Guide de sécurité de la cyberfamille

Un guide pratique pour vous aider à assurer la sécurité de votre cyberfamille

Par Anne-Sophie Clémot

Norton™ from symantec

Internet est un lieu riche et merveilleux, où les sources et ressources en information sont abondantes, où les occasions de rencontrer de nouveaux amis et de bâtir des communautés en ligne sont nombreuses. Pourtant, pour beaucoup de parents ou d'adultes en général, qui ont souvent moins de connaissance et d'expérience de ce nouveau media, Internet peut être une source d'inquiétude. Nous nous soucions de ce que nos enfants peuvent voir en ligne, des rencontres qu'ils peuvent faire et de la façon dont nous pouvons les protéger au regard de notre connaissance limitée.

Nos enfants ont grandi avec des technologies étonnantes que nous n'aurions jamais imaginées étant plus jeunes. Pour eux, Internet est simplement un autre endroit pour partager leurs idées et points de vue, pour jouer, pour créer des choses ou pour « trainer » avec leurs amis. Même si nous avons des craintes au sujet de la sécurité de nos enfants sur Internet, il est important de les encourager à explorer la toile, en sachant qu'ils peuvent nous parler de tout ce qu'ils font et voient.

Mon rôle en tant que « Norton Internet Safety Advocate » consiste à encourager chacun, parents et enfants, à tirer le meilleur d'Internet, en toute sécurité et tout en s'amusant. Ce guide est un point de départ sur ce chemin passionnant où vous et votre enfant pouvez apprendre et évoluer ensemble.
J'essaie d'expliquer certaines utilisations répandues d'Internet, tout en mettant en avant quelques sources d'inquiétude avec mes recommandations en termes d'étapes et de règles à suivre pour protéger vos enfants dans des situations spécifiques.

Que votre enfant s'aventure sur Internet pour la première fois, ou que votre adolescent ait développé une fascination pour un site Internet de socialisation, communément appelé réseau social, mon meilleur conseil est de ne pas avoir peur et d'apprendre avec votre enfant, en utilisant des outils comme ce guide, pour vous aider.

Anne-Sophie Clémot, Norton Online Safety Advocate

Sommaire

Au fil des âges

Les enfants (âgés de 5 à 10 ans)
C'est à cet âge que la plupart des enfants découvrent Internet. Aujourd'hui, de plus en plus d'écoles françaises sont équipées de salles informatiques ; les classes ont des PCs ou des Macs à leur disposition et souvent, l'enfant utilise Internet pour la première fois à l'école.

Les autres font l'apprentissage d'Internet à la maison, sous l'autorité des parents ou de la fratrie. Selon le Rapport Norton Online Living Report, publié en février 2008, 27% des parents français estiment que leurs enfants passent plus de six heures par mois sur Internet. Les jeunes enfants, dans un premier temps, se connectent majoritairement à des sites de jeux et sites éducatifs, mais ils découvriront très vite de nouveaux sites via leurs camarades.
Les sites Web, tels que KidNet, Tfou ou Barbie Girls, sont accessibles à partir de sept ou huit ans. Nous les qualifions de sites de socialisation ou réseaux sociaux de premier niveau car beaucoup d'entre eux possèdent des fonctions de « tchat », messagerie en direct et autres moyens de communication. Les parents de jeunes enfants doivent commencer par désactiver ces fonctions. Il est en effet difficile pour les enfants de cet âge de comprendre la notion de «danger de l'inconnu» associée à une personne les contactant par l'interface conviviale d'un

jeu ou de leur site préféré. Plus tard, vous pourrez expliquer à votre enfant qu'il ne faut discuter ou « tchatter » sur Internet qu'avec les personnes qu'il connaît vraiment, comme par exemple ses tantes, oncles ou amis ; et insister sur le fait qu'il doit toujours demander votre autorisation avant de discuter avec quelqu'un sur Internet.

Idéalement, avec un enfant de cet âge, vous devez vous impliquer dans ses activités en ligne aussi activement que pour ses devoirs.
Par exemple, vous devez faire en sorte que l'ordinateur utilisé par votre enfant se trouve dans une pièce commune, près de vous. Un logiciel de contrôle parental peut vous aider à limiter l'accès de votre enfant à certains sites, même lorsque vous êtes absent. Certains logiciels limitent également les informations que vous ne souhaitez pas que votre enfant divulgue, que ce soit son nom, son âge, son numéro de téléphone ou toute autre information d'ordre personnel.

Il est conseillé d'activer toutes les fonctions de filtre et de sécurité du moteur de recherche de votre ordinateur (par exemple, la fonction «SafeSearch» de Google, sous «Préférences») afin d'éviter que votre enfant n'accède malencontreusement à des sites inappropriés.

Montrez à votre enfant comment fermer une fenêtre de navigation, dites-lui qu'il est toujours conseillé de quitter un site si quelque chose de surprenant, de dérangeant ou de choquant se passe et de vous en parler si cela lui arrive.
Dites-lui de ne jamais discuter, écrire des messages ou échanger des informations avec toutes personnes connectées sur ces sites, en votre absence.

Recommandations principales :

- Limitez l'accès à des sites autorisés et le nombre d'heures de connexion.
- Définissez des paramètres élevés de sécurité pour les navigateurs, les inscriptions et les réseaux sociaux.

- Installez et maintenez à jour un logiciel de sécurité Internet (logiciel antivirus, suite de sécurité, etc.) ainsi que les contrôles parentaux.
- Utilisez les contrôles parentaux pour limiter les sites Web auxquels votre enfant peut accéder. Mais gardez à l'esprit qu'un logiciel de contrôle, aussi performant soit-il, ne remplacera jamais votre vigilance.
- Surveillez l'utilisation que votre enfant fait de l'ordinateur et, si possible, asseyez-vous à ses côtés lorsqu'il est connecté.
- Souvenez-vous que votre enfant peut accéder à Internet à la maison, à l'école, chez un ami, à la bibliothèque…; parlez à votre enfant de ses activités dans le cadre de tous ces scénarios.
- Parlez-lui de la protection des informations personnelles (nom, numéro de téléphone, etc.) et dites-lui de ne jamais communiquer ses mots de passe, même à ses amis.

