



Point Cyber Solidarité

Dossier spécial
Les dangers d'Internet

Touche pas à mon poste !
Ou comment surfer en toute confiance



CL@IR & NET


Quelques chiffres...

- 📄 10 millions de foyers Français sont connectés
- 📄 90% bénéficient du haut débit
- 📄 60% des connexions aboutissent à un achat en ligne
- 📄 2 tiers des 1200 formulaires utilisés par l'Administration sont disponibles sur Internet
- 📄 30% des 6 – 8 ans utilisent déjà le web
- 📄 80% des 13 – 14 ans surfent sur la Toile
- 📄 57% des jeunes de moins de 17 ans utilisent des « chats »
- 📄 62% pensent que c'est un bon outil pour se faire des amis
- 📄 83 % des jeunes surfent seuls
- 📄 17% des foyers connectés sont équipés de logiciels de contrôle parental

Avantage d'Internet

- 📄 On peut y trouver facilement des informations sur tout ce qu'on veut

Inconvénient d'Internet

 d'autres personnes peuvent facilement y trouver des informations sur vous

Les risques sont nombreux

- 📄 Utilisation frauduleuse ou indélicate de vos données personnelles
- 📄 Boîte aux lettres inondée de spams (publicité indésirable)
- 📄 Escroqueries
- 📄 Virus, chevaux de Troie et programmes espions
- 📄 Incitation à la haine raciale, contenus violents
- 📄 Pornographie en accès libre et facile
- 📄 Prédateurs pédophiles

Surfer en confiance, c'est possible

- ☞ Respectez quelques règles élémentaires concernant la confidentialité des données
- ☞ Utilisez un Logiciel antivirus et un pare-feu
- ☞ Utilisez un anti-spam
- ☞ Faites les mises à jour de vos navigateurs et logiciels de messagerie
- ☞ Enseignez à vos enfants les règles de sécurité et utilisez un logiciel de contrôle parental

Règles de confidentialité

- ❏ Ne transmettez des informations personnelles qu'à des sites ayant pignon sur le web, et si possible à des sociétés basées en Europe, ou mieux, en France (en cas de problème, il sera très difficile de trouver le responsable d'un site inconnu en Russie)
- ❏ Si vous achetez en ligne, ne choisissez que des sites qui utilisent une connexion sécurisée (https au début de l'adresse et un petit cadenas verrouillé s'affiche en bas à droite de votre écran)
- ❏ Lorsque vous remplissez des formulaires, vérifiez qu'il existe bien une petite case à cocher permettant de refuser que ces données soient transmises à des tiers
- ❏ Ne fournissez pas d'information si vous ne comprenez pas pourquoi on vous les demande
- ❏ Créez des mots de passe très personnels et difficiles à trouver, mélangeant si possible des lettres majuscules, minuscules et des chiffres
- ❏ Effacez les cookies et les fichiers temporaires de votre navigateur

Malgré toutes ces précautions, le pire est encore possible

Que faire contre les spams ?

- ☞ Installer dans votre machine un logiciel anti-spam (les 2/3 sont payants, de 30 à 50€ environ) mais avant d'être pleinement efficaces, vous devrez effectuer quelques réglages et tests, et avoir de la patience...
- ☞ Les services en ligne se révèlent plus adaptés au grand public car il n'y a aucun réglage à faire. Ils coûtent de 20 à 50€ par an
- ☞ Yahoo et Microsoft ont mis au point leurs propres solutions qui filtrent et vérifient les courriels. L'internaute sera prévenu à chaque fois qu'un message n'aura pu être vérifié (car son serveur est inconnu, par exemple)
- ☞ + d'info → www.spamanti.net -- <http://assiste.free.fr>

SPAM : les bons réflexes

- ☞ Ne communiquez pas votre adresse à n'importe qui
- ☞ Ayez plusieurs adresses électroniques et utilisez chacune de façon spécifique (le commerce en ligne, les lettres d'information, la recherche d'infos)
- ☞ Si vous recevez un SPAM, n'ouvrez pas la pièce jointe, elle peut contenir un virus ou un programme espion
- ☞ Ne cliquez pas sur un lien présent dans un SPAM, il peut vous envoyer vers un faux site officiel
- ☞ Ne répondez jamais à un SPAM, cela indiquerait au spammeur que votre adresse est valide
- ☞ Lorsque vous transférez du courrier à vos différents correspondants, mettez leur adresse en copie cachée (cci) et non en cc comme c'est souvent le cas
- ☞ Lorsque vous vous inscrivez à une lettre d'information, ou si vous répondez à un questionnaire en ligne assurez vous qu'il y a bien une case à cocher vous permettant de refuser que votre adresse soit divulguée à des « partenaires commerciaux »

Attention au phishing

Faux messages , mais vraies arnaques.
C'est parfois grossier mais ça marche !

