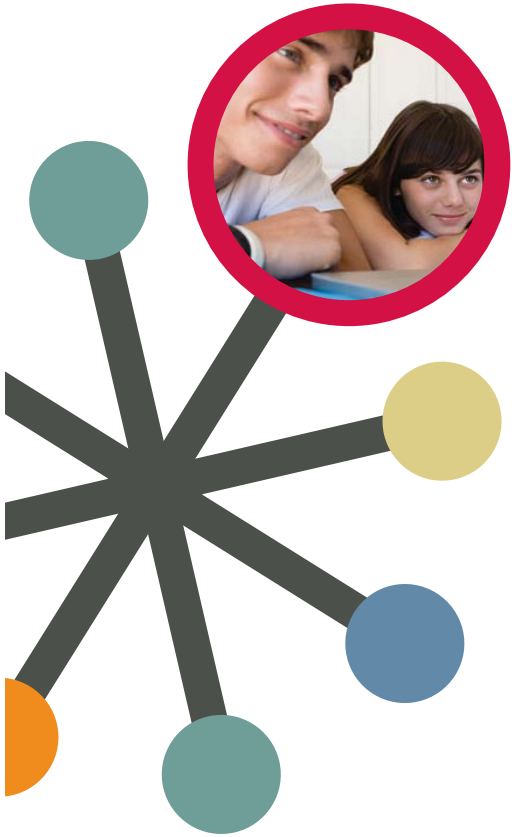
McAFEE - PLAN DE SÉCURITÉ INTERNET POUR VOTRE FAMILLE EN 10 ÉTAPES

Comment parler de la sécurité en ligne aux enfants, adolescents et novices de tout âge

McAfee

TABLE DES MATIÈRES



INTRODUCTION

Dans le monde entier, des millions de familles utilisent Internet chaque jour pour apprendre, chercher, faire des courses, acheter, gérer un compte en banque, investir, partager des photos, jouer, télécharger des films et de le musique, contacter des amis, faire des rencontres et participer à une multitude d'activités. Bien que le cyberespace offre de nombreux avantages, opportunités et facilités, il présente également des risques croissants et de nombreuses nouvelles menaces apparaissent chaque jour.

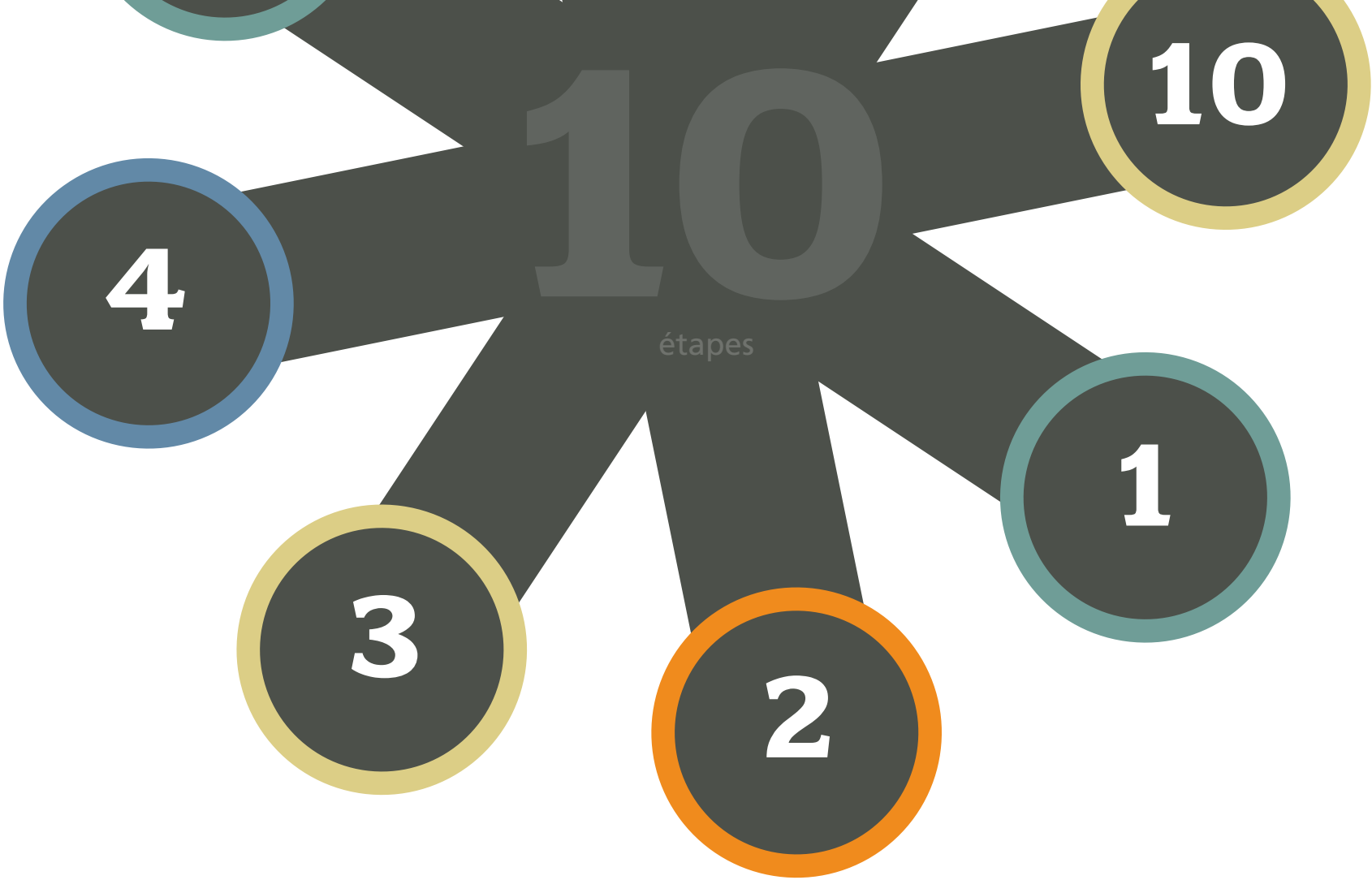
Il n'est guère surprenant que les cyber criminels profitent d'Internet et des gens qui l'utilisent. Vous-même et les membres de votre famille devez être sur vos gardes quand vous passez du temps en ligne. En plus d'installer un robuste logiciel de sécurité d'une compagnie réputée pour défendre votre famille contre les pirates, les usurpateurs d'identité, les escrocs de messagerie et autres prédateurs, vous devez suivre quelques règles élémentaires de sécurité sur Internet, sans oublier votre simple bon sens du monde réel. Il vous faut un plan de sécurité Internet pour votre famille.

