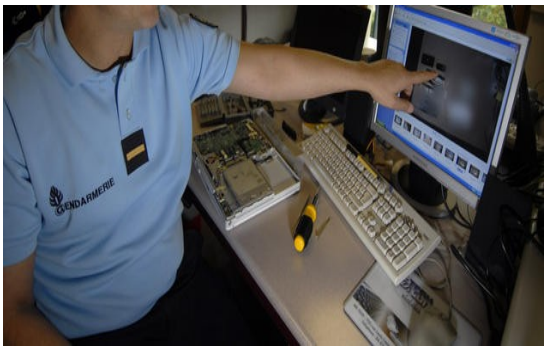
Internet est un espace de liberté où chacun peut communiquer et s'épanouir. Les droits de tous doivent y être respectés, pour que ce réseau informatique mondial reste un espace d'échanges et de respect.

Vous trouverez ci-dessous des informations, ainsi que des conseils pour mieux vous protéger et protéger vos proches dans leur utilisation de l'Internet.



(droits réservés)

Conseils aux Parents

Ne laissez pas vos enfants seuls face à Internet

Si vous deviez ne retenir qu'une règle : installez l'ordinateur dans la salle de séjour ou une pièce commune. L'internet doit être un outil familial et vos enfants vous sentiront présents. Si vous les laisser utiliser Internet dans leurs chambres, vous aurez plus de mal à les protéger.

Contrôlez l'accès à l'ordinateur

Lorsque vos enfants se retrouvent seuls, pensez à protéger votre ordinateur avec un mot de passe et les empêcher de se connecter à Internet en votre absence. Sachez que les adresses des sites visités sont enregistrées dans l'historique de votre logiciel « navigateur » auquel on peut accéder en utilisant la commande CTRL + H.

Établissez un dialogue

Laissez vos enfants vous montrer comment ils surfent : leurs sites préférés, ceux qui pourraient vous intéresser. Invitez-les à vous montrer ce qui les gêne, discutez-en avec eux.

Éduquez vos enfants à la prudence

Apprenez leur des règles simples : ne jamais donner d'informations personnelles (adresse, téléphone) ; quitter immédiatement un site qui les met mal à l'aise ; ne pas organiser de rendez-vous avec une personne rencontrée sur Internet sans vous en parler.

Installez un logiciel de contrôle parental

Ils permettent de filtrer l'accès à l'internet en interdisant la consultation de certaines informations sensibles ou illicites (pornographie, racisme, violence...) La majorité des fournisseurs d'accès à Internet propose des logiciels de filtrage parental. Des logiciels gratuits, performants et simples d'utilisation, peuvent être téléchargés. Il existe également des dispositifs de filtrage sur les systèmes d'exploitation ainsi que sur certains logiciels de navigations. Mais attention : ces outils ne peuvent en aucun cas remplacer la vigilance des parents.

Conseils aux jeunes

être méfiant à l'égard de ceux qui veulent en savoir trop : ne donner aucune information (nom, numéro de téléphone, adresse ou celle de l'école...) sans en parler aux parents.

Si on reçoit ou voit quelque chose qui met mal à l'aise , ne pas chercher à en savoir plus , se déconnecter et en parler aux parents.

Si une rencontre de quelqu'un d'inconnu est envisagée, ne jamais y aller sans en parler aux parents.

La messagerie : supprimer , sans les ouvrir, les mails non demandés ou envoyés par des personnes inconnues

Achats sur internet : ne rien acheter , sauf si les parents sont présents pour conseiller (voir plus bas)

Les mots de passe : Ne jamais donner un mot de passe.

Internet Prudent

Qu'est-ce que la prudence sur Internet ?

Être prudent sur Internet, c'est d'abord ne pas avoir peur de tout : la plupart des pièges de l'Internet sont grossiers. Pour les détecter, il suffit souvent de se dire : « si un inconnu me disait ça dans la rue, est-ce que je le croirais ? » la prudence sur Internet, c'est aussi résister aux tentations du téléchargement et se méfier du sentiment d'anonymat.

Qu'est-ce que le « scam » ?

