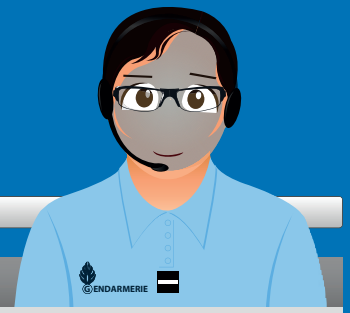


GENDARMERIE › Internet › Sécurité

QUESTIONS / RÉPONSES

Je viens de recevoir un e-mail bizarre, d'une personne que je ne connais pas, se disant d'origine étrangère et me demandant de l'aider. Que dois-je faire ?

Vous ne devez pas répondre, ni accuser réception. Ce type de message cache une tentative d'escroquerie.

J'ai voulu acheter un objet sur un site de vente aux enchères sur Internet. Après quelques échanges par mail avec le vendeur, je lui ai envoyé un virement de la moitié du prix. Je devais recevoir la marchandise dans les huit jours, mais je n'ai jamais rien reçu.

Vous avez été victime d'une escroquerie à la « fausse vente ». Vous devez signaler les faits au site marchand, et déposer une plainte au commissariat ou à la gendarmerie le plus proche de votre domicile, même si le vendeur est situé à l'étranger. Cette plainte permettra d'ouvrir une enquête.

En cas de plainte, des frais me seront-ils facturés ?

Le dépôt de plainte est une formalité totalement gratuite.

J'ai été victime d'une utilisation frauduleuse de mon numéro de carte de paiement sur Internet. Est-ce à moi de supporter le montant du préjudice?

Si vous avez signalé le problème à votre banque, elle vous a demandé un récépissé de dépôt de plainte - Si vous avez fourni ce document, votre banque doit recréditer votre compte du montant litigieux dans le délai d'un mois.

www.gendarmerie.interieur.gouv.fr

Le sentiment de culpabilité est fréquent chez les victimes d'escroquerie sur Internet. Mais les responsables sont les auteurs de ces infractions, déterminés à obtenir par tout moyen ce qu'ils veulent.

Si vous êtes victimes d'une escroquerie sur Internet :

- ➥ Appelez en priorité votre banque pour le signaler.
- ➥ Déposez une plainte à votre brigade de gendarmerie (si vous ne pouvez pas vous déplacer, les gendarmes peuvent prendre votre plainte à votre domicile).

CONTACTS

Pour aller plus loin ou obtenir de l'information :

www.gendarmerie.interieur.gouv.fr

Pour signaler :

- des contenus illégaux sur Internet : https://www.internet-signalement.gouv.fr
- des courriels ou sites d'escroqueries : https://www.internet-signalement.gouv.fr ou 0811 02 02 17
- des spams : https://www.signal-spam.fr/
- des sites de phishing : http://www.pishing-initiative.com/

EN CAS D'URGENCE, COMPOSEZ LE 17

Votre point de contact local ?

Selon la gravité de votre incident, ce point de contact local sera en mesure de faire intervenir des enquêteurs spécialisés en cybercriminalité.

COORDONNÉES DE VOTRE CONTACT LOCAL

Conception et impression : Service de diffusion de la gendarmerie à Limoges - SDG 15-35014-1 000

GENDARMERIE NATIONALE

INTERNET EN TOUTE SÉCURITÉ

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR
Gendarmerie nationale

LES PRINCIPAUX DANGERS D'INTERNET

L'HAMEÇONNAGE :

Vous pensez recevoir un courriel d'une société ou d'une administration notoirement connue (banque, opérateur téléphonique, impôt, caisse d'allocations familiales...) qui vous invite à fournir des informations confidentielles (code d'accès, n° de carte bancaire...). Les pirates récupèrent alors ces données et les utilisent à leur profit.

LES LOGICIELS MALVEILLANTS

Lorsque vous ouvrez un mail ou que vous accédez à un site web, votre ordinateur peut être infecté par un virus. Ce dernier permet alors d'intercepter vos données confidentielles (identifiants, codes secrets, n° de carte bancaire, cryptogramme visuel...).