Les préadolescents (âgés de 11 à 13 ans)
Les préadolescents se montrent beaucoup plus sociaux et aventureux dans leur utilisation d'Internet. Ils jouent en ligne, échangent des informations sur les derniers sites à la mode avec leurs copains, et peuvent ouvrir leurs premiers comptes de messagerie électronique et de messagerie instantanée ou créer leur premier blog. Demandez à votre enfant de vous fournir les informations sur ces comptes ainsi que les mots de passe, afin que vous puissiez contrôler leurs activités et savoir avec qui ils communiquent.

Les enfants de cet âge peuvent également commencer à vouloir accéder à des sites de socialisation, dits réseaux sociaux, tels que MySpace, Facebook ou Habbo qui rencontrent beaucoup de succès auprès des adolescents et des adultes. La plupart d'entre eux ne créeront pas de page, mais ils visiteront le site et dialogueront avec des amis, des membres de la famille et des parents qui ont leurs propres pages et profils.

Les préadolescents s'intéressent également à la musique et Internet est un moyen facile d'écouter, de découvrir et de télécharger de nouveaux morceaux, tout comme de rencontrer d'autres personnes qui partagent leurs goûts musicaux.

Ils ont la possibilité de s'informer sur les dernières actualités de leur groupe ou célébrité préférés en consultant leurs blogs ou leurs sites Web, et en accédant à différents sites pour lire les derniers potins et télécharger des photos. Les sites de vidéo en ligne, tels que YouTube!, rencontrent un énorme succès. De nombreuses vidéos emploient un langage vulgaire et des images violentes ; il est donc nécessaire de surveiller étroitement les visites effectuées par les préadolescents. Les plus créatifs des préadolescents apprennent à prendre leurs propres photos numériques, à éditer des vidéos et à échanger leurs créations avec leurs amis et la famille. Avec votre aide ou celle d'un ami plus expérimenté, ils commencent à publier leurs propres créations en ligne.

Recommandations principales :

- Vérifiez fréquemment l'historique Internet de votre ordinateur pour contrôler les sites visités par votre enfant et contrôlez ses comptes de messageries électronique et instantanée afin d'identifier les personnes avec lesquelles il communique. Et dites à votre enfant ce que vous faites afin de vous assurer que la confiance n'est pas brisée.
- Souvenez-vous que votre enfant peut accéder à Internet à la maison, à l'école, chez un ami, à la bibliothèque, dans un cybercafé, par le biais de son téléphone portable ou même d'un système de jeux; parlez à votre enfant de ses activités dans le cadre de tous ces scénarios.
- Définissez des règles sur la communication en ligne, le téléchargement illégal et la cyber-intimidation.
- Votre enfant doit savoir qu'il ne faut jamais cliquer sur un lien présent dans un courrier électronique ou un message instantané ; c'est en effet la façon la plus courante d'être infecté par un virus ou

de dévoiler des informations personnelles et confidentielles à des personnes malveillantes.
- Parlez à votre enfant des risques et inquiétudes liés à la publication et à l'échange d'informations personnelles, de vidéos et de photographies.
- Détectez tous signes de comportements obsessifs ou de dépendance en ligne (reportez-vous à Le jeu en ligne et les signes d'addiction).
- Veillez à ce que le ou les ordinateur(s) reste(nt) dans une pièce commune de la maison.
- Favorisez un dialogue ouvert et encouragez votre enfant à vous informer de tout ce qui le gêne lorsqu'il est connecté.

Les adolescents (âgés de 14 à 17 ans)
Les adolescents revendiquent plus d'indépendance et cela se reflète dans leurs comportements sur Internet. Les responsabilités vont de pair avec l'indépendance, et cela inclut l'adoption d'un comportement prudent sur Internet. A cet âge, les adolescents ont généralement constitué leurs mondes en ligne ou se sont inscrits sur des sites de socialisation tels que MySpace, Facebook ou Habbo par exemple.

Via des surnoms, l'adhésion à des groupes, les blogs, et autres sites Internet qu'ils visitent quotidiennement, les adolescents s'échangent des informations sur leur vie privée dont les « traces numériques » peuvent être disséminées sur le Web.
Ils ignorent souvent, ou oublient, que tout ce qui est publié sur le Web est visible par tous et probablement indéfiniment. Il suffit d'une simple recherche sur Google™ par le responsable des admissions d'une école ou université ou par un employeur potentiel, dans cinq, dix ou même vingt ans, pour que toutes les photos, les idées et les réflexions de votre adolescent s'affichent aux yeux de tous.

La précaution est donc de mise !

Recommandations principales :

- Renforcez les règles relatives aux comportements qui sont appropriés en ligne (langage, informations personnelles et images, cyber-éthique, téléchargement illégal, limitation des heures de connexion et interdiction d'accès aux sites réservés aux adultes).
- Soyez attentifs à la vie de votre adolescent sur Internet (réseaux sociaux, photographies, informations personnelles, clubs et activités sportives), que ce soit sur son site, le site d'un ami ou sur les pages Web de son école.
- Passez en revue les sites web visités par votre adolescent ; n'hésitez pas à discuter avec lui et à éventuellement limiter les sites qui vous choquent ou vous inquiètent.
- Souvenez-vous que votre adolescent peut accéder à Internet à la maison, à l'école, chez un ami, à la bibliothèque, dans un cybercafé, par le biais de son téléphone portable ou même d'un système de jeux; parlez à votre adolescent de ses activités dans le cadre de tous ces scénarios.
- Demandez-lui de ne pas télécharger de fichiers (musique, jeux, économiseurs d'écran, sonneries) et de ne pas effectuer des transactions financières sans votre autorisation.
- Apprenez-lui à ne jamais communiquer ses mots de passe et à faire preuve de prudence lors de la saisie d'informations personnelles sur un ordinateur public ou partagé, ou sur un PC qui ne semble pas bien sécurisé.
- Il doit savoir qu'il ne faut jamais cliquer sur un lien présent dans un courrier électronique ou un message instantané ; c'est en effet la façon la plus courante d'être infecté par un virus ou de dévoiler des informations personnelles et confidentielles à des criminels.
- Veillez à ce que le ou les ordinateur(s) reste(nt) dans une pièce commune de la maison et non dans la chambre de votre adolescent.
- Favorisez un dialogue ouvert et encouragez votre adolescent à vous informer de tout ce qui le gêne lorsqu'il est connecté. Gardez en tête que votre adolescent est encore un enfant.
- Rappelez à votre adolescent que le logiciel de sécurité Internet

(logiciel antivirus, suite de sécurité, etc.) doit toujours être activé et à jour, pour sa protection autant que la votre.