Dès qu'un membre de la famille devient actif en ligne, il faut l'éduquer sur la cyber sécurité, quel que soit son âge. Vous devez être conscient que même si vous n'avez pas d'ordinateur à la maison, des PC sont disponibles pratiquement partout : à l'école, à la bibliothèque, chez des amis, etc. Il est important pour chacun de posséder des notions de base sur la protection contre les dangers du cyber espace.

INTERNET AUJOURD'HUI :
procédez avec prudence

- Vos chances d'être victime d'un cybercrime sont d'environ 1 sur 4[1]
- Les pirates attaquent les PC par leur liaison Internet toutes les 39 secondes[2]
- Selon McAfee® Avert® Labs, il y a actuellement 222 000 virus informatiques dans la nature, et le nombre de menaces augmente chaque jour
- Des infections virales ont amené 1,8 million de foyers à remplacer leurs PC au cours des deux dernières années[3]
- En 2006, 8,9 millions d'américains ont été victimes de détournements d'identité[4]
- 71% des adolescents de 13 à 17 ans ont reçu des messages en ligne de la part de quelqu'un qu'ils ne connaissaient pas[5]

1 Consumer Reports, State of the Net 2007, septembre 2007
2 Hackers Attack Every 39 Seconds – James Clark École d'ingénierie James Clark de l'université du Maryland
3 Consumer Reports, State of the Net 2007, septembre 2007
4 2006 Identity Fraud Survey Consumer Report, Javelin Strategy & Research
5 "Teen Safety Search," Cox Communications and Teen Research Unlimited, Mars 2006



Plan de sécurité en 10 étapes pour protéger toute votre famille

étape 1

EMPLACEMENT DE L'ORDINATEUR

Dans une maison où habitent des enfants, l'emplacement de l'ordinateur familial est l'un des choix les plus importants que vous ayez à faire. Nous vous recommandons d'installer l'ordinateur à un endroit très fréquenté par la famille et que vous limitiez le nombre d'heures que vos enfants passent sur l'ordinateur. Veillez à ce qu'un logiciel de sécurité soit installé sur l'ordinateur et comporte un contrôle parental comme ceux présents dans les produits McAfee.

