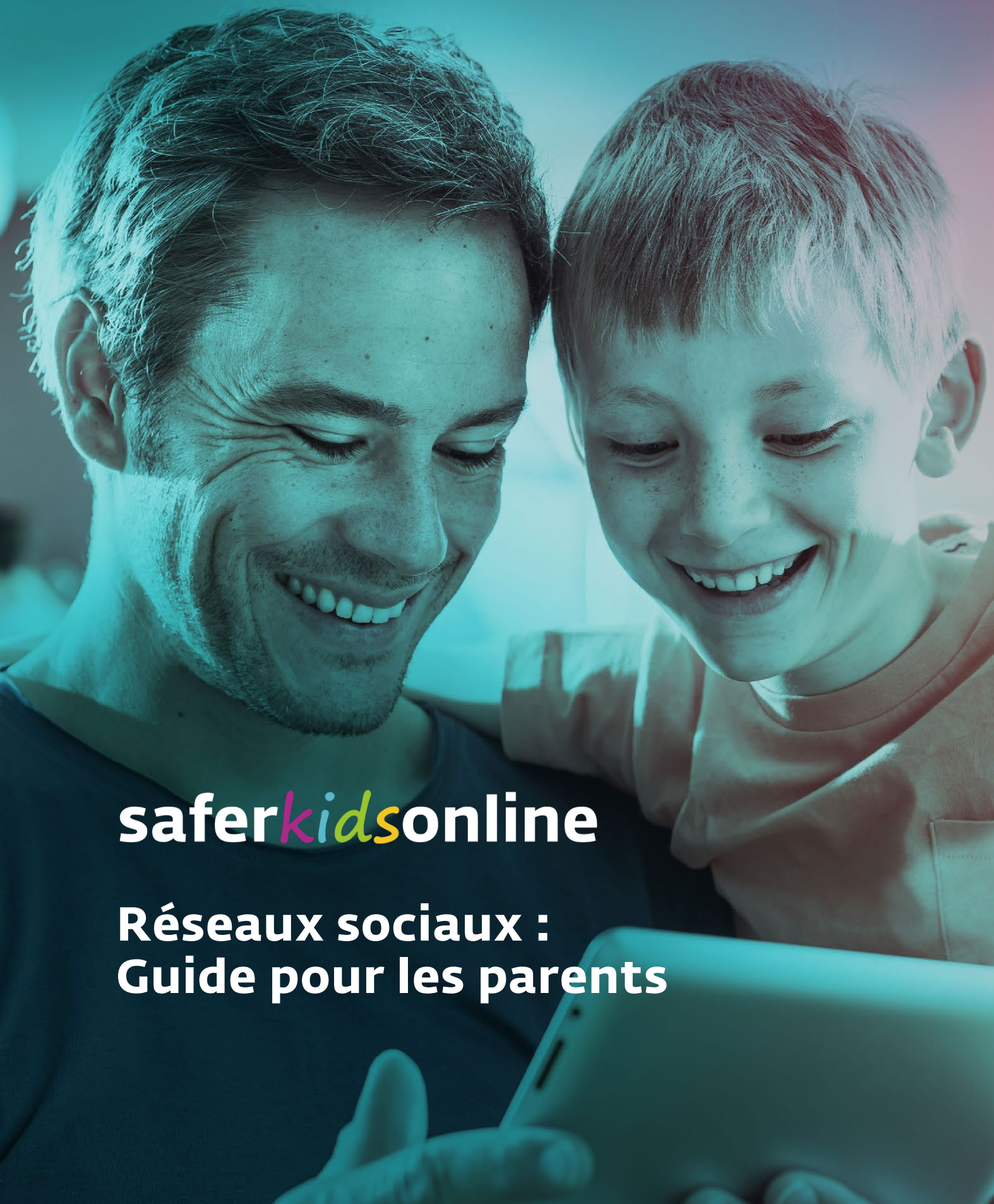
Digital Security
Progress. Protected.



saferkidsonline

Réseaux sociaux : Guide pour les parents

Introduction

Vous souvenez-vous d'une époque où les enfants jouaient à l'extérieur et ne rentraient à la maison que lorsqu'ils avaient faim ? Internet a changé tout cela. Aujourd'hui, les jeunes peuvent passer plusieurs heures chaque jour sur les réseaux sociaux.