Les années fac et au-delà

Votre adolescent a grandi et il quitte aujourd'hui la maison, pour étudier ou pour travailler. Il doit comprendre toutes les responsabilités supplémentaires assumées par les adultes vis à vis du monde en ligne.

Elles incluent la protection de sa vie privée, en particulier son numéro de sécurité social et ses informations financières ; la prévention de l'usurpation d'identité et les risques liés à sa solvabilité, ce qui est particulièrement important pour un jeune adulte.

Si votre jeune adulte utilise un ordinateur portable dans le cadre de ses études ou de son nouveau travail, assurez-vous qu'il a compris les risques additionnels liés à l'utilisation d'une connexion sans fil et qu'il a acheté le logiciel de sécurité nécessaire comportant une solution fiable de sauvegarde de données. Les jeunes adultes peuvent être tentés de négliger ces éléments; il convient donc d'insister sur l'importance d'être vigilant lorsqu'il s'agit de la sécurité des ordinateurs portables et des informations personnelles et confidentielles qu'il contient.

Respecter certaines règles

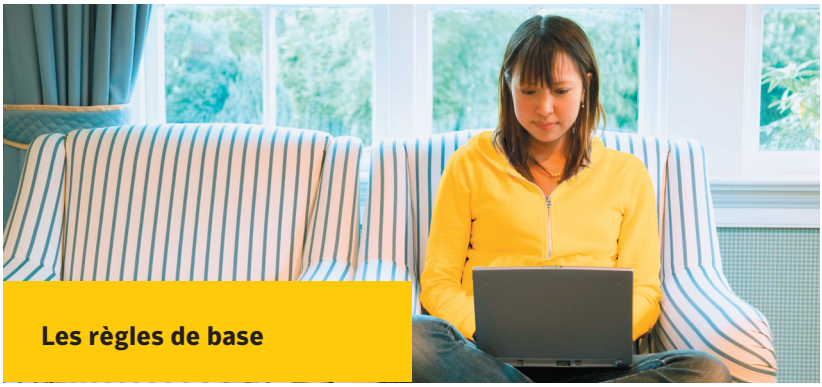
Parents

- Tenez-vous au courant des dernières technologies. Il n'est pas nécessaire que vous soyez un expert, mais une connaissance de base permet à votre famille de naviguer sur Internet en toute sécurité. Suivez une formation technique de base et apprenez à connaître les nouveaux produits au fur et à mesure qu'ils sont commercialisés. Visitez le site www.symantec.fr pour être informés des mises à jour.
- Communiquez en permanence avec vos enfants sur tout ce qu'ils voient et font sur Internet. Apprenez leur jargon et demandez-leur si vous ne comprenez pas quelque chose. Restez à l'écoute.
- Contrôlez régulièrement l'activité de vos enfants sur Internet. Vous devez connaître les sites qu'ils visitent. Faites-leur savoir que vous contrôlez leurs activités parce que vous les aimez, que vous voulez qu'ils comprennent qu'Internet est un espace public et donc, jamais véritablement privé.

Enfants

- Restez prudents et naviguez en toute sécurité : Ne divulguez jamais vos informations personnelles ! Ne donnez jamais votre nom, votre adresse, votre date de naissance, votre numéro de téléphone, le nom de votre école, une photographie de vous-même, ou de quelqu'un d'autre, à qui que ce soit sur Internet.

- Restez à distance et ne communiquez pas avec des inconnus : Les inconnus sur Internet sont dangereux - RESTEZ A DISTANCE ET N'ENTREZ PAS EN COMMUNICATION AVEC EUX.
  Peu importe ce qu'il ou elle vous dit, NE RENCONTREZ JAMAIS une personne connue sur Internet. Vous n'avez aucun moyen de savoir qui est véritablement cette personne. Ne parlez jamais avec un(e) inconnu(e) sur Internet et ne lui dites jamais où vous habitez.
- Restez en contact et parlez à vos parents : Faites part à vos parents ou à un adulte de confiance de tout ce que vous voyez sur Internet. Informez-les toujours si quelque chose vous met mal à l'aise. Et rappelez-vous que tout ce que vous voyez et entendez sur Internet n'est pas toujours «vrai» ou même «normal».



Les règles de base

Naviguez sur Internet en toute sécurité
Assurez-vous que votre navigateur est paramétré de façon à ce que vous bénéficiez de ses options de sécurité intégrées. Par exemple, Microsoft® Internet Explorer (le navigateur le plus répandu) offre des paramètres de sécurité et de protection de la vie privée. Elles sont accessibles sous «Outils», puis «Options Internet».

Les moteurs de recherche les plus prisés, comme Google™, offrent également certains dispositifs de sécurité. Par exemple, SafeSearch de Google™, accessible sous «Préférences» à partir de la page d'accueil de Google™, vous permet de limiter l'affichage de certains sites et contenus explicites (pornographiques) dans les résultats de recherche. Un utilisateur averti peut bien sûr facilement modifier ces paramètres, mais cela peut s'avérer très utile pour les plus jeunes internautes.