LES ESCROQUERIES

- Un courriel vous informe que vous avez gagné un cadeau mais on vous demande de payer des frais de livraison et de communiquer vos codes bancaires. Vous ne verrez jamais les cadeaux.
- Un courriel vous informe que vous avez gagné une somme importante à la loterie mais que vous devez envoyer de l'argent par mandat international pour les frais de transfert (Western Union par exemple). Vous ne verrez jamais la somme promise.
- Un courriel vous informe qu'une personne a besoin de votre aide (maladie, handicap, problèmes financiers), elle vous demande de lui envoyer de l'argent à l'étranger par mandat international.

POUR VOTRE SÉCURITÉ nos conseils

PROTÉGER VOTRE ORDINATEUR

- Installez un logiciel anti-virus, un logiciel anti-espion et un pare-feu régulièrement mis à jour.

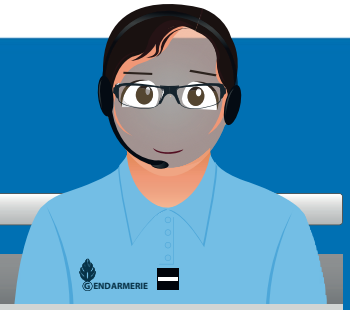
ÉVITER LES ESCROQUERIES

- Méfiez-vous des gains trop faciles, des cadeaux, des bonnes affaires et des demandes d'argent faisant appel à votre compassion.
- Méfiez-vous des demandes urgentes d'informations personnelles, surtout lorsqu'elles contiennent des fautes d'orthographe.
- N'ouvrez pas les courriels si vous avez des doutes sur leur provenance.
- Ne cliquez pas sur les liens reçus par courriel surtout si on vous demande vos coordonnées bancaires.

SÉCURISER VOS ACHATS EN LIGNE

- Réalisez vos achats uniquement sur les sites de confiance dont l'adresse, au moment de la transaction, commence par «https».

- L'apparition d'icônes en bas du navigateur (cadenas et clés) est un gage de sécurité.



GENDARMERIE › Internet › Sécurité

QUESTIONS / RÉPONSES

Je viens de recevoir un e-mail bizarre, d'une personne que je ne connais pas, se disant d'origine étrangère et me demandant de l'aider. Que dois-je faire ?

Vous ne devez pas répondre, ni accuser réception. Ce type de message cache une tentative d'escroquerie.

J'ai voulu acheter un objet sur un site de vente aux enchères sur Internet. Après quelques échanges par mail avec le vendeur, je lui ai envoyé un virement de la moitié du prix. Je devais recevoir la marchandise dans les huit jours, mais je n'ai jamais rien reçu.

Vous avez été victime d'une escroquerie à la « fausse vente ». Vous devez signaler les faits au site marchand, et déposer une plainte au commissariat ou à la gendarmerie le plus proche de votre domicile, même si le vendeur est situé à l'étranger. Cette plainte permettra d'ouvrir une enquête.

En cas de plainte, des frais me seront-ils facturés ?

Le dépôt de plainte est une formalité totalement gratuite.

J'ai été victime d'une utilisation frauduleuse de mon numéro de carte de paiement sur Internet. Est-ce à moi de supporter le montant du préjudice?

Si vous avez signalé le problème à votre banque, elle vous a demandé un récépissé de dépôt de plainte - Si vous avez fourni ce document, votre banque doit recréditer votre compte du montant litigieux dans le délai d'un mois.

www.gendarmerie.interieur.gouv.fr

Le sentiment de culpabilité est fréquent chez les victimes d'escroquerie sur Internet. Mais les responsables sont les auteurs de ces infractions, déterminés à obtenir par tout moyen ce qui veulent.

Si vous êtes victimes d'une escroquerie sur Internet :

- ➥ Apelez en priorité votre banque pour le signaler.
- ➥ Déposez une plainte à votre brigade de gendarmerie (si vous ne pouvez pa vous déplacer, les gendarmes peuvent prendre votre plainte à votre domicile).