Nous sommes nombreux chez ESET à être des parents, donc nous comprenons vos inquiétudes lorsque vous voyez votre enfant captivé par le monde digital. C'est pourquoi nous avons imaginé ce guide. Vous y trouverez des informations sur les éventuelles menaces qui planent sur les réseaux sociaux et des solutions qui vous aideront à protéger votre famille.

1. Voici ce à quoi vous devez faire attention :

Malwares

Ce terme désigne les logiciels malveillants, autrement dit des programmes nuisibles tels que les virus, vers et chevaux de Troie, quelques exemples parmi tant d'autres. Les escrocs utilisent les réseaux sociaux pour inciter les utilisateurs à télécharger des malwares, souvent avec la promesse qu'il s'agit de logiciels ou de jeux piratés.

Hameçonnage

Ce terme est un dérivé du monde de la pêche car dans ce cas de figure, un appât est utilisé pour attraper les victimes. De nombreux cybermalfaiteurs utilisent cette méthode pour voler des informations sensibles, telles que les identifiants d'accès au profil d'un enfant via un réseau social. Cela se fait généralement via un email prétendant provenir du réseau social en question. Il peut être assez difficile d'identifier une fausse page car les différences sont souvent mineures. Les enfants peuvent ainsi fournir des informations personnelles sans même se rendre compte que quelque chose cloche.

Vol d'identité

Veillez à ce que vos enfants ne publient pas d'informations sensibles telles que l'adresse et le numéro de téléphone du domicile, l'adresse de l'école, ou leur date de naissance, qui pourraient être utilisées pour les identifier. L'usurpation d'identité est une forme très répandue de cybercriminalité, par laquelle les criminels obtiennent les informations personnelles des utilisateurs afin de se faire passer pour eux et les utiliser à des fins malveillantes.

Un agresseur peut généralement obtenir ces données sensibles de deux façons :

- Soit par l'ingénierie sociale, souvent en se faisant passer pour un ami de votre enfant
- Soit par l'utilisation d'informations accessibles au public sur un profil de réseau social. La configuration appropriée des paramètres de confidentialité est donc cruciale.

Cyberharcèlement

Les menaces qui pèsent sur vos enfants sur les réseaux sociaux ne sont pas toutes le fait de cybercriminels. D'autres enfants peuvent également constituer un problème. Les brimades ne se limitent pas à l'enceinte de l'école : de nos jours, elles se prolongent sur Internet et peuvent être tout aussi néfastes que dans la vie réelle.

La manipulation psychologique à des fins d'abus sexuels, ou « grooming » est un autre risque majeur, surtout lorsqu'il s'agit de jeunes enfants. Elle implique qu'un adulte tente de gagner la confiance d'un enfant et d'établir une relation avec lui pour le persuader de se livrer à des activités sexuelles. Cela inclut souvent le sexting, des messages au contenu inapproprié qui pourraient être envoyés à votre enfant.

2. Quelles mesures pouvez-vous prendre pour protéger vos enfants ?

Au vu des menaces potentielles, l'utilisation des réseaux sociaux peut sembler être une activité dangereuse. Cependant, interdire à votre enfant de les utiliser ne résoudra probablement pas le problème, car il trouvera certainement le moyen de contourner cette interdiction. Vous trouverez ci-dessous des conseils qui rendront l'utilisation des réseaux sociaux plus sûre et assureront une protection adéquate de vos enfants et de votre famille.

Discutez

Le dialogue est l'un des éléments les plus importants pour assurer la sécurité de vos enfants en ligne, surtout lorsqu'il s'agit des réseaux sociaux. Il est essentiel de maintenir une communication ouverte et honnête avec vos enfants si vous voulez qu'ils aient confiance en votre jugement et suivent vos conseils.

La prévention du cyberharcèlement en est un bon exemple. Faites comprendre à votre enfant qu'un tel comportement, même s'il ne le concerne pas directement, doit être immédiatement signalé à quelqu'un : vous, un enseignant ou d'autres adultes responsables.

Utilisez un logiciel de contrôle parental

Utilisez un logiciel de contrôle parental adapté à l'âge de vos enfants. ESET Smart Security vous permet de définir une liste de sites web bloqués et de sélectionner les horaires pendant lesquels vos enfants peuvent passer du temps en ligne.

Les enfants devraient également avoir leur mot à dire. C'est pourquoi ESET Parental Control for Android leur permet de vous demander la permission de consulter des sites web spécifiques ou d'obtenir du temps supplémentaire sur les réseaux sociaux, par exemple s'ils ont terminé leurs tâches ou leurs devoirs plus tôt que prévu.