Protégez vos mots de passe
Evitez d'utiliser des mots de passe faciles à deviner, tels que des mots du dictionnaire, des noms ou des dates que votre enfant ou un pirate informatique peut découvrir.
Voici une bonne méthode pour définir et gérer ses mots de passe :

Choisissez un mot de passe principal que vous pouvez retenir, puis

personnalisez-le pour différents sites Web. La première étape consiste à choisir un bon mot de passe principal, composé de plus de six caractères et combinant lettres et numéros (plutôt que de véritables mots). Utilisons, par exemple, le mot de passe « mifflin8 ». Ajoutez-lui ensuite la première et la dernière lettre du site Web (exemple pour Amazon.com : «Amifflin8n»). Cette méthode permet de se souvenir de tous ses différents mots de passe et de conserver une complexité suffisante pour rendre la tâche difficile à un pirate informatique. L'ordre adopté est logique pour vous mais pas pour les autres. Cela permet également d'avoir des mots de passe différents pour différents comptes. Et si le mot de passe d'un compte est compromis, les autres sont toujours protégés.

Les mots de passe peuvent se multiplier à l'infini ! Chaque mot de passe est plus compliqué que l'autre. Il est donc difficile de tous les mémoriser et de les récupérer si besoin.

De quelle façon convient-il alors de les gérer ? Il existe des applications informatiques qui gèrent les mots de passe, et certains navigateurs offrent la possibilité d'enregistrer de nombreux mots de passe. Il est risqué d'avoir une liste de ses mots de passe stockée dans l'ordinateur, ou sur un bloc-notes à proximité de celui-ci, etc.

Note à l'attention des parents : assurez-vous de détenir les mots de passe de votre enfant pour accéder à sa messagerie électronique, messagerie instantanée, et même aux réseaux sociaux.
Cela vous permet de contrôler les personnes qui communiquent avec votre enfant.

Sécurisez votre réseau sans fil (Wireless network ou « wifi »)
Les réseaux domestiques sans fil présentent d'autres problèmes de sécurité et il y a donc un certain nombre d'étapes simples à suivre pour s'assurer que ces réseaux sont protégés contre l'intrusion d'inconnus qui pourraient utiliser votre bande passante ou pire,

héberger leur pourriel (spam) et effectuer d'autres attaques à partir de votre système. Egalement, un ordinateur portable et un réseau sans fil permettent à vos enfants d'accéder à Internet de n'importe quel endroit dans la maison, ce qui réduit à néant vos efforts de surveillance de leurs activités.

Si vous disposez à la maison d'une connexion sans fil (ou «wifi»), assurez-vous d'avoir pris toutes les dispositions nécessaires pour la sécuriser : redéfinissez le mot de passe du routeur de manière à ce qu'il respecte les bonnes règles en matière de mot de passe et qu'il ne soit pas facile à deviner, activez le cryptage sans fil pour éviter qu'un inconnu repère votre réseau sur Internet, restreignez l'accès partagé de votre système sur le réseau et assurez-vous que votre logiciel de sécurité Internet est bien à jour. Certains parents vont jusqu'à déconnecter leur routeur et à le mettre dans leur chambre la nuit. Adoptez les mesures qui vous conviennent le mieux.

Le logiciel de contrôle parental

Un logiciel de contrôle parental vous permet de choisir si votre enfant est autorisé à naviguer sur Internet et d'éviter qu'il accède à des sites dont le contenu est inapproprié.

Les contrôles parentaux diffèrent en fonction de l'application offrant cette possibilité. Il existe généralement différents niveaux, de telle sorte que vous pouvez personnaliser le programme en fonction de l'enfant à protéger. Par exemple, pour un enfant de cinq ans, vous pouvez fournir une «liste blanche» de sites Web présélectionnés et validés par vos soins que votre enfant est autorisé à visiter. Egalement, vous pouvez configurer des comptes de telle sorte que vous devez vous connecter pour que votre enfant puisse surfer sur Internet, ou limiter le temps de connexion pour éviter que votre enfant ne passe trop de temps sur le Web au détriment de ses devoirs, de ses activités sportives ou du temps passé avec ses amis.

Vous pouvez accorder un accès plus souple aux enfants plus âgés. Il est possible de restreindre l'accès à Internet par catégories de sites dans la bibliothèque de programmes afin d'éviter que votre enfant ne soit exposé à des sites ou du contenu à caractère raciste, pornographique ou douteux.

Aucun logiciel cependant n'offre une protection parfaite. Il est donc nécessaire que les parents associent le logiciel de sécurité à de l'éducation, de la surveillance et de la communication avec leurs enfants pour assurer leur protection, quel que soit leur âge.
Les ressources du Web sont riches et il est dommage de le verrouiller intégralement.

Les Favoris sur Internet
Les sites de socialisation ou réseaux sociaux tels que MySpace, Facebook ou Habbo rencontrent un franc succès auprès des adolescents. YouTube! est également très prisé mais constitue un problème pour les parents car il n'existe aucun filtre au niveau du langage ou des contenus réservés aux adultes.
Vérifiez auprès de l'administrateur du réseau informatique de l'école de votre enfant quels sont les sites les plus fréquemment visités. Demandez à votre adolescent s'il possède des comptes (et essayez également de toujours vérifier par vous-même).

Les plus jeunes enfants visitent et s'inscrivent sur des sites de loisirs, tels que Barbie Girls, KidNet ou Tfou. Ces sites proposent des jeux et des activités incluant des forums ou « tchat ». Ils ressemblent beaucoup aux réseaux sociaux. Les sites pédagogiques, tels que takatrouver.net ou nicoland.fr, aident les enfants à apprendre à lire ou les mathématiques en s'amusant. Que votre enfant soit adolescent, préadolescent ou plus jeune, demandez-lui quels sont les sites Internet sur lesquels lui et ses amis vont le plus souvent. Demandez-lui sur lesquels d'entre eux il s'est inscrit et de vous les présenter. Vous saurez rapidement si vous approuvez ou non. Faites en sorte que

la conversation reste «neutre» afin de ne pas donner à votre enfant l'impression de subir un interrogatoire.