Il n'y a pas plus de miracles sur Internet que dans la vie courante. Si vous recevez un courrier d'un inconnu vous proposant une transaction financière, vous pouvez être sûr que c'est une arnaque, appelée « scam ». L'inconnu vous parle d'une importante somme (héritage, pot-de-vin, comptes tombés en déshérence, fonds à placer à l'étranger, etc.) et demande votre aide pour son transfert, en échange de quoi il vous offre un pourcentage sur la somme. Il finira par vous demander de lui envoyer une avance ou des frais quelconques (notaires, entreprises de sécurité, pots-de-vin...) Vous ne reverrez jamais votre argent.

Puis-je servir d'intermédiaire pour des paiements internationaux ?

Si vous êtes contacté pour ouvrir un compte bancaire en France afin de servir d'intermédiaire pour des transactions internationales, il y a de fortes chances pour que vous vous rendiez complice d'escroqueries de grande ampleur, par exemple des opérations de « phishing ». C'est puni de peines d'emprisonnement et d'amende très lourdes.

Est-ce risqué d'acheter des produits sur des sites de vente aux enchères ou de petites annonces ?

Avec un minimum de prudence, vous pouvez faire vos achats sur Internet sereinement. Sur les sites d'enchères en ligne, privilégiez les services de tiers de confiance proposés par les sites eux-mêmes, notamment pour les sommes importantes. Un tiers de confiance protège à la fois le vendeur et l'acheteur ; c'est un intermédiaire qui conserve le paiement de l'acheteur jusqu'à ce que le vendeur ait envoyé l'objet. Avant de le choisir, vérifiez les garanties qu'il offre en cas de litige. Soyez particulièrement méfiant lorsqu'un acheteur vous propose d'utiliser un service de transfert de fonds international (exemple Western Union) ; ces services ne sont pas adaptés à ce type de transactions et doivent de préférence être utilisés entre personnes qui se connaissent. Enfin, méfiez-vous des annonces miraculeuses : les annonces proposant un prix anormalement bas, **notamment pour les véhicules**, sont souvent des escroqueries, même lorsque le vendeur est bien noté par le site de vente. Voyez et essayez toujours un véhicule avant de l'acheter. **De façon générale, rencontrez le vendeur - ou l'acheteur - lorsque le montant de la vente est important.**

(droits réservés)

Est-ce risqué de payer avec mon numéro de carte bancaire sur Internet ?

Ce n'est pas plus risqué que dans des magasins. Effectuez vos achats sur des sites connus, référencés par des magazines sérieux ou que vos amis ont l'habitude d'utiliser. Ainsi vous éviterez les mauvaises surprises.

Qu'est-ce que le « phishing » ?

C'est la « pêche aux victimes ». Des escrocs envoient des messages à un maximum d'internautes (des spams) en se faisant passer pour une banque. Ils invitent les destinataires à mettre à jour leurs comptes bancaires sur Internet en indiquant leur noms et mots de passe. En fait, ils les communiquent aux escrocs qui peuvent alors vider les comptes bancaires. Pour éviter de se faire piéger, quelques conseils simples :

ne jamais communiquer des données sensibles (numéro de carte bancaire, mot de passe) en cliquant sur un lien envoyé par courrier électronique.

toujours partir de la page d'accueil d'un site pour accéder aux autres pages, notamment celles où sont demandées des identifiants.

lors de la consultation de sites sécurisés (sites bancaires, par exemple), s'assurer de l'activation du cryptage des données (l'adresse du site doit commencer par https et non par http).

en cas de doute, prendre contact directement avec l'entreprise concernée (votre banque, votre fournisseur d'accès à l'internet, etc.)

Ai-je le droit d'utiliser le « peer to peer » ?

La plupart des films et musiques téléchargeables en peer-to-peer sont protégés par des droits d'auteur. En dehors des œuvres et logiciels libres de droits, télécharger constitue une contrefaçon, infraction punie de trois ans d'emprisonnement et de 300 000 euros d'amende (article 321-1 du Code pénal). Cela prive les artistes du juste revenu de leur travail et cela nuit à la diversité de la création artistique, les « petits » artistes étant plus pénalisés que les autres. - La **HADOPI** (Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet) a pour mission de protéger le droit d'auteur en rappelant au citoyen ses droits et ses devoirs. A la suite de réponses graduées, elle peut transmettre à la justice les cas des abonnés qui restent négligents, malgré deux recommandations successives.