Utilisez une solution de sécurité fiable

Les malwares étant l'une des menaces les plus répandues dans le cyberespace, l'installation d'une solution de sécurité dotée de fonctionnalités de détection proactive sur les appareils de votre enfant est essentielle pour éviter les infections lors de l'utilisation des réseaux sociaux.

L'antispam et le pare-feu permettent également de renforcer la sécurité du système face à ces risques. De même, votre enfant ne doit jamais utiliser un compte administrateur pour surfer sur les réseaux sociaux. Créez un profil utilisateur spécial pour vos enfants afin de minimiser l'impact des incidents de sécurité.

Utilisez des mots de passe robustes et l'authentification à deux facteurs

Est-ce que vos enfants savent à quoi ressemble un mot de passe solide ? Assurez-vous qu'ils n'utilisent pas de mots de passe faciles à deviner tels que leur prénom ou « 12345 ». Ils doivent comporter au moins 10 caractères, des majuscules et des minuscules, un chiffre et un caractère spécial comme # ou @. Adaptez par exemple une phrase ou les paroles d'une chanson :

Au clair de la lune devient @uclairde1aLune

Rappelez-leur également de ne pas communiquer leurs mots de passe à quiconque, pas même avec leurs meilleurs amis.

Si vous vous connectez à Facebook, Twitter ou d'autres réseaux sociaux populaires, veillez à ce que vos enfants utilisent l'authentification à deux facteurs proposés dans les paramètres de sécurité. Le fait de recevoir un code d'accès à usage unique sur leur smartphone ajoute une autre couche de sécurité difficile à pirater.

Passez le profil en mode « privé »

Les paramètres de confidentialité par défaut des réseaux sociaux ne garantissent pas la sécurité de votre enfant. Il est donc conseillé de consacrer un peu de temps à les configurer et à rechercher les informations susceptibles d'être divulguées. Prenons l'exemple de Facebook :

Facebook

Paramétrez le profil afin de vous assurer que rien ne soit partagé avec tous les utilisateurs. De préférence, ne partagez des informations qu'avec les amis et la famille et, si possible, qu'avec de petits groupes (tels que la famille proche ou les meilleurs amis).

Limitez le public autorisé à consulter les photos, publications et autres contenus dans lesquels votre enfant a été tagué. Empêchez les applications d'accéder à leurs informations personnelles ou de publier sur leur mur.

Apprenez-leur à n'accepter que les demandes de connexion de personnes qu'ils connaissent personnellement. Faites-leur comprendre que parler à des inconnus ou être contacté sur Internet peut s'avérer aussi dangereux qu'une rencontre dans le monde réel.

Pour des informations détaillées sur l'utilisation des paramètres de Facebook, veuillez lire notre article https://www.welivesecurity.com/fr/2020/02/05/facebook-parametres-confidentialite/

