et vérifiez régulièrement les emails pour repérer les notifications de renouvellement cachées. Vous pouvez également utiliser des outils qui signalent les frais récurrents ou envoient des alertes pour chaque transaction.

6. Faire attention aux signes avant-coureurs d'usurpation d'identité

Si les informations personnelles ou financières de votre enfant ont été divulguées, vous pouvez remarquer :
– des achats inattendus – des blocages de compte ou des emails de réinitialisation de mot de passe – des notifications étranges provenant de plateformes qu'il n'utilise pas

Utilisez des outils de surveillance ou des alertes de crédit, le cas échéant, pour détecter rapidement toute activité suspecte. Apprenez à vos enfants plus âgés à reconnaître ces signaux d'alerte et à les signaler immédiatement, plutôt que de les ignorer par peur.



IdO et appareils intelligents

Haut-parleurs intelligents, jouets interactifs, montres intelligentes, assistants domestiques, tablettes d'apprentissage : l'Internet des objets (IdO) devient progressivement partie intégrante de la vie quotidienne des enfants. Ces appareils rendent l'apprentissage plus interactif, le divertissement plus immersif, et les tâches quotidiennes plus simples. Cependant, ils présentent également de nouveaux risques en matière de confidentialité et de cybersécurité, que bon nombre de familles ignorent. Contrairement aux écrans traditionnels, les appareils de l'IdO sont toujours allumés, toujours connectés et souvent à l'écoute, ce qui crée un besoin unique de vigilance et de contrôle numériques permanent.

1. Superviser l'utilisation et choisir des appareils sécurisés

Au début, il est essentiel de surveiller la manière dont votre enfant interagit avec les appareils intelligents. Qu'il s'agisse d'un assistant vocal, d'un jouet intelligent ou d'une tablette d'apprentissage connectée, tenez-vous informé de la manière dont il est utilisé et des fonctionnalités activées.

Lorsque vous choisissez un appareil, privilégiez :
– le contrôle parental intégré – des paramètres axés sur la confidentialité – des politiques claires en matière de données utilisateur – la possibilité de couper les microphones ou de désactiver l'écoute lorsqu'ils ne sont pas utilisés – l'approbation manuelle des nouvelles fonctionnalités et applications et des nouveaux contacts

Dans la mesure du possible, laissez les appareils intelligents dans les pièces communes comme la cuisine ou le salon, et non dans les chambres, et envisagez de limiter leur utilisation sans supervision.

2. Enseigner à votre enfant les règles de sécurité de base pour les interactions intelligentes

Les enfants peuvent anthropomorphiser les assistants vocaux ou les jouets intelligents et commencer à leur parler comme à des amis de confiance. C'est pourquoi il est essentiel de leur enseigner les limites d'une communication sûre, en particulier lorsque l'appareil est connecté à Internet.

Apprenez à votre enfant :
– à ne jamais communiquer son nom complet, son numéro de téléphone, son adresse ou des informations sur son école
– à ne pas parler de ses habitudes familiales, de ses mots de passe ou de ses problèmes personnels – que les assistants vocaux peuvent « sembler sympathiques », mais qu'il ne s'agit pas de personnes et qu'ils ne sont pas confidentiels

Entraînez-vous ensemble en faisant des jeux de rôle pour déterminer « ce qu'il est acceptable et ce qu'il n'est pas acceptable » de dire à haute voix. Expliquez à votre enfant comment certains jouets intelligents enregistrent les interactions afin d'améliorer leurs performances, et pourquoi il est important de les traiter comme des inconnus numériques.

3. Ajuster les paramètres de confidentialité et désactiver les fonctionnalités inutiles

De nombreux appareils intelligents sont dotés de paramètres par défaut qui privilégient le confort au détriment de la sécurité. En tant que parent, prenez le temps d'examiner attentivement les paramètres.

Voici les actions clés :
– désactiver le téléchargement automatique des enregistrements vocaux ou la synchronisation dans le cloud, si possible – désactiver le suivi de localisation, sauf en cas d'absolue nécessité – supprimer régulièrement l'historique des interactions ou les journaux vocaux – préférer les mises à jour manuelles aux mises à jour automatiques lorsque cela est possible, afin de pouvoir examiner les changements – vérifier si des compétences ou des fonctionnalités tierces ont été activées sans votre consentement

4. Mettre à jour les micrologiciels et surveiller l'accès aux appareils

Les appareils intelligents obsolètes sont plus vulnérables aux cyberattaques. Veillez à ce que les micrologiciels et les logiciels soient toujours mis à jour, soit manuellement, soit à l'aide de paramètres de mise à jour automatique fiables.

Par ailleurs :
– limitez les comptes et applications connectés à l'appareil – utilisez des mots de passe forts et uniques pour les hubs intelligents et les comptes d'application – vérifiez régulièrement l'historique de connexion ou les journaux d'accès si la plateforme les fournit – éteignez les microphones et les caméras lorsqu'ils ne sont pas utilisés.