Nouvelle arnaque en vogue, le phishing consiste à se faire passer pour une banque ou un commerçant en ligne, très connu de préférence, et à solliciter, par courriel, des informations confidentielles, parfois même vos codes d'accès...

Phishing : les bons réflexes

- ☞ Lire les courriels avec attention, ne pas y répondre immédiatement
- ☞ Garder à l'esprit que les entreprises et institutions ne demandent JAMAIS dans un courriel de divulguer des informations confidentielles
- ☞ Quel que soit le prétexte invoqué, ne jamais cliquer sur un lien hypertexte situé dans un message vous demandant de redonner vos coordonnées personnelles
- ☞ Vérifier l'authenticité d'un site en repérant la présence d'indicateurs de sécurisation tels que le petit cadenas en bas à gauche de la page et au début de l'adresse du site les lettres https
- ☞ Ne pas hésiter à appeler votre banque pour vérification si vous recevez un tel message de sa part
- ☞ Utiliser un dispositif anti-spam (vus page 8)
- ☞ Mettre à jour le plus souvent possible vos différents logiciels de sécurité, ainsi que les logiciels vous permettant de surfer et de recevoir votre courrier électronique

Payer en toute sécurité

- 📄 L'utilisation de la carte bancaire sur Internet suscite de fortes inquiétudes. Le système est pourtant sûr.
- 📄 Le principal risque réside dans l'utilisation sur le réseau des numéros de cartes récupérés par ailleurs.
- 📄 En France, le consommateur reste assez bien protégé contre de tels abus, même si, souvent, l'origine de la fraude reste inconnue.

Payer en ligne sans donner son numéro de carte bancaire

- 📄 L'E-carte bleue à usage unique. Son numéro est communiqué par votre banque avant un achat. Il faut posséder une carte visa et son usage peut vous être facturé
- 📄 Le système Id-tronic, mis en place par la Caisse d'Epargne, vous permet d'utiliser un numéro de carte fictif dont le code vous est envoyé par sms et vous permet de valider votre commande
- 📄 Vous pouvez toujours effectuer vos paiements par chèque et par voie postale, en joignant votre bon de commande que vous aurez imprimé.
La plus part des sites marchands le permettent...mais pas tous, hélas

Payer en ligne : les bons réflexes

Sur votre navigateur, désactivez la mémorisation automatique de vos identifiants et mots de passe :

- 📄 Menu Outils, Options Internet, onglet Contenu
Dans les paramètres de saisie semi-automatique, décocher les propositions « Nom d'utilisateur » et « Mots de passe sur les formulaires »
- 📄 Le cas échéant, profitez en pour effacer vos mots de passe déjà enregistrés
- 📄 + d'info sur www.lesclesdelabanque.com

Les virus : une menace bien réelle

- 📄 **Virus** : petits programmes qui s'insinuent dans votre machine pour en modifier le comportement, souvent de façon progressive, et qui finissent par en bloquer le fonctionnement, ou pire, par faire des dégâts matériels et/ou vous faire perdre vos données
- 📄 **Chevaux de Troie** : petits programmes bien plus nombreux que les virus, ils ne servent qu'à introduire le parasite (virus ou autre), visant à créer une faille du système pour en prendre le contrôle à distance, souvent contenus dans des économiseurs d'écrans ou même dans des logiciels connus et très couramment utilisés
- 📄 **Logiciels espions** : une terrible menace pour la confidentialité des données et la protection de la vie privée. Ils peuvent récupérer toutes sortes de données, y compris vos codes confidentiels, n°s de carte bleue, de compte bancaire, adresse électronique, sites visités, habitudes de consommation. Ils enrichissent ensuite des bases de données qui sont utilisées pour vous envoyer des spams. **Plus de 90% des ordinateurs en contiennent !**

Les logiciels anti-virus

- ❏ Aucun ne permet une protection totale, même si les principaux offrent une protection honnête, voire très efficace.
- ❏ Ils recherchent les traces de virus déjà répertoriés dans la base virale établie par l'éditeur, qui est mise à jour dès qu'un code « malicieux » a été découvert, puis sa parade trouvée, puis testée. Or, de nouveaux virus naissent chaque jour et leur durée de vie est de plus en plus courte, certains n'excèdent pas quelques jours.
- ❏ Ces logiciels ne sont pas parfaits : ils sont couramment victimes de failles de sécurité.

