

Guide parental en matière de sites de réseau social

Un nombre croissant d'enfants passent un temps considérable sur des sites tels que Facebook et MySpace. Ce sont là deux des sites de réseau social les plus populaires permettant aux jeunes internautes de rester en contact avec leurs amis. Hélas, ceux-ci y dévoilent trop souvent des informations personnelles, une situation qui peut parfois les mettre en danger.

Ce guide a pour but de vous aider à gérer les problèmes associés à l'utilisation des sites web communautaires et de réseau social. Les recommandations fournies vous permettront de mieux assurer la sécurité de vos enfants en ligne.

Cinq leçons à l'intention des parents ayant des enfants et adolescents membres de sites de réseau social

Leçon 1

Définition d'un site de réseau social

Un réseau social est un site web qui propose une communauté virtuelle aux utilisateurs intéressés par un sujet particulier ou simplement désireux de communiquer entre eux. Les enfants et les adolescents adorent ce type de sites car ils les utilisent comme plates-formes pour discuter en ligne avec la famille et les amis ou encore pour échanger des e-mails et des photos.

- Parlez avec vos enfants de leurs activités en ligne.
- Créez votre propre profil Facebook ou page MySpace avec l'aide de vos enfants.
- Informez-vous des avantages et des dangers des réseaux sociaux, par exemple via le site McAfee® Security Advice Center.

Leçon 2

Risques associés aux réseaux sociaux

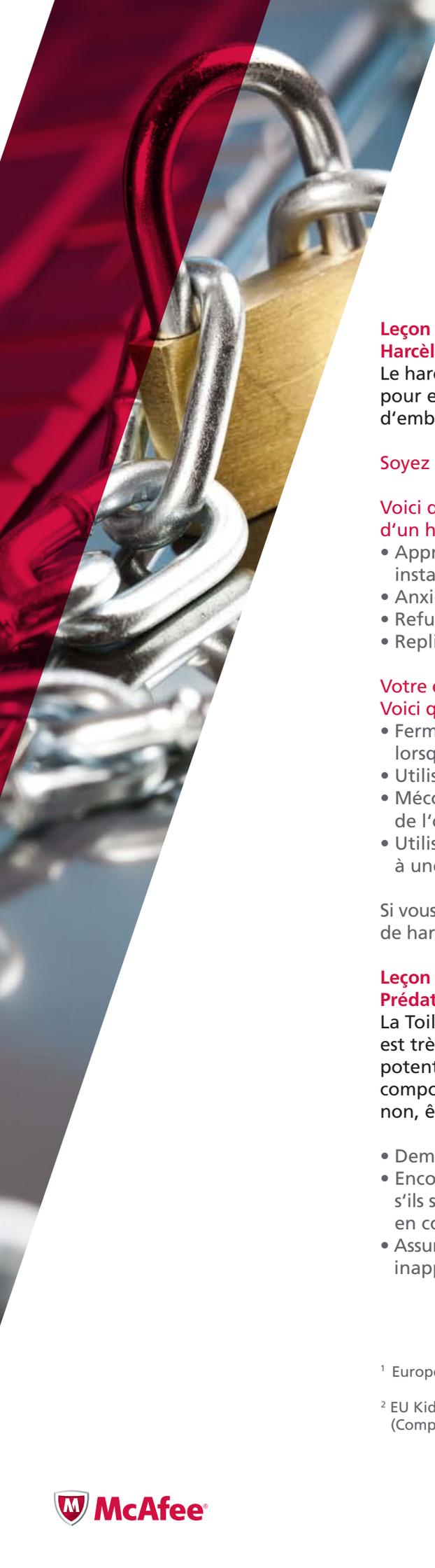
Le problème majeur de ce type de sites est l'excès d'informations que les internautes y dévoilent. Vos enfants doivent comprendre qu'en communiquant trop d'informations sur eux-mêmes et leur vie privée, ils se mettent en danger.

- Définissez des limites et des règles en matière de comportement en ligne.
- Limitez le temps que vos enfants sont autorisés à passer sur Internet.
- Discutez du contenu qui peut, ou non, être partagé en ligne.
- Recommandez à vos enfants d'être prudents lorsque des inconnus souhaitent rejoindre leur réseau.
- Défendez-leur de rencontrer en personne les internautes connus en ligne.
- Encouragez-les à vous informer s'ils remarquent un événement ou comportement inhabituel ou s'ils ressentent une appréhension ou crainte quelconque.
- Apprenez-leur à se méfier des e-mails contenant des questions, des offres ou des liens vers d'autres sites web.

QUELQUES FAITS EDIFIANTS SUR LES SITES DE RESEAU SOCIAL

67 % des adolescents européens passent une grande partie de leur temps sur des sites de réseau social.¹

La divulgation d'informations personnelles constitue le risque le plus fréquemment encouru par les adolescents européens.²



Leçon 3

Harcèlement en ligne

Le harcèlement en ligne consiste à utiliser Internet ou d'autres technologies pour envoyer ou publier du texte ou des images dans le but de blesser ou d'embarrasser une autre personne.

Soyez vigilant face à ce problème et parlez-en avec vos enfants.

