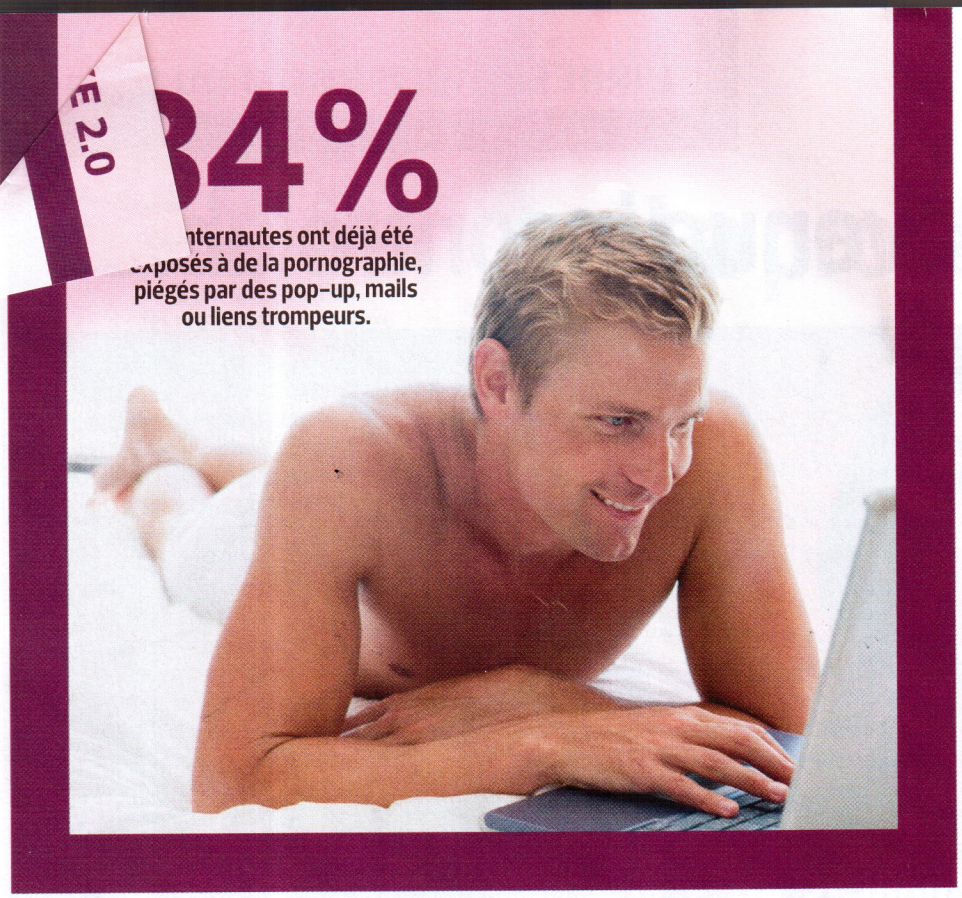


*SOURCE : ONLINEMBA, 2010

Fans de cybersexe ou simples curieux, gare aux arnaques !

Abonnements sauvages, prélèvements abusifs, chantage à la webcam... les amateurs d'expériences coquines sont une proie facile sur Internet. Et les escroqueries sont désormais bien rodées.

Je me suis fait avoir en cliquant sur un site porno". Tout commence en général par une photo sexy et une première prise de contact par mail ou par messagerie instantanée : "Jessica69 a flashé sur votre profil ! Cliquez ici pour voir son message". Plus sournoise, la proposition d'amis sur Facebook. Une certaine Monica Legrand, que vous ne connaissez pas, veut faire partie de votre cercle. Il arrive qu'elle n'ait même pas besoin de vous démarcher directement : des profils de filles et de garçons visiblement portés sur le sexe arrivent de plus en plus souvent de manière automatique dans les suggestions d'amis faites par le réseau social. Selon un porte-parole de Facebook France, il suffit de pas grand-chose : "Toute personne qui remonte dans les suggestions a un point commun avec vous. Il peut s'agir de votre emploi, votre ville, d'un autre ami...

Vous avez cliqué ? Vous êtes ferré. Plusieurs scénarios sont alors possibles. Premier cas, vous êtes redirigé sur un site de charme où il faut s'inscrire "gratuitement" pour poursuivre. À la demande du site, qui dit vouloir vérifier que vous êtes majeur, vous acceptez de saisir vos coordonnées bancaires. Les ennuis commencent. Comme pour Benoît, 25 ans. "Stupeur quand je découvre que j'ai été prélevé de 1 euro, pour 10 minutes d'accès. Dans les conditions de vente, j'apprends en plus que je dois me désabonner pour éviter un prélèvement de 89 euros. Et je dois le faire pendant mes 10 minutes d'essai. Et trouver le bon lien pour se désabonner, courage !", raconte-t-il désabusé. Ce genre de pratiques est en infraction avec la loi. "Le client doit savoir clairement sur quoi il s'engage", souligne Murielle Isabelle-Cahen, avocate spécialisée dans les nouvelles technologies. De plus, selon le Code civil, les conditions contractuelles ne peuvent être en contradiction avec l'offre publicitaire. La solution pour vous sortir de cette situation : faire opposition au prélèvement et vous désabonner voire porter plainte.

