Crypter le courrier

Votre courrier est facile à lire ... même par ceux qui n'ont pas le droit de le faire. De l'expéditeur à la réception sur votre ordinateur, il passe par les étapes suivantes, qui permettent toutes son interception :

Etape	Danger
Le serveur de l'expéditeur	Le courrier est lisible par le fournisseur d'accès de l'expéditeur.
Internet	Le courrier passe par un certain nombre d'étapes et de centres de redirection, ou il peut être intercepté et lu, en totalité ou en partie.
Serveur de votre fournisseur d'accès	Le courrier est lisible par votre fournisseur d'accès, jusqu'à ce que vous le retiriez, ou à perpétuité si le courrier n'est pas effacé après le retrait[1].

Tout cela est techniquement possible, mais ne signifie pas pour autant que votre courrier sera systématiquement examiné par des personnages mal intentionnés. Chaque seconde, des millions de messages transitent sur l'Internet, dans toutes les directions, et il faudrait d'excellentes raisons pour que vos messages confidentiels tombent dans de mauvaises mains ... c'est évidemment illégal, mais faisable.

Pour le courrier confidentiel, une solution consiste à crypter les messages. Interceptés ou pas, ils seront illisibles pour ceux qui n'en possèdent pas la clé.

[1] Un des mes amis s'est aperçu que tous les messages reçus depuis trois mois étaient encore sur le serveur ! ! Renseignez-vous auprès de votre fournisseur pour connaître sa politique. Vérifiez que vous n'avez pas coché la case *Conserver une copie des messages sur le serveur* dans la configuration des comptes de courrier d'Outlook Express (à l'onglet *Avancé*)

Vous utilisez déjà, peut-être sans le savoir, le cryptage dans vos communications sur l'Internet. Chaque fois que votre navigateur vous annonce que vous allez passer dans une zone sécurisée, par exemple quand vous tapez votre numéro de carte de crédit, vous envoyez des données cryptées.

Pourquoi crypter ?

Le cryptage n'est pas une nécessité, sauf si vous avez des informations **vraiment** confidentielles à protéger, et êtes prêt à organiser votre travail.

- L'interception d'un courrier n'est pas à la portée de tous. Pour pirater votre courrier, il faut disposer d'équipements et de logiciels et avoir une très forte motivation.
- Le cryptage exige du temps, une certaine connaissance technique, et une procédure relativement compliquée, non seulement pour vous, mais aussi pour vos correspondants.

Ce type de protection ne s'impose donc que dans les cas ou le secret est ***impératif***. Crypter dans d'autres circonstances est franchement une perte de temps.

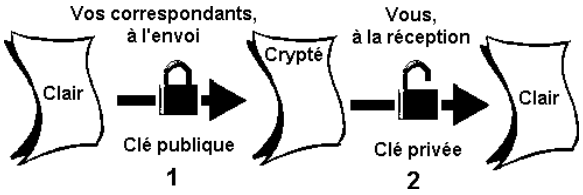
Si toutefois vous pensez avoir besoin de crypter, ou si vous êtes simplement curieux de voir comment cela fonctionne, ce chapitre vous montrera comment faire.

Les clés de cryptage

Le cryptage de PGP repose sur le principe des **clés de cryptage** :

- Une **clé publique**, accessible à tous, que vos correspondants utiliseront pour crypter le courrier qu'ils vous enverront.
- Une **clé privée**, que vous êtes le seul à connaître. Vous l'utiliserez pour décrypter les messages que vous recevrez.

Il est impossible d'expliquer ici les rouages de cette forme de cryptage : il y faudrait bien plus d'un manuel, mais le schéma suivant illustre le cheminement d'un message, de vos correspondants jusqu'à ce que vous le lisiez en clair.



- A l'étape 1, votre correspondant utilise, pour crypter un message qui vous est destiné, votre **clé publique**, qu'il a trouvé sur un serveur public (où cette clé est disponible), ou tout simplement dans un message que vous lui avez envoyé. Le courrier ainsi crypté ne sera lisible qu'à l'aide de votre clé privée : même la personne qui vous envoie le message serait incapable de le décoder.

  Cette clé publique sert uniquement à l'encodage et ne pourrait pas être utilisée pour le décodage. C'est la force du cryptage sur deux clés.
- A l'étape 2, une fois le message reçu, vous décryptez le message à l'aide de votre **clé privée**, *que vous êtes le seul à connaître*. Cette clé ne doit être communiquée à **personne**. Faites bien attention à ne **jamais** la perdre, car vous ne pourriez plus lire les messages qui vous seraient envoyés.