CONTACTS

Pour aller plus loin ou obtenir de l'information :

www.gendarmerie.interieur.gouv.fr

Pour signaler :

- des contenus illégaux sur Internet : https://www.internet-signalement.gouv.fr
- des courriels ou sites d'escroqueries : https://www.internet-signalement.gouv.fr ou 0811 02 02 17
- des spams : https://www.signal-spam.fr/
- des sites de phishing : http://www.pishing-initiative.com/

EN CAS D'URGENCE, COMPOSEZ LE 17

Votre point de contact local ?

Selon la gravité de votre incident, ce point de contact local sera en mesure de faire intervenir des enquêteurs spécialisés en cybercriminalité.

COORDONNÉES DE VOTRE CONTACT LOCAL

Conception et impression : Service de diffusion de la gendarmerie à Limoges - SDG 15-34577-5 000

GENDARMERIE NATIONALE

LA GENDARMERIE S'ENGAGE

LES SÉNIORS FACE AUX DANGERS D'INTERNET

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Gendarmerie nationale

LES PRINCIPAUX DANGERS D'INTERNET

L'HAMEÇONNAGE :

Vous pensez recevoir un courriel d'une société ou d'une administration notoirement connue (banque, opérateur téléphonique, impôt, caisse d'allocations familiales...) qui vous invite à fournir des informations confidentielles (code d'accès, n° de carte bancaire...). Les pirates récupérent alors ces données et les utilisent à leur profit.

LES LOGICIELS MALVEILLANTS

Lorsque vous ouvrez un mail ou que vous accédez à un site web, votre ordinateur peut être infecté par un virus. Ce dernier permet alors d'intercepter vos données confidentielles (identifiants, codes secrets, n° de carte bancaire, cryptogramme visuel...).

LES ESCROQUERIES

- Un courriel vous informe que vous avez gagné un cadeau mais on vous demande de payer des frais de livraison et de communiquer vos codes bancaires. Vous ne verrez jamais les cadeaux.
- Un courriel vous informe que vous avez gagné une somme importante à la loterie mais que vous devez envoyer de l'argent par mandat international pour les frais de transfert (Western Union par exemple). Vous ne verrez jamais la somme promise.
- Un courriel vous informe qu'une personne a besoin de votre aide (maladie, handicap, problèmes financiers), elle vous demande de lui envoyer de l'argent à l'étranger par mandat international.

POUR VOTRE SÉCURITÉ nos conseils

PROTÉGER VOTRE ORDINATEUR

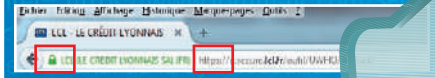
- Installez un logiciel anti-virus, un logiciel anti-espion et un pare-feu régulièrement mis à jour.

ÉVITER LES ESCROQUERIES

- Méfiez-vous des gains trop faciles, des cadeaux, des bonnes affaires et des demandes d'argent faisant appel à votre compassion.
- Méfiez-vous des demandes urgentes d'informations personnelles, surtout lorsqu'elles contiennent des fautes d'orthographe.
- N'ouvrez pas les courriels si vous avez des doutes sur leur provenance.
- Ne cliquez pas sur les liens reçus par courriel surtout si on vous demande vos coordonnées bancaires.

SÉCURISER VOS ACHATS EN LIGNE

- Réalisez vos achats uniquement sur les sites de confiance dont l'adresse, au moment de la transaction, commence par «https».



- L'apparition d'icones en bas du navigateur (cadenas et clés) est un gage de sécurité.