Un code pour un strip-tease. Tout aussi efficace, l'arnaque aux codes AlloPass. Elle pullule sur les sites de rencontres hot de seconde zone. Pendant un tchat avec une interlocutrice très entreprenante, on vous propose : "Pour que je te fasse un strip-tease, juste pour toi, par webcam, envoie-moi un code AlloPass". Il s'agit alors de vous procurer un code en envoyant un SMS ou en appelant un numéro surtaxé.

Ce code, c'est comme une "autorisation" d'utiliser la somme d'argent demandée pour le strip-tease. Une fois obtenu, vous le fournissez par tchat pour accéder à la webcam... Sauf que rien ne se passe. On vous invite donc à réessayer en vous demandant un nouveau code (et cela jusqu'à vingt fois de suite parfois !), sous prétexte d'un problème technique... Lorsque vous abandonnez, par lassitude ou après avoir compris la supercherie, la communication est rompue. Les sommes sont débitées sur votre facture téléphonique. Il ne s'agit que de quelques euros, parfois plusieurs dizaines dans le pire des cas. Pourquoi porter plainte pour des montants relativement faibles ? D'autant que vous n'avez fourni que des codes, et de plus, de votre plein gré Une escroquerie difficile à prouver.

Plus d'un million et demi d'euros: c'est le montant estimé des arnaques menées par une organisation dirigée par deux cybercriminels arrêtés fin juin à Abidjan (Côte d'Ivoire). Le FBI et la Plateforme de lutte contre la cybercriminalité poursuivent leurs recherches pour démanteler leur vaste réseau. Celui-ci s'est principalement spécialisé dans les chantages à la webcam, "l'arnaque nigériane", en recrudescence en 2012 selon l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

Le chantage à la hot vidéo. Le principe est simple : faire chanter une future victime – très souvent un homme –avec une vidéo compromettante. Pour la ferrer, le maître chanteur la repère d'abord sur un site de charme. Il se fait passer pour une femme et l'aguiche via la messagerie du site. Après un tchat suffisamment long pour mettre notre homme en confiance, il l'invite à se connecter à Skype pour poursuivre la conversation en vidéo. "Les profils sont faux, les images préenregistrées et les conversations alimentées par des garçons de 18 ans basés en Afrique", dénonce Camilla Pariso, de l'Association des Victimes d'escroqueries à la nigériane.

La proie se croît en direct avec une sublime jeune fille. En réalité, elle regarde une vidéo toute prête diffusée par les voyous et dans laquelle la jeune fille sublime lui demande de se dénuder, voire plus. Evidemment, tout ce que fait la victime devant sa webcam est minutieusement enregistré et sera utilisé contre elle. La menace est enfantine : payer sinon la vidéo compromettante est diffusée sur le Net... Il arrive que les maîtres chanteurs mettent effectivement la vidéo sur YouTube ou Facebook. "Notre association peut se charger de demander à YouTube de la supprimer, précise Camilla Pariso. Mais nous avons plus de mal à obtenir de l'aide de la part de Facebook". Reste que le principal problème des victimes est d'être pris au sérieux par l'entourage et les autorités. Et de surmonter la gêne d'avoir été piégé et... Difficile à assumer. ■ AM ET FB

Dix conseils pour surfer sur des sites "de charme" en toute sécurité

1. Utilisez une adresse mail spéciale

En visitant les sites chauds, on est souvent amené à laisser un mail pour accéder à plus de services. Évitez de donner une adresse mail qui vous sert au quotidien. Votre boîte aux lettres sera inéluctablement spammée par des offres promotionnelles ou des messages douteux. Il serait aussi fâcheux que vos proches tombent sur ces racolages par mégarde. Créez plutôt une adresse (Yahoo, Gmail ou Outlook par exemple) que vous n'utiliserez que pour ces sites. Ne donnez pas non plus votre vrai nom, mais un pseudo. Relevez le courrier de cette adresse par webmail et non avec un logiciel.

2. Séparez vie publique et vie privée

Certains sites Web proposent le célèbre bouton Facebook pour accélérer votre inscription. En un clic, le site visité reprend tous les paramètres enregistrés pour le réseau social et connaît donc presque tout de vous, dont vos amis. Et, peut même, pourquoi pas, publier sur votre mur. Alors, restez prudent et prenez le temps de remplir le formulaire d'inscription du site visité, et ne cliquez surtout pas sur son bouton Facebook.