Les risques

Les prédateurs sur Internet

Il n'y a évidemment pas une personne malveillante ou un prédateur sexuel derrière chaque internaute, mais on dénombre suffisamment de cas - au dénouement tragique - d'enfants approchés par des prédateurs sexuels pour que les parents s'inquiètent. Veillez à ce que votre enfant sache qu'il ne doit jamais communiquer par courrier électronique (e-mail), « tchat » sur des forums ou par messagerie instantanée ou envoyer des messages texte (sms) à des inconnus ; et qu'il ne doit jamais rencontrer « dans le monde réel » un inconnu dont il aurait fait la connaissance sur Internet. Assurez-vous qu'il comprend bien que toute personne rencontrée sur Internet reste un INCONNU et ce, quel que soit le nombre de messages échangés, ou la durée des échanges (1 semaine, 1 mois ou plus)
Au cas où un inconnu contacterait votre enfant sur Internet pour parler de sexe, informez immédiatement la police ou la gendarmerie ainsi que l'école de votre enfant.

Le plagiat et la fraude

Il est très facile de trouver sur Internet des corrigés pour les principaux manuels scolaires et de nombreux sites Web proposent la vente de rédactions, de dissertations, d'exposés ou de thèses ! Tricher n'a jamais été aussi facile, aussi accessible et aussi tentant pour nos

enfants. Rappelez à votre enfant qu'il est très important d'utiliser Internet à des fins de recherche uniquement. Expliquez-lui également que le contenu généré par l'utilisateur, comme sur Wikipédia par exemple, peut constituer un point de départ à de nouvelles recherches mais que ce contenu n'est pas toujours aussi fiable que les sources d'information traditionnelles, telles que les encyclopédies.

La cyber-intimidation et le cyber-harcèlement

La technologie n'a jamais offert à nos enfants autant de moyens pour se connecter, faire des rencontres et communiquer. Malheureusement, certains enfants utilisent la messagerie électronique (e-mail), la messagerie instantanée, la téléphonie mobile et les messages texte (sms) pour embarrasser, porter atteinte à la réputation d'autres enfants ou les intimider. En outre, les messages « numériques » des enfants peuvent être édités afin d'en modifier la signification pour les transmettre à d'autres enfants, dans le but de les embarrasser, les intimider ou les insulter.

Assurez-vous que votre enfant sache qu'il doit protéger tout message texte, même le plus banal, et qu'il doit faire attention aux mots qu'il emploie. Il ne doit jamais être ou devenir une « cyber-brute », une « cyber-terreur » ou un « cyber-agresseur » et il doit toujours signaler s'il est victime de cyber-intimidation.

Gardez une copie de tous les messages d'intimidation en utilisant la touche «Impression écran» (ImpEc) du clavier de votre ordinateur et en copiant le message dans votre programme de traitement de texte.

Le cyber-harcèlement est un développement dangereux de la cyber-intimidation et est utilisé par des personnes qui pratiquent le harcèlement dans le mode réel ou « hors ligne ». En étant conscients du danger, nos enfants peuvent apprendre à se défendre et il appartient donc aux parents de savoir comment les aider. Le « harceleur » peut détourner un compte de messagerie et se faire passer pour la personne victime de ce détournement.

L'agresseur peut « déformer » la page d'un réseau social et adresser

des messages haineux aux amis de la victime, se lancer dans le vol d'identité ou tenter de détruire la crédibilité ou la réputation de quelqu'un. Le cyber-harcèlement est dangereux et doit être signalé à la police, aux fournisseurs d'accès Internet et aux hébergeurs de sites Web. Conservez toutes les preuves de cyber-harcèlement et cyber-intimidation.

Le partage de fichiers et le téléchargement de musiques et de vidéos

Les enfants apprennent très vite les joies de l'échange de morceaux de musique. C'est souvent vers la préadolescence que les enfants sont informés de l'existence de sites de partage de fichiers, en particulier les sites gratuits.

Apprenez à votre enfant les dangers liés aux programmes et sites de partage de fichiers, qui permettent à des inconnus d'accéder à votre ordinateur. L'utilisation de sites de partage de fichiers peut exposer votre ordinateur et vos informations aux logiciels « robots », logiciels espions, enregistreurs de frappe clavier, virus et autres codes malveillants et dangereux.

En outre, le téléchargement gratuit de musiques ou de vidéos est souvent illégal. Indiquez à votre enfant les sites permettant le téléchargement légal de musiques et de vidéos, tels que iTunes et Virginmega.

Les informations personnelles et l'usurpation d'identité

Votre enfant ne sait pas automatiquement ce que signifie informations « personnelles ». Vous devez donc lui expliquer: il s'agit de toute donnée, information ou renseignement qui permet de l'identifier et qui permet à un inconnu d'accéder à des informations personnelles et/ou financières. Les informations personnelles ou confidentielles sont des données du monde « réel » : un nom, un numéro de téléphone, une adresse, le nom de son club de sports ou de son école, et même le nom du médecin de famille.

Les fraudeurs ou cybercriminels peuvent transformer un tout petit

indice en un dossier complet sur un enfant et/ou ses parents. Ils négocient et vendent ensuite ces données confidentielles contre de l'argent. Il est étonnamment facile pour des personnes mal intentionnées de faire une demande de crédit au nom de votre enfant et d'obtenir des biens/marchandises et de l'argent du monde réel, tout en portant atteinte à solvabilité et à la réputation du nom de l'enfant (ou du votre).
Si vous pensez avoir été victime d'usurpation de votre identité, contrôlez vos relevés de compte bancaire ou de crédit afin de rechercher toute preuve de nouveaux comptes ou d'emprunts. Après avoir établi la preuve qu'il y a eu usurpation d'identité, vous devez le signaler à la police ou à la gendarmerie. Ce rapport de police renforcera votre dossier lorsque vous travaillerez avec les sites et les entreprises impliquées. Vous pouvez également «geler» votre compte et celui de vos enfants.