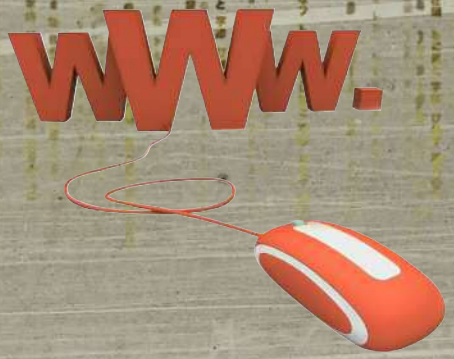
fotolia©Scott Hancock

Internet est, sans conteste, le nouvel instrument de communication et d'information; il fait partie intégrante de notre quotidien.

Espace de liberté par excellence, il permet de communiquer avec le monde entier et ne connait aucune frontière, ni géographique, ni juridique.

Malheureusement, il n'est pas sans conséquences sur le développement des jeunes qui comptent parmi les utilisateurs les plus actifs et les plus curieux du réseau.

Votre rôle de parents ou d'éducateur est déterminant pour la sécurité des enfants.



fotolia©Franck Boston

Sirpa gendarmerie©ADC F. Balsamo

Une interrogation ??

Consultez le site :
http://www.internetsanscrainte.fr/

Vous désirez signaler une infraction ?
https://www.internet-signalement.gouv.fr

Cette plaquette est réalisée par la division de lutte contre la cybercriminalité de Rosny-sous-bois

avec l'aide de l'association
181 avenue Victor Hugo
75116 Paris
www.actioninnocence.org

SIRPA Gendarmerie 2011-725

GENDARMERIE NATIONALE

Guide à l'usage

des PARENTS et ÉDUCATEURS

pour un **internet** plus sûr

01 Rôle d'accompagnement et de conseil des parents ou des éducateurs


fotolia©Goodluz

■ Éduquez vos enfants à la prudence sur l'Internet : ne jamais donner d'informations personnelles, ne pas répondre à un message choquant, quitter rapidement le site qui les met mal à l'aise, ne pas organiser de rendez-vous avec une personne rencontrée dans un forum de discussion.

■ Les jeunes enfants de moins de 10 ans ne devraient pas surfer seuls. Pour les plus grands, ne les laissez pas surfer avec la porte de la chambre fermée.

■ Répétez que dialoguer sur le web avec quelqu'un depuis six mois ne signifie pas qu'on le connait.

■ Répétez leurs que sur un chat, un Blog, il ne doit donner aucun renseignement personnel (pas de numéro de téléphone, d'adresses de domicile ou d'école, d'emploi du temps, ni d'âge, ni d'adresses favorites, encore moins son mot de passe, voire une photo s'il est jeune...)

■ Rappelez la stratégie de la double adresse : une adresse personnelle que l'on garde secrète pour ses amis ou sa famille, et une autre qui ne donne aucune indication (par exemple : mickey731@hotmail.com) que l'on peut indiquer si besoin.

■ Développez son esprit critique : non, tout n'est pas bon à prendre sur Internet ! Un texte publié n'est pas plus qu'ailleurs « La Vérité ». S'il est surpris par une information sur le web, qu'il en parle à un adulte de confiance.

■ Responsabilisez-le s'il tombe par mégarde sur une image violente, un site douteux, des propos racistes, il doit le signaler à ses parents. Quant à vous parents, vous devez faire un signalement sur le site ad hoc (*https://www.internet-signalement.gouv.fr*).

■ Expliquez clairement ce qu'est le droit d'auteur et que le téléchargement illicite est punissable,

■ Profitez de l'internet en famille : organisez vos vacances, choisissez un film, préparez un exposé, envoyez un mail aux grands-parents, créez une bibliothèque familiale des bons sites web.

02 Lieu pour placer l'ordinateur

■ L'ordinateur devrait toujours être placé dans une pièce commune (salle de séjour, bureau, lieu de passage) notamment quand on a des enfants en bas âge. En effet, installer l'ordinateur dans une pièce commune permet de favoriser les échanges et vos enfants vous sentiront présents.

■ Pensez qu'installer un ordinateur avec un accès Internet dans la chambre de votre enfant revient, peu ou prou, à le laisser se promener seul dans la rue à 03h00 du matin, ce que vous ne feriez pas. En effet, on ne sait pas qui ou quoi il peut y rencontrer.