Twitter

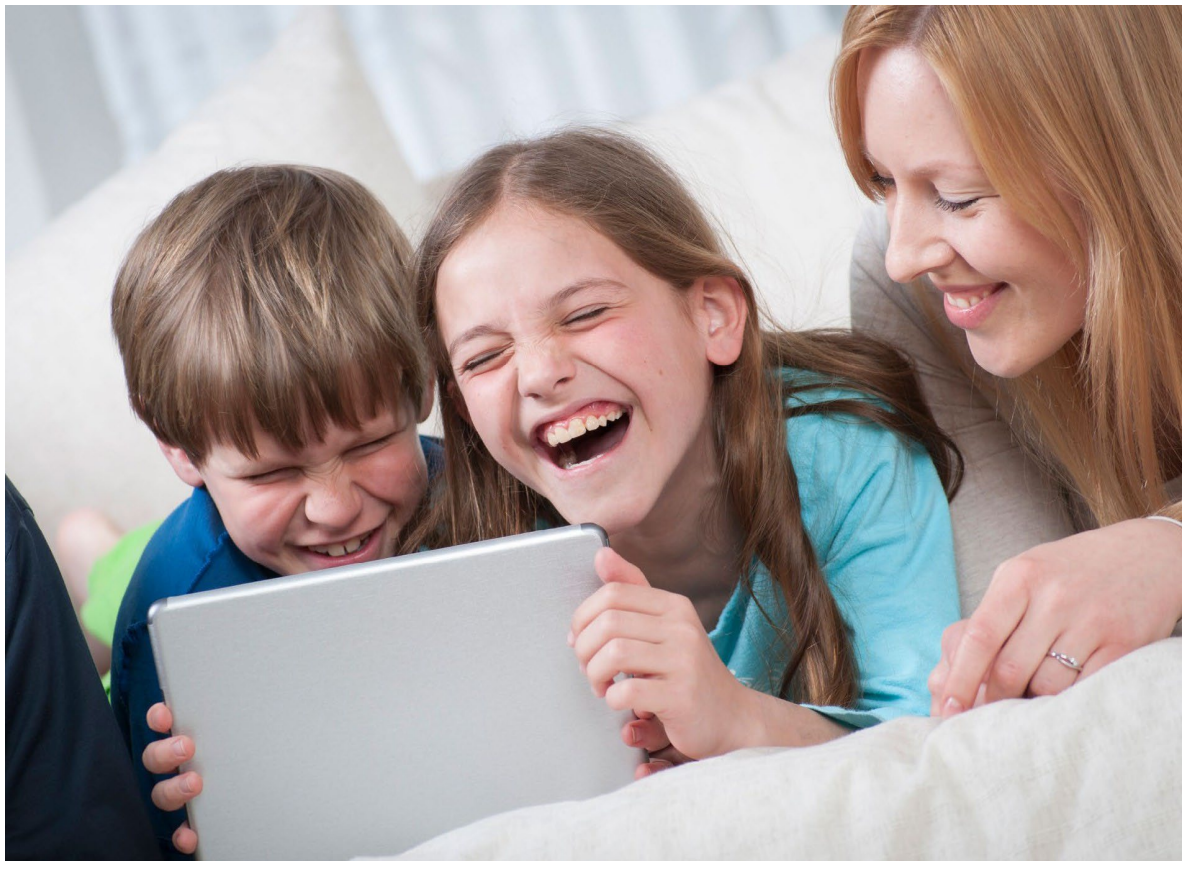
Twitter possède ses propres caractéristiques, notamment la limite de 280 caractères ou l'utilisation fréquente d'URL raccourcies. Ce sont des différences que vous devez également aborder lorsque vous expliquez à votre enfant comment assurer sa sécurité.

En plus de ne suivre que les personnes qu'ils connaissent et d'éviter les liens suspects, ils doivent également vérifier la légitimité de tout message qu'ils peuvent recevoir. Les messages malveillants sont souvent identifiés par les autres utilisateurs et les informations communiquées. La recherche rapide d'une partie du message peut donc souvent être utile.

Installez également sur leur ordinateur ou leur appareil un plug-in de bonne réputation pour navigateur, qui permet à vos enfants de voir le lien d'origine d'une adresse URL écourtée sans avoir à cliquer dessus.

Autres réseaux sociaux

Il existe de nombreux réseaux sociaux répondant à différents centres d'intérêt et groupes d'âge. Il est important de vérifier que vos enfants utilisent ceux qui leur conviennent. Nous disposons de guides vidéo sur Snapchat, Instagram et YouTube, et avons également dressé une liste des réseaux sociaux appropriés pour les enfants.



3. Conclusion

Les réseaux sociaux peuvent constituer une ressource précieuse pour les internautes. Pourtant, comme le montre ce guide, il existe de nombreuses menaces auxquelles les enfants peuvent être exposés lorsqu'ils utilisent les réseaux sociaux. Ne sous-estimez pas les cybercriminels et les autres acteurs malveillants. Il est essentiel de mettre en œuvre de bonnes pratiques et d'utiliser des outils de sécurité fiables pour protéger les personnes importantes de votre vie.

Les aider à configurer correctement leur profil sur les réseaux sociaux et leur offrir des conseils simples mais utiles pourrait être la chose décisive à faire pour assurer leur sécurité.

10 conseils utiles

1. Apprenez à vos enfants à prendre du recul et à réfléchir avant de cliquer sur les liens et les boutons de téléchargement
2. Apprenez-leur à aborder la communication en ligne avec beaucoup de prudence
3. Mettez les comptes de vos enfants en mode privé
4. Apprenez-leur à refuser les demandes de connexion provenant d'inconnus
5. Maintenez leur système d'exploitation et leur logiciel de sécurité à jour
6. Soyez un bon modèle et contrôlez également vos activités en ligne
7. Soyez à l'affût de tout signe qui pourraient indiquer qu'un enfant est victime de cyberharcèlement
8. Utilisez une application de contrôle parental réputée comme ESET Parental Control
9. Encouragez-les à utiliser des mots de passe robustes
10. Demandez-leur de réfléchir avant de communiquer des informations, des vidéos ou des photos personnelles.