Voici quelques indices susceptibles d'indiquer que votre enfant est victime d'un harcèlement en ligne :

- Appréhension de l'enfant lorsqu'il reçoit un e-mail, un message instantané ou un texto
- Anxiété après avoir utilisé l'ordinateur
- Refus de quitter la maison ou d'aller à l'école
- Repli sur soi

Votre enfant peut lui-même se livrer à des activités de harcèlement en ligne.

Voici quelques signes susceptibles de vous indiquer un tel comportement :

- Fermeture de programmes ou basculement vers une autre fenêtre lorsque vous passez à proximité de l'ordinateur
- Utilisation de l'ordinateur à une heure avancée de la nuit
- Mécontentement ou colère en cas d'interdiction d'utilisation de l'ordinateur
- Utilisation de plusieurs comptes en ligne ou d'un compte appartenant à une autre personne

Si vous remarquez certains de ces signes, parlez avec vos enfants du problème de harcèlement en ligne, tant du point de vue de la victime que de l'auteur.

Leçon 4

Prédateurs en ligne

La Toile est un lieu de prédilection pour les prédateurs en ligne car il leur est très facile de dissimuler leur identité et d'avoir accès à des victimes potentielles. Il est donc capital que vos enfants et vous-même discutiez du comportement en ligne à respecter et des informations qui peuvent, ou non, être publiées en ligne.

- Demandez à vos enfants de vous informer de tout événement inhabituel.
- Encouragez-les à se confier à vous ou à une autre personne de confiance s'ils sont victimes de harcèlement en ligne ou si des prédateurs sont entrés en contact avec eux.
- Assurez-vous qu'ils savent comment signaler les abus ou les comportements inappropriés sur les sites de réseau social.

¹ European Online Safety Study (Etude sur la sécurité en ligne en Europe) — Cross Tab Media

² EU Kids Online, Comparing Children's Online Opportunities and Risks Across Europe (Comparaison des opportunités et risques en ligne des enfants en Europe), juin 2008



Leçon 5

Atteinte à la vie privée, usurpation malveillante ou vol d'informations d'identité

Il est essentiel que vos enfants restent prudents quant aux informations qu'ils divulguent et aux personnes à qui ils les communiquent. Ils doivent impérativement comprendre qu'aucune donnée n'est privée lorsqu'elle est publiée en ligne. Les sites de réseau social offrent aux pirates une mine d'informations de nature privée. Les arnaqueurs utilisent souvent des fausses demandes émanant en apparence de sources légitimes pour obtenir des mots de passe, des numéros de téléphone ou des informations de carte de crédit.

- Encouragez vos enfants à faire preuve de bon sens.
- Discutez avec eux et établissez certaines limites.
- Vérifiez que personne n'usurpe l'identité de votre enfant.
- Créez votre propre profil et participez aux interactions de vos enfants sur les sites de réseau social.
- Utilisez les options de configuration de la sécurité et de la confidentialité de ces sites, notamment les profils privés, le blocage et l'approbation préalable des commentaires.
- Assurez-vous que votre logiciel de sécurité est à jour.
- Envisagez l'installation d'un logiciel qui vous permette de surveiller les activités en ligne de votre enfant et de mieux le protéger.

Informations essentielles

Que faire si votre enfant est victime d'une quelconque manipulation en ligne ?

- Ignorer le prédateur en ligne et ne plus se connecter au site web sur lequel l'incident s'est produit.
- Bloquer le nom d'utilisateur du responsable du délit ainsi que son adresse e-mail.
- Modifier les informations de votre enfant apparaissant en ligne ou, si besoin est, supprimer son compte.
- Contacter le site web sur lequel l'incident s'est produit et, le cas échéant, demander la suppression de toutes les données de votre enfant.
- Signaler l'incident à votre fournisseur d'accès Internet (FAI) et à celui de l'auteur du délit.
- Signaler l'incident aux autorités.
- Conserver un journal de toutes les communications émanant de l'auteur du délit ou de l'abus.
- Prendre note de son nom d'utilisateur, de son adresse e-mail et, le cas échéant, de son fournisseur d'accès Internet.



McAfee® Family Protection protège vos enfants contre le contenu inapproprié, les risques posés par les sites de réseau social et d'autres menaces Internet. Il vous permet en outre de surveiller les activités en ligne de vos enfants.



Pour en savoir plus, consultez le document «Un guide parental pour sites d'interaction sociale».

Téléchargez le guide électronique à l'adresse www.mcafee.com/advice.



McAfee
Tour Franklin, La Défense 8
Paris La Défense Cdx 92042
France
<http://service.mcafee.com>

McAfee et/ou les produits McAfee cités dans le présent document sont des marques déposées ou des marques de McAfee, Inc., et/ou de ses affiliés aux Etats-Unis et/ou dans d'autres pays. McAfee Red pour ce qui est de la sécurité est distinct des produits de la marque McAfee. Tout produit autre que McAfee, toute marque déposée et/ou non déposée mentionnés dans le présent document sont cités uniquement par référence et sont la propriété exclusive de leurs propriétaires respectifs. © 2009 McAfee, Inc. Tous droits réservés.