étape 2

TRAVAILLEZ EN ÉQUIPE
pour définir des limites

Définissez ensemble ce qui est acceptable et ce qui ne l'est pas en ce qui concerne :

- Le genre de sites Web qu'il est acceptable de visiter.
- Les salles de discussions et les forums auxquels il est autorisé de participer :
  - N'utilisez que les salles de discussions surveillées.
  - Veillez à ce que vos enfants évitent les salles de discussions « .alt » , qui sont orientées sur des sujets alternatifs éventuellement peu appropriés à un jeune public.
- Le genre de sujets de discussion auxquels vos enfants peuvent participer en ligne et le genre de langage qui serait considéré déplacé.

étape 3

TROUVEZ UN ACCORD ENSEMBLE AUTOUR DES

règles d'utilisation du PC familial

Nous recommandons de prendre les précautions suivantes :

- Ne vous connectez jamais sous un nom d'utilisateur qui révèle votre vraie identité ou se montre provocateur.
- Ne révélez jamais vos mots de passe.
- Ne révélez jamais vos numéros de téléphone ou adresses.
- Ne publiez jamais d'informations qui révèlent votre identité.
- Ne publiez jamais de photos déplacées ou révélant votre identité (par exemple T-shirt portant un nom de ville ou d'école).
- Ne partagez jamais d'informations avec des étrangers rencontrés en ligne.
- Ne rencontrez jamais physiquement d'étrangers rencontrés en ligne.
- N'ouvrez jamais de pièce jointe provenant d'un étranger.

Lorsque vous aurez établi les règles, imprimez-les sur une affichette que vous placerez à côté de l'ordinateur.

étape 4

SIGNEZ UN ACCORD
portant sur un comportement en ligne acceptable

Rédigez un accord ou utilisez celui de la page suivante, afin qu'il existe une bonne compréhension entre tous les membres de la famille au sujet de l'utilisation de l'ordinateur et du comportement approprié en ligne.

DÉCLARATION SUR LA SÉCURITÉ EN LIGNE

L'utilisation de l'ordinateur et d'Internet est un privilège que je ne veux pas perdre. Pour cette raison,

- Je veillerai à la sécurité chaque fois que je serai en ligne pour surfer, chercher, travailler, jouer ou discuter.
- J'observerai toutes les règles sur lesquelles nous sommes d'accord.
- Je ne révèlerai pas mon nom, mon numéro de téléphone, mon adresse ou mes mots de passe à des « amis » en ligne.
- Je ne rencontrerai jamais physiquement des personnes que j'aurai rencontrées en ligne.
- Si je me trouve dans une situation en ligne où je ne me sens pas en sécurité ou pas à l'aise, je promets de vous en avertir (parents/tuteur/professeur) afin que vous puissiez m'aider.
- Je m'engage à respecter cet accord, et je sais que toutes mes actions ont des conséquences.

Signature de l'enfant _____

- En tant que parent/tuteur/professeur, je promets de me mettre à ta disposition lorsque tu me demanderas de l'aide et de t'aider à résoudre tout problème qui pourrait survenir du mieux que je pourrai.

Signature du parent/tuteur/professeur _____

étape 5

INSTALLEZ LE LOGICIEL DE SÉCURITÉ

Veillez à ce qu'un logiciel de sécurité efficace protège votre ordinateur contre les virus, les pirates et les logiciels espions. Il doit également filtrer les contenus, images et sites Web offensants.
Ce logiciel doit être fréquemment actualisé, car de nouvelles menaces apparaissent chaque jour. Idéalement, une sécurité qui se met à jour automatiquement – comme le logiciel McAfee à « installer et oublier » – constitue le meilleur choix.

étape 6

UTILISEZ LE CONTRÔLE PARENTAL

Tous les grands fournisseurs de logiciels de sécurité proposent un contrôle parental. Veillez à actualiser la fonctionnalité. Si vous utilisez un logiciel gratuit ou dépourvu de contrôle parental, envisagez d'acheter un logiciel possédant cette fonctionnalité. Prenez le temps de comprendre le fonctionnement de ce contrôle et utilisez les options destinées à filtrer et bloquez les contenus non appropriés. Naturellement, ces outils ont leurs limitations. Rien ne peut se substituer à des parents attentifs et présents pour suivre les activités en ligne de leurs enfants.