Les sites de socialisation ou réseaux sociaux
Les sites Web de socialisation, communément appelés réseaux sociaux, sont le phénomène sur Internet qui enregistre le plus fort taux de croissance, tant auprès des enfants que des adultes. Ce sont cependant les préadolescents et adolescents qui animent cette croissance. Les réseaux sociaux qui rencontrent le plus vif succès sont MySpace, Facebook et Habbo. Tous les trois offrent aux enfants la possibilité de discuter avec des amis existants et d'en rencontrer de nouveaux. S'ils sont utilisés avec précaution, ces sites sont un formidable moyen pour les enfants de communiquer et de partager leurs expériences.
Cependant, si des mesures de sécurité ne sont pas respectées, ils peuvent exposer vos enfants à l'usurpation d'identité et aux prédateurs.

Apprenez à votre enfant à ne pas afficher d'informations personnelles ou de photographies inappropriées ou tendancieuses. Une fois publiées, ces informations deviennent en effet publiques et peuvent

être stockées sur les ordinateurs et les fichiers d'historique Internet d'autres personnes.
Et même si vous supprimez ces informations ou ces photos, elles restent présentes sur Internet et donc accessibles à des personnes qui peuvent les utiliser et en abuser.

Les réseaux sociaux permettent aux enfants de se constituer des réseaux d'amis communiquant librement entre eux.
Assurez-vous que votre enfant n'autorise pas des personnes qu'il ne connait pas à intégrer son ou ses réseau(x). Les pages doivent rester privées, de façon à ce que seuls les amis « invités » peuvent les trouver et les voir sur le site. En effet, lorsqu'un inconnu s'infiltre dans un réseau, les autres membres de ce réseau lui accordent automatiquement un certain niveau de confiance, basé sur la relation avec votre enfant. Si l'inconnu est une personne malintentionnée, il peut essayer d'abuser de votre enfant ou de ses amis du réseau.

Veillez à ce que votre enfant paramètre correctement les fonctions de communication de façon à valider tous les affichages apparaissant sur sa page. Cela limitera même la possibilité, pour l'un de ses amis, de publier une photo amusante mais embarrassante ou de faire une remarque que vous préféreriez que sa grand-mère ne lise pas !

Pornographie, racisme, anorexie et sites prônant la haine
La face la plus sombre d'Internet comporte des éléments dangereux et illégaux. En l'absence de contrôles parentaux ou de filtres de navigation, il est pratiquement inévitable que votre enfant soit exposé à ce que vous et lui trouvez choquant.

Veillez à ce que votre enfant vous signale s'il est confronté à ce type de situation et rassurez-le : vous ne serez pas fâché si c'est le cas.

Certains enfants et adolescents peuvent afficher leur curiosité face à des sites à caractère raciste, des messages prônant la haine ou

encourageant des comportements dangereux, tels que l'anorexie, l'automutilation ou le suicide. Vous ne pourrez le détecter qu'en vérifiant régulièrement l'historique du navigateur de votre ordinateur. Même une seule visite doit vous encourager à en parler avec votre enfant. Ne supposez pas automatiquement qu'il ne s'agit que de simple curiosité. Expliquez les règles s'appliquant à la maison à propos de ces sites et demandez à votre enfant quelles sont ses motivations pour les visiter. Dans le dialogue, si votre enfant évoque des problèmes tels que la dépression ou le dégoût de soi, demandez l'aide d'un thérapeute ou d'un spécialiste compétent pour gérer ces situations.

Le respect de la vie privée sur Internet

Nous avons été suffisamment avertis (ou aurions dû l'être) que les personnes sur Internet ne sont pas toujours ce qu'elles prétendent être. Il est très facile de mentir à propos de son âge, de son sexe et de son adresse; de nombreuses personnes le font innocemment et d'autres pour des raisons qui le sont moins.

Rappelez en permanence à votre enfant, quel que soit son âge, qu'il ne peut pas faire davantage confiance à des inconnus sur Internet qu'à des inconnus dans la rue. Il ne doit jamais autoriser un inconnu à s'inscrire dans une liste d'amis ou à s'insérer dans un dialogue ou une conversation par messagerie instantanée. De même, il ne doit jamais accepter des logiciels gratuits, des sonneries ou des économiseurs d'écran provenant d'inconnus.

Rappelez à votre enfant que les adresses électroniques, noms de compte utilisateur et pseudonymes doivent être différents de son véritable nom, du nom de son école ou d'une association des deux. Egalement, ils ne doivent pas être provocants ou incitatifs pour une personne malintentionnée. Votre enfant doit rester aussi anonyme que possible et il ne doit jamais communiquer un mot de passe, même à un ami.

Veillez à ce que le site Web de l'école de l'enfant soit protégé par un mot de passe ou nécessite une ouverture de session pour obtenir plus que des informations superficielles et publiques. Par exemple, les écoles utilisent aujourd'hui un site Web pour communiquer des itinéraires ou la composition d'équipes sportives ou d'autres groupes itinérants. Il est évidemment impératif que ces informations ne soient pas dans le domaine public.
La publication sur le site Web des listes des élèves de la classe, des adresses des étudiants et des numéros de téléphone personnels peut également constituer un probléme si le site n'est pas sécurisé.

La messagerie électronique et instantanée
Assurez-vous que le filtre anti-spam des comptes de messagerie de votre enfant est paramétré au niveau de sécurité le plus élevé. Selon une étude de Symantec, 80% des enfants déclarent recevoir des spams indésirables quotidiennement. Les enfants doivent donc utiliser des noms de comptes de messagerie qui n'incitent pas des inconnus à les contacter.

Par exemple, ils ne doivent pas utiliser des associations « prénom & nom ». Ils ne doivent pas non plus utiliser des adresses ou des pseudos suggestifs, tels que «sexylexy» ou «sauvageonne», même si cela semble «sympa». Veillez à ce que votre enfant utilise des mots de passe à haut niveau de sécurité et que ceux-ci ne soient jamais communiqués, même à des amis. Vous devez connaître les mots de passe des comptes de messagerie de votre enfant afin de pouvoir surveiller ses activités régulièrement. Regardez à qui il envoie des messages électroniques et de qui il en reçoit. Connaissez-vous tout le monde ? Dites à votre enfant que vous faites cela pour assurer sa sécurité et non pas parce que vous ne lui faites pas confiance.