Ma liberté d'expression me permet-elle de tout écrire ?

La liberté d'expression est un droit fondamental de tout citoyen. Internet est un outil formidable au service de ce droit. Mais cette liberté trouve ses limites dans le respect des autres. La loi définit ces limites. Elle interdit d'inciter à la haine raciale, ethnique, ou religieuse et de faire l'apologie de crimes de guerre. Elle proscrit les propos discriminatoires à raison d'orientations sexuelles ou d'un handicap. Elle interdit d'inciter à l'usage de produits stupéfiants. Le sentiment d'anonymat de l'Internet est trompeur ; les auteurs de tels propos peuvent être identifiés et s'exposent à de lourdes peines.

Protéger son ordinateur

N'installez que les logiciels indispensables à vos activités

Internet est plein de logiciels pratiques ou amusants, à télécharger gratuitement : mini-jeux, utilitaires, etc. Il s'agit parfois de véritables virus ou logiciels espions.

Téléchargez à partir de sites connus

Méfier vous des sites inconnus qui proposent de télécharger des logiciels et des patches. Parfois, ils déguisent des programmes malveillants en leur donnant le nom des applications que vous recherchez. Une fois que vous avez repéré un site de confiance, évitez d'en changer trop souvent.

Installez un antivirus, un pare-feu et un anti-espiogiciels

L'antivirus analyse les contenus de votre ordinateur et ce que vous recevez pour détecter les programmes malveillants. Le pare-feu ou « firewall » vous protège en temps réel des tentatives d'intrusion sur votre ordinateur : certains pirates de l'Internet passent leur temps à chercher des ordinateurs vulnérables, non protégés contre les intrusions, comparables à une maison dont la porte d'entrée serait grande ouverte. L'anti-espiogiciel ou « anti-spyware » analyse les contenus de votre ordinateur pour détecter les programmes espions. Il existe de nombreux antivirus, pare-feu et anti-espiogiciels gratuits ou payants.

Mettez à jour votre système d'exploitation

Le système d'exploitation est le premier programme que vous installez. Les plus connus sont Linux et Windows. Faites des mises à jours régulières, voire automatiques, en les téléchargeant depuis le site de l'éditeur de votre système d'exploitation. Les navigateurs Internet comme Internet Explorer, Firefox, Chrome, Opéra, etc... doivent être également mis à jour afin d'être plus résistants face aux nouvelles menaces.

Méfiez vous des pourriels

Ne répondez jamais à un spam, vous seriez identifié comme une adresse valide. N'ouvrez jamais les pièces jointes des messages provenant d'expéditeurs inconnus. N'ouvrez pas les pièces jointes des messages provenant d'expéditeurs connus, quand vous trouvez le message trop impersonnel (certains virus utilisent le carnet d'adresse de vos amis). Vous pouvez installer un logiciel anti-spam sur votre ordinateur. Signalez les spams que vous recevez à http://www.signal-spam.fr .

Les pouvoirs publics mettent un portail à votre disposition (https://www.internet-signalement.gouv.fr).

En cliquant sur le bouton « SIGNALER », vous pouvez transmettre des signalements de contenus ou de comportements illicites auxquels vous vous seriez retrouvés confrontés au cours de votre utilisation d'Internet.

N'utilisez pas le formulaire dans les cas suivants:

* Si vous avez simplement reçu un pourriel (spam), utilisez le site de Signal Spam: http://www.signal-spam.fr

* Pour un différend commercial ou privé relatif à Internet, contactez le Médiateur du net: http://www.mediateurdunet.fr

- Pour un problème de consommation, de qualité ou de sécurité de produits commerciaux, écrivez à la direction Général de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF) en vous rendant sur: http://www.dgccrf.bercy.gouv.fr/contacts.htm

(images : Gendarmerie Nationale)