étape 7

RAPPELEZ AUX MEMBRES DE LA FAMILLE QUE

les personnes rencontrées en ligne sont des étrangers

Toute personne allant en ligne doit comprendre que :

Quel que soit le nombre de fois où vous bavardez avec des « amis » en ligne et le temps passé ensemble, même si vous croyez bien les connaître, les personnes rencontrées en ligne sont des étrangers. Il est facile de mentir et de prétendre être quelqu'un d'autre en ligne. Les jeunes enfants doivent savoir qu'un « ami » peut être en réalité un homme de 40 ans et non quelqu'un de leur âge.

Les sites Web d'interaction sociale comme www.MySpace.com et www.Facebook.com constituent une excellente approche pour rencontrer des gens en ligne. Toutefois, les parents doivent visiter ces sites et vérifier le profil défini pour leurs enfants afin d'éviter que des conversations déplacées n'interviennent ou que des photos inacceptables ne soient publiées. Les parents doivent surveiller les conversations de leurs enfants dans les messageries instantanées pour éviter qu'ils ne soient inquiétés par des prédateurs en ligne.

étape 8

CRÉEZ DES MOTS DE PASSE SOLIDES

Pour créer des mots de passe difficiles à découvrir, utilisez au minimum 8 caractères avec une combinaison de lettre, de chiffres et de symboles. Les mots de passe doivent être modifiés périodiquement pour réduire le risque qu'un mot de passe spécifique ne soit compromis à long terme.

Techniques pour créer des mots de passe solides

- Utilisez un système « phonétique » : « LeSs6vAFeR »
- Utilisez plusieurs petits mots séparés par des ponctuations : « betty,boop$chat »
- Insérez une ponctuation au milieu d'un mot : « Roos%velt »
- Utilisez une abréviation inhabituelle : « anticstitnel »
- Utilisez la première lettre de chaque mot d'une phrase, avec un chiffre aléatoire : « difficile de trouver ce mot de passe » = « ddtc5mdp »
- Ne révélez jamais vos mots de passe !

étape 9

VÉRIFIEZ LE LOGICIEL DE SÉCURITÉ DE VOTRE ORDINATEUR

Ouvrez le logiciel de sécurité que vous utilisez et vérifiez que votre ordinateur bénéficie des trois protections essentielles suivantes : antivirus, antispyware et pare-feu.

Ces protections de base doivent être complétées par un logiciel antispam et de recherche sécurisée comme McAfee SiteAdvisor®, qui comporte une protection antiphishing et des évaluations de sécurité. Une excellente idée pour les familles consiste à installer sur les PC une suite logicielle de protection incluant des outils de contrôle parental et contre le détournement d'identité.

étape 10

RESTEZ INFORMÉ

Plus vous en savez, plus vous êtes en sécurité. Consultez McAfee's Security Advice Center. Des matériaux pédagogiques faciles à lire sur la sécurité informatique et Internet sont disponibles à l'adresse www.mcafee.com/advice.

Le B A BA de La Sécurité en Ligne
POUR LES JEUNES ENFANTS

3 à 7 ans

JEUNES ENFANTS

10

étapes

A Parler aux jeunes enfants

Lorsque vous parlez de la sécurité sur Internet à de jeunes enfants, faites-le avec l'ordinateur éteint pour avoir toute leur attention. Commencez par leur expliquer qu'un ordinateur est un outil et qu'Internet est comme une immense bibliothèque électronique remplie d'informations.

Expliquez qu'il est important de veiller à la sécurité en ligne, parce que l'ordinateur peut être utilisé comme une porte ouverte vers vos informations confidentielles importantes. Parlez-leur des personnes malveillantes qui peuvent prendre le contrôle de votre ordinateur et le casser, ce qui vous obligera à en acheter un autre.

Expliquez-leur pourquoi il est important de ne pas communiquer d'informations à quelqu'un en ligne. Dites-leur de ne pas utiliser leur vrai nom et de ne pas parler de l'endroit où ils habitent ni de leur école.

B Créez une liste de règles spéciales pour l'ordinateur utilisé par de jeunes enfants

Cette liste doit inclure les instructions suivantes :

- Ne pas télécharger de musique ou de fichiers de programme sans l'autorisation des parents.
- N'utiliser que les salles de discussion comme Disney Virtual Magic Kingdom, où un adulte supervise réellement les discussions.
- Ne jamais envoyer de photographie de soi-même sans en parler d'abord aux parents.
- Ne pas utiliser un langage grossier.