■ Si vous deviez vous résoudre à le faire, en particulier avec un adolescent, imposez lui de maintenir la porte de sa chambre ouverte lorsqu'il surfe.

03 Ordinateur «Nounou»

■ Si vous êtes parent, n'imaginez pas une seconde que l'internet peut remplacer la nounou, ni être un moyen d'avoir « la paix » en installant l'enfant devant son ordinateur.

04 Importance de savoir utiliser l'ordinateur pour les parents

■ Prenez le temps d'apprendre à utiliser un ordinateur, au moins les bases et ainsi d'accéder aux services fournis par Internet (des formations parfois gratuites sont souvent mises en place, se renseigner dans votre mairie).

■ Rencontrez éventuellement d'autres parents internautes, améliorez votre pratique, échangez vos expérience... dans les forums de parents, les cyber-cafés et les espaces publics numériques qui vont être de plus en plus nombreux.

05 Nécessité de sécuriser l'ordinateur


fotolia©Monkey Business

■ Il est nécessaire d'avoir installé sur l'ordinateur, un système d'exploitation maintenu à jour (cf. options dans le centre de sécurité pour les ordinateurs sous Windows XP), un logiciel antivirus activé et à jour, un logiciel pare-feu et un anti malware pour le surf sur Internet. Il existe des suites intégrées comprenant ces 3 outils offrant une bonne protection.

■ Mais il est également indispensable que les parents installent (ou fassent installer) un logiciel de « protection » ou « contrôle parental » sur l'ordinateur utilisé par l'enfant, et en paramètrent le filtrage pour l'accès aux sites Web, par le biais de listes noires (sites interdits) et listes blanches (sites autorisés). Pour les e-mails et les chats, il convient de voir au cas par cas, avec le fournisseur d'accès (F.A.I.), les filtrages proposés. Depuis juin 2006, les F.A.I. sont dans l'obligation de fournir ce type de logiciel, gratuitement ou non. Vous pouvez lire une évaluation de ces produits sur le site *http://www.linternaute.com/comparatif/categorie/83/.*

06 Laissez vos enfants vous montrer comment ils se servent d'internet

■ Internet, c'est super! Prenez le temps de surfer sur le Net avec vos enfants et laissez-les vous montrer comment ils surfent sur l'Internet : leurs sites préférés, ceux qui pourraient vous intéresser. Cela vous permettra aussi de mieux connaître leur comportement face à Internet.

■ Établissez un dialogue bienveillant autour d'Internet avec vos enfants : invitez-les à montrer ce qui les gêne, discutez-en avec eux.

■ Si c'est le cas, n'hésitez pas à reconnaître votre méconnaissance technique : "Moi tu sais, Internet, je n'y connais rien, tu me montres?..."

■ Attention aux Webcams ! C'est une fenêtre ouverte sur votre domicile et l'intimité de vos enfants. Bien plus qu'un anodin visiophone, la Webcam expose au grand jour à tous l'identité visuelle, les objets personnels, les vêtements, la chambre… quand elle ne sert pas à des mises en scènes scabreuses ou pédopornographiques.

07 Sachez déchiffrer un comportement


Srpa gendarmerie©ADC F. Balsamo

■ Ne négligez pas un indice comme une adresse de site laissée en évidence dans sa chambre, parfois elle peut être l'équivalent d'une interrogation voire d'un S.O.S. Allez vérifier le contenu de ce site sur Internet.

■ Soyez attentif à tout changement de comportement. Chute des résultats scolaires, grande fatigue résultant de nombreuses heures sur l'Internet... sont susceptibles d'être les premiers symptômes d'une emprise psychologique. Cette dernière pourrait résulter d'une dépendance vis-à-vis de jeux en ligne ou d'échanges avec des personnes mal intentionnées comme des pédophiles. Gardez un oeil sur les cadeaux "reçus" ou "gagnés" sur l'Internet (colis postaux …).