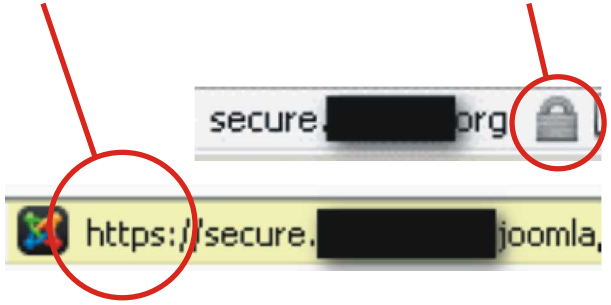
3 - LE PAIEMENT SUR INTERNET

Si plus de la moitié des internautes n'ont jamais acheté ou initié une commande sur Internet à cause du problème de la sécurité des paiements en ligne, d'autres ignorent certaines règles fondamentales et deviennent les proies des cyber-escrocs.

S'il est impossible de supprimer totalement les risques, il est facile de les réduire. Pour ce faire, il suffit de respecter quelques règles simples et de se montrer un minimum vigilant :

Savoir repérer les sites sécurisés. Le moyen le plus sûr de reconnaître un site sécurisé est l'adresse des pages. Toutes les adresses sécurisées commencent par : ***https: ...*** *(**s** pour sécurisé) et sont suivies d'un cadenas.*



Ne fournir son numéro de carte que sur des sites sécurisés.

N'effectuer des achats que sur des sites connus, existant depuis longtemps et bénéficiant d'une bonne réputation, adhérents à la « net-étiquette ».

Eviter les achats à l'étranger, les recours étant très difficiles dans ce cas. Si vous devez absolument effectuer ce type d'achat, essayez de payer à réception et dans tous les cas soyez extrêmement prudents.

Adhérer à un système de paiement par « e-carte ».
Pour effectuer des paiements sécurisés sur Internet, les banques mettent à la disposition de leurs clients des « e-cartes bleues ». A chaque transaction, vous obtenez un numéro de carte à usage unique fourni par votre banque.

4 - QUELQUES ADRESSES DE SITES POUR DES INFORMATIONS COMPLÉMENTAIRES

http://www.internetsanscrainte.fr/

http://www.foruminternet.org/

http://ddm.gouv.fr/surfezintelligent/

http://www.securite-informatique.gouv.fr/

Plaquette réalisée par le groupement de gendarmerie de Tarn-et-Garonne avec la collaboration du bureau de la communication interministérielle de la préfecture de Tarn-et-Garonne
mars 2008

Gendarmerie nationale

Internet & SÉCURITÉ

Internet connaît ces dernières années un développement spectaculaire.

Dans la vie quotidienne, Internet, c'est d'abord plus de liberté pour les individus, qui se connectent chaque jour par millions, par-delà les frontières.

Mais Internet, c'est aussi **des menaces nouvelles pour la sécurité :** *escroquerie, faux mails, vols de numéros de carte bancaire, pédopornographie, trafic de stupéfiants, atteinte aux réseaux, intimidations...*

La prévention s'avère être un outil indispensable pour faire face à cette menace qui appartient au domaine de l'immatériel.

1 - LES JEUNES INTERNAUTES ET LA CYBERINTIMIDATION

Internet a créé un univers de nouvelles formes de communications pour les jeunes. Ils peuvent utiliser les courriels, sites Web, bavardoirs («chat» en anglais) ou messageries pour rester en contact avec leurs amis ou s'en faire de nouveaux. Souvent laissés sans surveillance, certains jeunes deviennent les victimes d'intimidation, de harcèlement, de travestissement d'identité et de diffamation.

Le rôle des parents :

Renseignez-vous le mieux possible sur Internet et sur l'utilisation qu'en font vos enfants. Discutez avec eux des sites qu'ils fréquentent et des activités qu'ils pratiquent en ligne. Soyez au courant de ce qu'ils affichent sur des sites Web ou sur leurs propres pages personnelles (blog).

Formez vos enfants à l'utilisation d'Internet en leur exposant les dangers. L'instauration d'un code de conduite peut s'avérer une bonne idée. Les jeunes sont beaucoup moins enclins à se livrer aux activités auxquelles les parents établissent des règles précises.