Recommandations principales :

- Apprenez à votre enfant à ne pas cliquer sur des liens figurant dans des courriers électroniques reçus, car ces liens peuvent le rediriger vers de faux sites Web.
- Désactivez la fonction « prévisualisation » du courrier électronique. Cela empêche en effet l'exécution d'un potentiel code malveillant dans la zone de message.
- Votre enfant ne doit pas répondre à des courriers électroniques ou à des messages instantanés d'une personne qu'il ne connait pas ou de qui il ne s'attendait pas à recevoir de courriers.
- Ne cliquez jamais sur un lien ou ne téléchargez pas un fichier par le biais de la messagerie instantanée.
- Votre enfant ne doit pas rendre public son profil de messagerie instantanée ou sa page de réseau social.
- Paramétrez les préférences de messagerie instantanée pour tenir les inconnus à l'écart.
- Votre enfant ne doit pas laisser les sites tels que Yahoo!® (entre autres) afficher son statut de connexion lorsqu'il est en ligne ou publier son identité ou des informations personnelles sur les pages qu'il visite.
- Votre enfant doit toujours se déconnecter lorsqu'il n'utilise pas la messagerie instantanée ou lorsqu'il édite sa page de réseau social afin d'assurer la protection de sa vie privée.

Les blogs

Un blog est un journal personnel en ligne qui peut être très général ou dédié à un sujet spécifique. Les adolescents ont souvent des blogs qui ressemblent davantage à des journaux intimes, sauf qu'ils sont accessibles à tout le monde sur Internet, par l'intermédiaire du propre site Web de l'adolescent ou du réseau social auquel il est inscrit. Cela revient à publier son journal sur Internet, à la vue de tous. Votre adolescent doit être sûr de l'objectif qu'il s'est fixé pour son blog avant de le réaliser. Les moteurs de recherche peuvent généralement collecter les informations qui sont publiées, anéantissant vos efforts

pour protéger la vie privée de votre enfant ou la votre. Si vous publiez des photos ou des liens vers des sites Web privés sur votre blog, vous restreignez également votre vie privée.

En outre, des personnes, telles que des employeurs potentiels ou responsables d'admission dans des écoles peuvent lire votre blog.

Cette visibilité peut également avoir un impact négatif sur d'autres domaines de votre vie. Par exemple, des personnes interviewées pour un emploi peuvent ne pas être retenues en raison d'éléments figurant dans leurs blogs personnels ou sur les blogs d'amis qui parlent d'eux. Ne laissez pas votre enfant devenir une victime du blog.

Les virus, vers et logiciels espions

Les virus informatiques sont présents depuis plus de 25 ans et prennent différentes formes. Avec le succès des courriers électroniques et de l'échange de fichiers sur Internet, la diffusion de ces menaces a véritablement explosé ! Les personnes qui créent des virus et autres formes de codes malveillants ou «maliciels» avaient l'habitude de faire des ravages pour prouver leurs compétences en informatique ou pour épater l'entourage. Mais aujourd'hui, les enjeux sont bien plus importants et de nombreux délinquants sont des cybercriminels internationaux, motivés par les gains financiers générés par leurs activités illégales.

La diffusion de maliciels, tels que les logiciels espions ou les enregistreurs de frappe clavier le biais des courriers électroniques, des messageries instantanées, des pages de réseau social infectées et des sites de partage de fichiers peuvent occasionner beaucoup de problèmes. Les logiciels espions et les enregistreurs de frappe clavier contrôlent l'activité normale de votre ordinateur et transmettent par Internet vos données personnelles aux criminels.
Assurez la sécurité de votre (vos) enfant(s) et de votre (vos) ordinateur(s) en installant un logiciel de sécurité Internet sur chaque

ordinateur du foyer et en vous assurant qu'il est mis à jour. Demandez à votre enfant de ne pas désactiver le programme de vérification de virus ou le pare-feu, même s'il pense que cela accélérera un jeu. Ce n'est vraiment pas un risque à prendre !

Les « robots »
Un « robot » est un type de logiciel malveillant qui s'infiltre dans votre ordinateur afin de permettre à des cybercriminels de prendre le contrôle de votre ordinateur, sans même que vous soyez au courant.

Ces « robots Web » font généralement partie d'un réseau de machines infectées qui sont utilisées pour effectuer différentes tâches automatiques, dont la diffusion de virus, de logiciels espions, de spams, de messages de phishing (hameçonnage) et autres codes malveillants. Pire encore, les robots servent à dérober vos informations personnelles et à provoquer des ravages sur votre compte, comme l'utilisation illégale de vos cartes de crédit et de vos comptes bancaires. Les robots peuvent également afficher des sites Web fictifs, prétendant être légitimes, transférer des fonds à votre insu, fournir vos noms d'utilisateur et vos mots de passe, à des fins d'activités illégales.

La meilleure défense contre ces robots est d'installer un logiciel de sécurité et de définir les paramètres de votre logiciel pour que les mises à jour soient effectuées automatiquement, garantissant ainsi un très haut niveau de protection.

Les photos et vidéos numériques
De nombreux enfants ont aujourd'hui des téléphones portables avec des fonctions appareil photo et parfois caméra numérique. Expliquez à votre enfant qu'il est nécessaire de protéger ses photographies ou vidéos sur Internet contre des inconnus ou même des copains qui peuvent les utiliser de façon inappropriée ou les trafiquer.
Vous pouvez suivre l'envoi des photos numériques à partir de votre téléphone (il suffit de vérifier votre relevé de communication). Veillez

à ce que votre enfant vous montre les photos sur son téléphone de manière à ce que vous puissiez l'avertir si quelque chose vous semble risqué ou inapproprié pour le partage. Si vous utilisez des sites de partage de photos, tels que Flickr, veillez à ne pas autoriser les autres à utiliser vos photos, en particulier les photos de personnes.