Le pare-feu : indispensable

- ☞ Filtre les entrées et les sorties de données
- ☞ Lorsqu'il détecte une intrusion ou une sortie suspecte, il vous avertit immédiatement
- ☞ Vous pouvez soit autoriser l'action, soit la bloquer
- ☞ Il faut le configurer et passer par une période d'adaptation afin qu'il finisse par reconnaître les bonnes et les mauvaises entrées et sorties

Internaute, vous êtes le maillon faible

- ☞ Une baisse de vigilance ou une erreur de manipulation est toujours possible (personne n'est parfait)
- ☞ Le réglage des différents logiciels de sécurité peut être parfois compliqué, or, pour être vraiment efficaces, ces logiciels doivent être correctement configurés
- ☞ Le phishing est fait pour vous induire en erreur et il faut parfois être extrêmement méfiant pour ne pas tomber dans le piège

Parents, restez vigilants

- Internet est avant tout un formidable outil d'apprentissage, mais on y trouve aussi des escrocs, des propagandistes de tous ordres, de la pornographie à foison, et parfois des pédophiles qui tentent de piéger des mineurs
- Ce média fait maintenant partie intégrante des loisirs des jeunes. Plutôt que de leur en interdire l'accès, il faut leur apprendre à en dépister les dangers
- Il existe des outils pour filtrer l'accès au web mais ils ne dispensent pas d'un accompagnement actif des parents

Les logiciels de contrôle parental

- ☞ Très utiles, ils filtrent les contenus qui parviennent à l'ordinateur et peuvent limiter ou bloquer certaines activités préalablement interdites, comme l'utilisation de la messagerie instantanée par exemple.
- ☞ On doit prendre le temps de faire les réglages nécessaires pour obtenir une protection efficace

ControlKids – LogProtect – sont les plus connus...

Enfants : les règles essentielles

- ❏ Ne donne jamais d'informations personnelles sur toi et ta famille (nom, adresse, nom de ton école, n°de téléphone, âge, les endroits où tu aimes jouer...)
- ❏ Ne rencontre jamais seul une personne que tu as connue sur le web
- ❏ Dès que tu vois quelque chose qui te met mal à l'aise, déconnecte toi et parles en à tes parents
- ❏ Sauf si tes parents sont présents auprès de toi pour t'aider à le faire, n'achète jamais rien sur Internet

Parents : les règles essentielles

- ☞ Si vous tombez sur un site dont le contenu est illicite (pornographie infantile, incitation à la haine raciale...) signalez-le au site gouvernemental de protection des mineurs : www.internet-mineurs.gouv ou au site www.pointdecontact.net
- ☞ Incitez vos enfants à choisir un pseudonyme ou une adresse de messagerie qui ne révèle rien de personnel (âge, sexe, hobbies, école fréquentée, lieu de résidence...)
- ☞ Dialoguez souvent avec eux, afin de leur apprendre, sans dramatiser, l'utilisation d'internet et à en détecter les pièges

Les différents âges du net

- 📄 **De 2 à 4 ans : les premiers pas** - Sur les genoux de leurs parents. Les risques sont très faibles.
- 📄 **De 5 à 6 ans : la découverte** - Votre enfant montre sa volonté de surfer seul, il s'est approprié cet univers qu'il ne trouve pas dangereux. Un logiciel de contrôle parental est indispensable.
- 📄 **De 7 à 8 ans : les premiers tests** - Il risque de s'aventurer sur des sites ou dans des salons réservés aux adultes ou dont le contenu est illicite. Vous devez lui apprendre les règles de sécurité. Le filtrage du logiciel de contrôle doit être plus précis.
- 📄 **De 9 à 12 ans : la découverte des interdits** - Il peut tomber sur des sites au contenu dangereux (pornographie, fabrication de bombe artisanale, propos racistes...) Discutez avec lui afin qu'il comprenne mieux les dangers de certains sites. Protégez votre logiciel de contrôle parental par un mot de passe.
- 📄 **De 13 à 17 ans : la maîtrise** - A cet âge, les jeunes ont le sentiment (souvent avéré) d'en savoir plus sur Internet que leurs parents. Consultez les rapports d'activité de votre logiciel de contrôle, afin de surveiller les connexions. Choisissez un mot de passe plus difficile à découvrir que le nom du chien ou de votre acteur préféré !

Quelques sites utiles

📄 Infos sur la sécurité + logiciels à télécharger :
inoculer.com , secuser.com
telecharger.com , protegetonordi.com
www.lesclesdelabanque.com
www.cnil.fr (dossier complet sur le spam)
www.spamanti.net -- <http://assiste.free.fr>

📄 Protection des mineurs :

cnil.fr/juniors , droitdunet.fr , educaunet.org/vraifaux ,
mrccd.com

<https://www.internet-mineurs.gouv.fr> Ce site permet à toute personne ayant connaissance d'un site pédophile d'en faire le signalement aux autorités en remplissant, anonymement ou non, un questionnaire. Les informations sont ensuite transmises à un officier de police judiciaire affecté à la vérification et à la localisation des sites pédophiles.