Apprenez à vos enfants à être responsables lorsqu'ils visitent des sites Internet :

Ne pas donner d'information personnelle à son sujet ou au sujet de la famille

Ne pas prendre de texte, d'image ou de son d'un site Web sans permission

Ne pas envoyer de message insultant, grossier ou menaçant à qui que ce soit

Ne jamais faire un achat en ligne sans permission

Réagissez lorsque votre enfant est victime d'intimidation en ligne. Soyez attentifs aux signes de détresse révélateurs d'une possible intimidation.
Ex : aller à l'école à contre coeur ou refuser d'utiliser un ordinateur.

Rapportez tous les cas de harcèlements en ligne ou de menaces physiques à la police ou la Gendarmerie. N'effacez rien et soyez réactifs.

Le rôle des enfants et adolescents :

Protégez vos coordonnées personnelles (téléphone cellulaire, messagerie) en les communiquant uniquement à des personnes connues.

Prenez les mesures suivantes en cas d'intimidation en ligne :

Prévenez un adulte de confiance (parents, enseignant, frère, soeur, grand-parent...)

Quittez immédiatement l'environnement ou l'activité en ligne où a lieu l'intimidation (bavardoir, forum, jeux, messagerie, etc)

*Bloquez les messages de courriel ou de messagerie de la personne qui harcèle et **ne jamais y répondre.** Vous devez vous contenter de relever les propriétés du mail, vous assurer de ne pas effacer les traces et de prévenir au plus tôt les services de gendarmerie*

Le happy slapping, qui consiste à filmer les violences entre adolescents (bien souvent à l'aide d'un téléphone portable) et à les diffuser par MMS ou sur internet, tombe sous les coups des articles du code pénal :

- 222-1 à 222-14 et 222-23 à 222-31 qui répriment les atteintes volontaires à l'intégrité physique des personnes (poursuite du ou des auteurs des violences)

- 222-33-3 qui punit l'enregistrement et la diffusion d'infractions de violences (permet de poursuivre celui qui filme l'agression et en publie les images)

2 - QUELQUES CONSEILS POUR ETABLIR DES RELATIONS SECURITAIRES SUR INTERNET

Voici quelques conseils pratiques pour vous aider à naviguer en sécurité sur le net :

Employez des noms d'utilisateur et des mots de passe différents pour vos divers services. Choisissez de préférence des noms qui ne vous identifient pas.

Il est indispensable pour un internaute d'avoir un anti-virus (mis à jour), un anti-spam (blocage « pourriels » et messages) et un pare-feu.

Si vous êtes abonné à un service de clavardage («chat») ou de rencontre en ligne, renseignez-vous sur le service avant de vous inscrire.

Ne donnez jamais votre adresse domiciliaire à quelqu'un que vous rencontrez en ligne.

N'affichez pas de photographies de vous ou de votre maison sur internet. Si vous voulez échanger des photographies, ne le faites qu'avec des personnes que vous connaissez bien. Envoyez-leur directement en les annexant à votre message.

Si vous avez une page Web personnelle, sélectionnez avec soin les renseignements personnels que vous allez y afficher. Demandez-vous si l'information contenue sur votre site pourrait être utilisée contre vous.

Si vous recevez un courriel, une photographie ou un enregistrement offensant ou menaçant, transmettez-le avec ses propriétés à votre fournisseur d'accès Internet pour qu'il fasse enquête à l'adresse suivante : abuse@... suivi du fournisseur d'accès internet. Toujours en prenant soin de ne pas effacer les traces, prenez contact également avec la gendarmerie.

Si vous souhaitez rencontrer réellement une personne dont vous avez fait connaissance sur Internet, il faut savoir, que sans tomber dans la paranoïa, des précautions s'imposent :
- Prenez des mesures pour que votre rencontre se déroule en toute sécurité.
- Même si vous croyez connaître votre ami et que vous pensez qu'il n'est pas « dangereux », il s'agit quand même d'un étranger et vous devriez le traiter ainsi.
- Avant de partir à votre rendez-vous, dites à un ami qui vous rencontrez, à quel endroit a lieu la rencontre et à quelle heure vous prévoyez rentrer.