Par exemple, les téléviseurs et haut-parleurs intelligents et les tablettes sont autant de points d'accès potentiels non autorisés s'ils ne sont pas correctement sécurisés.

5. Continuer à discuter

L'évolution des appareils intelligents s'accompagne d'une augmentation des risques. Ce qui semble sûr aujourd'hui pourrait être exploité demain. Instaurez une culture familiale où poser des questions et signaler les comportements étranges est toujours encouragé.

Posez les questions suivantes :
– « Est-ce que quelque chose d'étrange s'est produit pendant que tu utilisais l'appareil ? »
– « Est-ce que l'appareil t'a demandé de dire ou de faire quelque chose ? »
– « Est-ce que l'appareil a agi d'une manière qui t'a surpris ou effrayé ? »

Ces questions permettent à votre enfant de faire preuve de vigilance et vous aident à détecter rapidement les problèmes potentiels.

Ressource complémentaire : Liste de vérification des premiers appareils

Tôt ou tard, (presque) tous les parents en viennent inévitablement à acheter à leurs enfants leur propre appareil électronique. D'après une étude de Kaspersky, 61 % des enfants reçoivent leur premier appareil entre 8 et 12 ans et, cela peut paraître étonnant, ils sont 11 % à recevoir leur propre téléphone portable ou tablette avant l'âge de cinq ans. Il est essentiel pour les parents de connaître les recommandations avant d'introduire un appareil dans la vie de leurs enfants pour la première fois.

Kaspersky présente, en collaboration avec la psychologue clinicienne Dre Saliha Afridi, les considérations sécuritaires et psychologiques à avoir en tête avant d'offrir à ses enfants leurs tout premiers gadgets technologiques.

Que faire avant d'offrir un appareil électronique à un enfant ?

Configurez un compte enfant avant d'offrir son premier appareil électronique à votre enfant. Qu'il s'agisse d'un téléphone ou d'une tablette, il est essentiel de s'assurer que l›appareil convient à l'âge de l'utilisateur et qu'il est sûr. Même s'il s'agit d'un cadeau flambant neuf, configurez cette fonctionnalité en premier lieu. Un compte enfant agit comme une protection sur l'appareil, empêchant des opérations comme le téléchargement de contenu pour adultes ou de chansons au contenu explicite. Pour obtenir des informations détaillées sur la création d'un compte enfant, consultez notre guide pour Android ou celui pour iOS.

Installez toutes les applications de base qui prennent en charge la communication ou la géolocalisation (comme les applications de messagerie et de cartes), ainsi que les applications d'apprentissage. Et n'oubliez pas de configurer les paramètres de confidentialité dans chacune des applications installées, pour éviter que le numéro de téléphone ne permette à des inconnus de remonter jusqu'à votre enfant. Des outils comme un vérificateur de confidentialité peuvent vous aider à configurer les paramètres de protection optimaux pour différents appareils et plateformes.

Pensez aussi à installer une application parentale numérique. Celle-ci vous permettra de gérer le contenu, de surveiller le temps que votre enfant passe sur des applications spécifiques (et de définir des limites si nécessaire) et de suivre sa position actuelle.

Comment introduire un nouvel appareil dans la vie d'un enfant ?

Expliquez-lui les fonctionnalités de l'appareil ainsi que les dangers potentiels en lui offrant. C'est le moment idéal pour explorer ses fonctionnalités et comprendre ses pièges potentiels.

Rédigez ensemble une série de règles d'utilisation familiales. Au cours de cette conversation, il est important de favoriser la compréhension et le consensus sur les responsabilités et les attentes liées à la possession d'un appareil. Pour garantir un équilibre sain, définissez des zones et des horaires sans technologie, peut-être pendant le dîner ou les heures précédant le coucher. Désignez des moments dédiés aux loisirs non virtuels, comme la lecture, les jeux d'extérieur ou les puzzles, autant d'options bénéfiques pour remplacer le temps passé devant un écran. Il est essentiel de revoir et d'affiner régulièrement ces règles à mesure que votre enfant grandit et que la technologie progresse.

Et n'oubliez pas : à moins qu'un enfant ne montre un niveau d'engagement sain dans les activités de la vie réelle et dans les rencontres en personne, ne lui proposez pas de smartphone ni de réseaux sociaux. Un enfant pourrait par exemple montrer qu'il « mérite » un appareil en effectuant ses tâches quotidiennes de manière régulière et constante. On parle notamment de l'activité physique, du sommeil, des devoirs, des activités sociales, d'une alimentation saine et des périodes de repos éveillé.

Comment parler cybersécurité à un enfant ?