3. Surfez sans laisser de traces

Tous les navigateurs Web disposent d'un mode de "navigation privée". Même si ce mode n'est pas fiable à 100 % (il reste toujours des traces de fichiers téléchargés sur votre disque dur), il vous évitera de vider votre historique à tout bout de champ, ou de laisser traîner des cookies par mégarde...

4. Paramétrez le contrôle parental

Quel que soit votre fournisseur d'accès à Internet (Free, Orange, SFR, Bouygues, Numericable, etc.), tous proposent un outil de contrôle parental. À vous de ne pas oublier de le paramétrer afin que vos enfants n'accèdent pas aux mêmes sites Web que vous.

5. Vérifiez le niveau de confiance du site

Avant d'aller surfer sur des sites coquins, dotez votre navigateur d'une extension WOT, par exemple. Un petit indicateur vous montrera si le site visité a la réputation d'être sûr ou pas. Le niveau de fiabilité est renseigné par les utilisateurs eux-mêmes.

6. Maintenez votre antivirus à jour

Vous restez seul maître de ce que vous décidez d'installer sur votre PC. Néanmoins, un logiciel antivirus, bien à jour, est un bon moyen de vous assurer que vous n'avez pas téléchargé un peu vite – ou à votre insu – un outil douteux (cheval de Troie, virus, malware, adware). Maintenez également à jour le système d'exploitation de votre machine. Tout comme votre navigateur Web et le lecteur Flash, très souvent utilisé comme porte d'entrée par les virus. Enfin, équipez votre navigateur de l'extension AdBlock. Elle empêchera l'affichage intempestif des publicités qui abondent sur les sites de charme et peuvent dissimuler des codes malveillants.

7. Créez une session Windows dédiée

La plupart du temps, on utilise une session Windows où l'on est administrateur. On dispose du coup de tous les droits de modification ou de paramétrage du système... et les virus aussi ! Mieux vaut donc utiliser une session Windows en tant qu'utilisateur standard. Ainsi, même si l'on est victime d'un logiciel malveillant, les dommages seront moindres. C'est aussi un bon moyen de garder secrètes vos activités sur des sites coquins (à condition de verrouiller cette session par un mot de passe).

8. Utilisez un moyen de paiement sécurisé

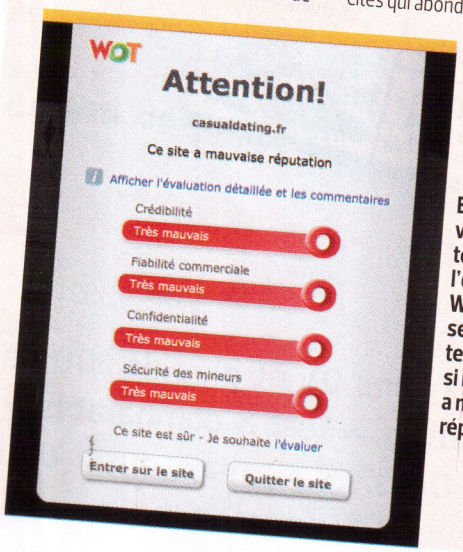
On n'est jamais à l'abri d'une arnaque, surtout sur des sites étrangers. Si vous souhaitez accéder à un service payant, n'utilisez pas votre carte bancaire. Faites plutôt appel à une e-Carte bleue ou carte de paiement virtuelle. Celle-ci est à usage unique et ne pourra être débitée qu'une seule fois pour un montant que vous pouvez préciser. Un bon moyen de ne pas être abonné de force à un service.

9. Lisez les conditions générales de vente

Souvent longues et indigestes... Néanmoins, leur lecture vous apportera des précisions quant à d'éventuels frais d'accès à des services. Même si le moment n'est pas des plus opportuns pour les parcourir, n'omettez jamais cette étape avant de cliquer sur le bouton J'accepte les conditions. Cela vous évitera les mauvaises surprises sur votre facture téléphonique ou sur votre compte bancaire.

10. Équipez votre PC d'un bouton Panic

C'est plutôt gênant d'être pris en flagrant délit de surf sur un site de charme alors que l'on est censé travailler. Dotez votre PC d'un bouton Panic : un petit programme qui, sitôt que vous pressez une touche sur le clavier de l'ordi (celle de votre choix), ferme toutes les fenêtres ouvertes et nettoie l'historique de navigation. Vous pouvez en télécharger un ici : http://goo.gl/10Pjpu



En équipant votre navigateur Web de l'extension WOT, vous serez immédiatement averti si le site visité a mauvaise réputation.

MONKEY BUSINESS IMAGES/ISTOCKPHOTO