- Ne pas visiter les sites Web pour adultes.
- Ne partager des informations qu'avec des personnes connues dans le monde réel, comme des camarades de classe, des amis et des membres de la famille.
- Ne pas remplir de formulaires en ligne ou d'enquêtes sans l'aide d'un parent.
- N'utiliser que les moteurs de recherche spéciaux pour les enfants, comme Ask for Kids et Yahoo! Kids.

C Utilisez des navigateurs et des moteurs de recherche spécialement conçus pour les enfants

Vérifiez que vos enfants utilisent des navigateurs qui n'affichent pas de termes ou d'images inadaptés. Vérifiez que ces navigateurs sont préchargés avec des sites Web sûrs et des filtres terminologiques préconfigurés. Il vous suffit de parcourir et d'approuver les sites Web et termes par défaut.

Le B A BA de La Sécurité en Ligne
POUR LES ENFANTS

8 à 12 ans

ENFANTS

10

étapes

A Parler aux enfants

Les enfants dont l'âge est compris entre huit et douze ans sont beaucoup plus évolués qu'auparavant. Cette population est désignée « Tweens » pour signifier qu'il ne s'agit plus de jeunes enfants mais pas encore d'adolescents (teenagers). Il faut comprendre que les Tweens sont très à l'aise avec un ordinateur, car ils ont grandi à côté d'un PC à la maison ou à l'école.

Avant de parler à des enfants de cet âge, vous devez prendre quelques décisions pour définir des limites autour de leur utilisation d'Internet. Pour communiquer clairement sur les règles, vous devez d'abord définir celles-ci. Pour protéger vos enfants, vous devez connaître la réponse aux questions suivantes :

- L'ordinateur est-il installé dans une zone commune de la maison ?
- Quels sites Web sont sûrs pour vos enfants ?
- Combien de temps les sessions peuvent-elles durer ?
- Que peuvent-ils faire pendant qu'ils sont en ligne ?
- Avec qui sont-ils autorisés à communiquer ?
- Si vous ne prévoyez pas de surveiller vos enfants, quand doivent-ils demander votre aide et votre accord ?

Lorsque vous connaissez la réponse à ces questions, vous pouvez menez la conversation. Avec l'ordinateur éteint pour avoir toute l'attention de vos enfants, expliquez qu'un ordinateur est un outil et qu'il est important de veiller à la sécurité en ligne.

Veillez à traiter les points suivants :

- Parlez des antivirus, des antispyware et des pirates.
- Parlez des prédateurs qui tentent de faire parler les enfants sur eux-mêmes.
- Expliquez qu'il est important de veiller à la sécurité en ligne, parce que l'ordinateur peut être utilisé comme une porte ouverte vers vos informations confidentielles importantes.
- Expliquez comment le détournement d'identité se produit.
- Indiquez que vous-même ou un expert (si vous n'en êtes pas un) pouvez détecter absolument tout ce qui est fait sur votre ordinateur.
- Expliquez comment des criminels peuvent prendre le contrôle de votre PC et le casser, ce qui vous obligera à en acheter un autre.

Demander de l'aide s'il se passe quelque chose de spécial

Insistez sur le fait que vos enfants doivent vous prévenir s'ils reçoivent des messages étranges ou dérangeants pendant qu'ils discutent, que vous ne serez pas fâché avec eux pour cela et qu'ils ne seront pas privés d'Internet pour cela. Expliquez clairement à vos enfants que vous comprenez qu'ils ne peuvent pas contrôler ce que d'autres personnes leur disent et qu'ils ne sont pas à blâmer.

Vérifiez également que votre enfant n'est pas brimé et ne brime pas d'autres enfants en ligne. Lorsque des élèves quittent l'école, ils ne laissent pas forcément leurs condisciples et leurs conflits derrière eux. Ils peuvent maintenir le contact en permanence avec un ordinateur ou un téléphone et abuser de ces technologies pour importuner ou persécuter d'autres enfants.

C Comment bloquer des utilisateurs et signaler des problèmes

Vous pouvez enregistrer des sessions en copiant et en collant le message texte dans un programme de traitement de texte. La plupart des programmes de discussion permettent de bloquer un utilisateur en cliquant sur leur nom dans votre liste de contacts avec le bouton droit de la souris et en choisissant l'option « Bloquer » ou « Ignorer ». Si votre enfant subit un incident en ligne avec l'individu, envoyez le rapport copié au modérateur de la salle de discussion ou à l'administrateur. Les informations de contact sont disponibles dans l'aide ou dans la section Rapport du programme.