Encouragez une communication ouverte dès le départ. Entamez avec les enfants des discussions sur leur expérience en ligne, en vous assurant qu'ils se sentent en sécurité pour partager le positif comme le négatif.

Restez au fait des dernières tendances et menaces numériques, ainsi que des cas plus médiatisés de cyberharcèlement ou de violation des données. Partagez ces informations avec votre enfant d'une manière qu'il comprend. Vous pouvez suivre l'actualité en matière de cybersécurité sur notre blog.

Insistez sur le caractère permanent de ce qui se passe en ligne. Cela inclut la façon dont tout ce qui est partagé en ligne y reste pour toujours et peut avoir une incidence sur leur réputation et sur les opportunités futures. L'enfant doit être particulièrement prudent quant aux informations qu'il partage sur lui-même et ne jamais divulguer son adresse, sa géolocalisation, ses identifiants et mots de passe. De plus, il doit éviter d'utiliser son vrai nom comme identifiant, car celui-ci peut être utilisé par les individus malintentionnés pour découvrir ses autres comptes sur les réseaux sociaux. Aidez-le à comprendre le concept de vie privée et les risques liés au partage de trop d'informations.

Apprenez à votre enfant à refuser les demandes d'amis de personnes inconnues dans la vie réelle. Il est essentiel d'expliquer que si un inconnu cherche constamment à obtenir des informations personnelles à son sujet ou à propos de ses parents, il faut s'inquiéter. Votre enfant ne doit pas se sentir impoli ou grossier s'il ne répond pas à une demande d'amitié. Sur les réseaux sociaux, comme dans la vie, certaines informations doivent rester privées.

Grâce à ces conversations et en éduquant vos enfants sur les risques en ligne de manière non conflictuelle, vous élevez des enfants plus susceptibles de venir vers vous s'ils tombent sur quelque chose de suspect en ligne. Assurez-vous qu'ils gardent un sentiment de curiosité, et non de jugement ou de peur. Vos réactions détermineront dans quelle mesure ils seront ouverts au partage à l'avenir.

Et une **application parentale numérique** est un outil précieux pour vous permettre de surveiller les recherches et activités en ligne de vos enfants, afin de garantir une expérience virtuelle plus sûre.

Quels sont les principaux risques à signaler à mon enfant ?

À l'ère numérique, les enfants sont vulnérables aux cybercriminels, souvent parce qu'ils ne connaissent pas les principes fondamentaux de la cybersécurité et les tactiques courantes contre les escroqueries. Il est de notre devoir en tant qu'adultes de les éduquer à ce sujet avant qu'ils n'en fassent les frais par inadvertance.

Par exemple, aidez votre enfant à identifier les publicités trompeuses, les fausses propositions de sondage, les loteries contrefaites et d'autres stratagèmes qui peuvent compromettre ses données personnelles. Aidez-le à comprendre que, s'il peut être tentant de télécharger un film Barbie avant sa sortie officielle, de telles offres peuvent être un stratagème de la part des cybercriminels visant à voler des données, voire de l'argent de la carte de ses parents. Une solution de sécurité fiable peut détecter et bloquer tout site Internet de phishing ou tout logiciel malveillant.

Inculquez à votre enfant l'esprit critique et la prudence sur Internet. Apprenez-lui à faire une pause avant de cliquer sur des liens douteux, des pièces jointes inconnues d'un email ou des messages de provenance inconnue. Discutez des autorisations appropriées à accorder aux applications sur ses appareils. Par exemple, une application de calculatrice n'a aucune raison valable de demander l'accès à la position.

Rendez les conversations sur la cybersécurité plus agréables et intéressantes en abordant le sujet à l'aide de jeux et d'autres formats ludiques. Plus important encore, veillez à ce qu'il n'ait pas peur de s'adresser à un adulte de confiance s'il est confronté à des situations troublantes ou suspectes en ligne.

Comment vérifier si vous êtes prêt ?

L'arrivée d'un appareil électronique va inévitablement transformer votre vie de famille, puisque votre enfant sera attiré par Internet. Plutôt que de l'interdire, il est conseillé de lui montrer comment se comporter en ligne. Un appareil électronique, s'il est utilisé correctement, peut vraiment aider les enfants à apprendre et à grandir. Cependant, c'est seulement possible si les enfants savent quand et comment alerter leurs parents sur les menaces rencontrées en ligne, qu'il s'agisse de messages étranges d'adultes, de demandes d'informations personnelles ou de sites de phishing.

Cependant, l'apprentissage est un processus progressif et ne garantit pas la perfection dès le début. Votre enfant n'est pas à l'abri d'une erreur, comme télécharger par erreur un programme malveillant, interagir avec des individus suspects ou avoir du mal à gérer le temps passé devant son écran. Cependant, en tant que parent, votre rôle est de le soutenir et l'aider dans ses apprentissages. C'est la seule façon d'assurer la sécurité de votre enfant en ligne.