Recommandations principales :

- Ne diffusez pas vos albums de photos.
- Exigez des personnes visitant un site de partage de photos qu'elles utilisent un mot de passe.
- Sauvegardez vos photos avec un logiciel de sauvegarde car les plantages informatiques, les pannes de courant ou les catastrophes naturelles peuvent facilement détruire vos photos et d'autres fichiers informatiques.
- Utilisez uniquement les services de photo en ligne assurant une protection de la sécurité.
- Lorsqu'un service de photo en ligne vous propose l'option d'envoyer un courrier électronique par l'intermédiaire de leur service, protégez la vie privée de vos amis en leur envoyant un lien vers le site.

Le shopping sur Internet

Internet est le paradis des acheteurs, en particulier pour les adolescents possédant une carte de crédit ou une carte-cadeau prépayée (ou ayant accès à la votre).
Il y a, cependant, des règles à respecter pour acheter en toute sécurité.

Avant tout achat en ligne, assurez-vous que votre logiciel de sécurité est activé et à jour. N'achetez que sur des sites connus et réputés, car l'utilisation d'un site Web inconnu peut être risquée. Pour une plus grande sécurité, assurez-vous également que toute page sur laquelle vous saisissez vos données personnelles, comme votre adresse ou votre numéro de carte de crédit, utilise le cryptage. Pour le savoir, vérifiez que l'adresse Web commence par «https». Egalement, la présence d'un icône représentant un cadenas, situé en bas du cadre

de navigation, indique que le site Web sur lequel vous vous trouvez utilise le cryptage pour protéger vos communications.

Effectuer des achats sur des sites Internet réputés ne constitue que le premier réflexe d'un acheteur en ligne avisé. Ne cliquez jamais sur des liens figurant dans des courriers électroniques pour accéder à votre magasin ou à votre site de vente en ligne préférés. Vous devez toujours saisir l'adresse du magasin dans la fenêtre de navigation. Cela vous évitera d'être victime d'une attaque de phishing (hameçonnage) et donc d'être redirigé vers une version fausse de votre site d'achat préféré, où les cybercriminels pourraient, entre autres, dérober vos mots de passe, vos paramètres d'ouverture de session et les informations stockées sur votre carte de crédit.

Contrôlez vos relevés de carte de crédit aussi souvent que possible, au minimum tous les mois. C'est la meilleure façon d'identifier les utilisations frauduleuses de votre carte de paiement. Les établissements bancaires offrent une protection aux consommateurs et collaboreront pour gérer tous les frais contestés ou non autorisés.

Les services bancaires et le paiement de factures sur Internet
Si vous ou votre enfant effectuez des activités bancaires sur Internet, ne le faites jamais sur un ordinateur public ou partagé ou sur un réseau sans fil non équipé de fonctions de sécurité telles qu'un pare-feu (firewall).
Vous pourriez en effet courir le risque qu'un cybercriminel dérobe les informations relatives à votre compte et vos paramètres d'ouverture de session pour voler votre argent. Saisissez l'adresse Web de votre banque ou de l'organisme que vous souhaitez régler dans le navigateur Web ; ne cliquez jamais sur un lien figurant dans un courrier électronique.

Le jeu en ligne et les signes d'addiction
Que signifie MMORPG ? Ce sigle fait référence aux « jeux de rôle en

ligne massivement multi-joueurs » dont le succès est croissant et dont l'utilisation peut potentiellement rendre dépendant. Des jeux tels que le Monde de Warcraft (World Of Warcraft), Le Seigneur des Anneaux ou Everquest, rencontrent actuellement un franc succès. Ils peuvent plonger certains adolescents dans un monde virtuel et, pour certains d'entre eux et en particulier les garçons, ils peuvent réellement les détourner de leurs vies réelles.

Selon une étude réalisée par le Professeur Mark Griffiths, directeur de l'Unité de recherche internationale sur les jeux de l'Université de Nottingham Trent en novembre 2006, les joueurs en ligne peuvent présenter les mêmes signes d'accoutumance que les joueurs du monde réel, tels que l'état de manque, la perte de contrôle et la négligence envers d'autres activités.

Définissez des règles avec votre enfant sur le temps passé sur ces sites, qu'il y ai ou non besoin d'argent pour l'inscription ou pour acheter des accessoires de jeux (dans le monde réel ou dans le cadre du jeu en ligne) et sur toutes autres inquiétudes que vous pourriez avoir.

Un mot pour conclure

Internet est une ressource formidable, dont les éléments font souvent penser à une ville réelle. Internet nous offre des sources d'éducation, des loisirs, des nouvelles du monde entier et améliore nos vies en nous permettant d'accéder, entre autres, à des services formidables comme la messagerie électronique, le « tchat », la messagerie instantanée, le shopping en ligne, etc.

En s'informant, en étant conscient des risques et des dangers sur Internet et en utilisant un logiciel de sécurité Internet à jour, vous pouvez aider votre enfant à naviguer en toute sécurité dans ce « cyber monde » exceptionnel et à y être de plus en plus indépendant. Maintenez-vous informé sur les nouvelles technologies et les problèmes ou risques sur Internet. Assurez-vous que votre comportement sur Internet soit un modèle pour votre enfant, en adoptant des bonnes pratiques de sécurité.

Principaux conseils pour protéger votre famille sur Internet

- Laissez l'ordinateur dans une pièce commune.
- Etablissez des règles d'utilisation d'Internet.
- Comprenez ce qu'est un réseau social.
- Aidez vos enfants à protéger leurs informations personnelles.
- Protégez les mots de passe de vos enfants.
- Vérifiez régulièrement l'historique de navigation Internet de votre ordinateur.
- Passez du temps sur Internet avec vos enfants.
- Apprenez la cyber-éthique à vos enfants.
- Soyez un Internaute avisé.
- Apprenez à vos enfants à informer un parent, un enseignant ou un adulte de confiance s'ils ont vu quelque chose de gênant ou de choquant sur un ordinateur.

Sites Utiles

www.norton.com/fr/familyresource
www.actioninnocence.org (organisation non gouvernementale qui contribue à préserver la dignité et l'intégrité des enfants sur Internet.)
www.mineurs.fr
www.foruminternet.org
www.saferinternet.org

Consultez le site **www.symantec.com/fr/familyresource**