Le B A BA de La Sécurité en Ligne
POUR LES ADOLESCENTS

13 à 19 ans

ADOLES-
CENTS

10

étapes

A Parler aux adolescents

Tout comme il faut enseigner aux adolescents la sécurité routière avant de les laisser conduire, vous devez leur apprendre la sécurité Internet avant de les laisser surfer sans surveillance.

Une différence essentielle entre la conduire d'une voiture et Internet est qu'il n'y pas de vrai « code de la route » sur Internet. Cela en fait un véhicule à la fois très puissant et très dangereux. Pour éviter les blocages de l'ordinateur ou pire, vous devez donc définir ce code vous-même et l'imposer. L'objectif ici est d'enseigner aux adolescents le bon sens qui les tiendra à l'écart des dangers en ligne.

Expliquez à vos adolescents pourquoi il est important de veiller à la sécurité en ligne. Veillez à traiter les points suivants :

- Parlez des virus, des logiciels espions et des pirates, ainsi que de la manière dont ils opèrent.
- Parlez des prédateurs qui tentent de faire parler les enfants sur eux-mêmes.
- Expliquez qu'il est important de veiller à la sécurité en ligne, parce que l'ordinateur peut être utilisé comme une porte ouverte vers vos informations confidentielles importantes.
- Expliquez comment le détournement d'identité se produit.
- Indiquez que vous-même ou un expert (si vous n'en êtes pas un) pouvez détecter absolument tout ce qui est fait sur votre ordinateur.
- Expliquez comment des criminels peuvent prendre le contrôle de votre PC et le casser, ce qui vous obligera à en acheter un autre.

B Rappelez à vos adolescents que les personnes rencontrées en ligne sont des étrangers

Quel que soit le nombre de fois où ils bavardent avec des personnes en ligne et le temps passé ensemble, les personnes que vos adolescents rencontrent en ligne sont des étrangers. Les gens peuvent mentir sur leur compte et le nouvel « ami » de vos adolescents peut être en réalité un homme de 40 ans et pas quelqu'un de leur âge.

C Vérifiez le profil de vos adolescents sur les sites Web d'interaction sociale

Vérifiez que vos adolescents ne publient pas trop d'informations sur eux-mêmes sur MySpace.com ou Facebook. Vérifiez que les photographies qu'ils publient ne sont pas provocantes. Rappelez-leur qu'ils risquent d'attirer l'intérêt de prédateurs en ligne, d'embarrasser leurs amis et leur famille ou d'influencer négativement un futur employeur.

Le B A BA de La Sécurité en Ligne
POUR LES NOVICES

Tout âge

NOVICES

10

étapes

Votre conjoint, votre partenaire, vos parents ou vos grands-parents peuvent être novices dans l'utilisation de leur ordinateur et d'Internet. Ils sont peut-être moins expérimentés que vous ne le pensez et risquent d'être victimes d'escroqueries en ligne et d'attaques Internet. Il leur faut donc un peu d'aide de votre part. Votre discussion sur la sécurité Web doit couvrir les rubriques suivantes :

A

Virus, logiciels espions et pirates

Si nécessaire, la définition de ces termes est disponible dans un glossaire en ligne sur www.McAfee.com/advice.

B

Détournement d'identité et phishing

Phishing : des criminels interrogent le site Web et la messagerie d'une société légitime pour tenter de voler des mots de passe et des numéros de carte de crédit. Cela peut être une bonne idée de s'abonner à un service de contrôle de carte de crédit. Veillez à contrôler fréquemment vos relevés de compte bancaire et de carte de crédit.

C

L'importance d'être prudent en téléchargeant des produits « gratuits »

Rappelez à vos proches que tout a un prix, même ce qui est gratuit ! Avertissez-les également que s'ils téléchargent des logiciels, ils risquent de récupérer des logiciels publicitaires et espions en même temps que l'application.

Autres informations sur la Sécurité PC et Internet

Pour en savoir plus sur la protection en ligne, visitez McAfee Security Advice Center à l'adresse http://www.mcafee.com/advice.

À propos de McAfee

McAfee, Inc., leader sur le marché des technologies de sécurité, est basée à Santa Clara, Californie. La société fournit des solutions et des services éprouvés pour sécuriser les systèmes et les réseaux à travers le monde. Forte de son expertise inégalée et de sa volonté d'innovation, McAfee® apporte aux particuliers, aux entreprises, au secteur public et aux fournisseurs de services la possibilité de bloquer les attaques, d'éviter les interruptions et de contrôler et améliorer en permanence leur sécurité.

http://www.mcafee.com