Entre les étapes 1 et 2, le message n'est transmis qu'à l'état crypté. Même s'il est intercepté au passage, il est illisible. Vous seul pouvez le déchiffrer.

La législation française

La majorité des pays du monde, reconnaissant l'intérêt du cryptage pour la protection des intérêts commerciaux et de la vie privée, encourage son utilisation.

En France, la cryptographie est soumise à une législation particulière, régie par le décret du 17 mars 1999 (n° 99-200), qui autorise l'importation et l'utilisation des matériels et logiciels de cryptage dont la clé est d'une longueur comprise entre 40 et 128 bits (Journal Officiel du 19 mars 1999, page 4051). La réglementation change constamment, et a longueur de la clé de cryptage autorisée est régulièrement allongée.

L'organisme qui délivre les autorisations d'utiliser les logiciels de cryptographie et leur degré de sécurité s'appelle la SSI, dont vous pouvez aller consulter le site à l'adresse www.ssi.gouv.fr, et qui dépend directement du cabinet du Premier Ministre.

Sur ce site, vous pourrez consulter la liste des produits homologués, et bien d'autres choses encore. Si la cryptologie vous intéresse, ou si vous chercher à comprendre comment elle fonctionne, c'est un site à visiter !

Les logiciels de cryptage

La sécurité du cryptage se mesure en bits qui sont la *longueur de la clé* de cryptage. Plus le temps passe, plus la clé des nouveaux systèmes de cryptage s'allonge, pour garder une longueur d'avance sur les méthodes de décryptage, qui s'améliorent aussi : dans quelques années, les systèmes de cryptage considérés aujourd'hui comme fiables seront facilement décryptables.

Plusieurs produits de cryptages du courrier sont disponibles, dont certains sont gratuits. Le plus connu est PGP.

PGP

Parmi ces derniers, le plus connu (et un des plus fiables) s'appelle **PGP** (***P**retty **G**ood **P**rivacy*, confidentialité relativement bonne). Il permet de crypter non seulement le courrier électronique, mais aussi les fichiers et des dossiers entiers. La dernière version française du programme est disponible à www.pgpi.org.

PGP est loin d'être le seul bon logiciel de cryptage, mais il est le plus répandu, et vous devrez communiquer avec des correspondants qui

l'utilisent aussi, sinon ils ne pourront pas décrypter vos messages.

Sur cette première page, cliquez sur **Download**, puis sur **PGP** à la page suivante.

Suivant votre version de Windows, vous devrez choisir entre deux versions de PGP :

Avec Windows 95, 98 ou NT

Vous pouvez télécharger une version en français nommée **PGP 6.5.1i**. Si vous essayez d'installer cette version sous Windows XP, vous n'obtiendrez qu'un message d'erreur.

1. Cliquez sur **Windows 95/97/NT**
2. La dernière version de PGP en français s'appelle 6.5.1. Cliquez sur **6.5.1i**.
3. Cliquez sur **French**, puis sur **Download PGP 6.5.1int, French version** pour télécharger la version française.
4. Choisissez un site de téléchargement, et téléchargez **PGP651intFreeware_FR.exe**. La taille de ce fichier est de 14,7 Mo, et le téléchargement peut durer longtemps si vous n'avez pas de connexion à haut débit.

Avec Windows XP

Vous devez télécharger PGP 8.0, version Freeware, qui n'existe qu'en anglais. C'est cette version que je décris dans ce chapitre. Elle fonctionne également sous Windows 98, ME, NT 4.0 et 2000.

1. Cliquez sur **Windows XP**.
2. Cliquez sur **PGP 8.0**.
3. Cliquez sur **Download PGP 8.0**.
4. Vous passez au site de PGP Corporation, qui exploite maintenant PGP sur une base commerciale, mais où vous pouvez toujours trouver une version Freeware, mais que vous n'avez pas le droit de redistribuer. En bas de la page, cochez la case **Please check this box**, et cliquez sur le bouton **Download Now** situé en face de ...**for Windows**.
5. Vous téléchargez le fichier **PGP800-PF_W.zip** (8,7 Mo) que vous devez d'abord décompresser, avant de double-cliquer sur **PGP8.8.exe**.

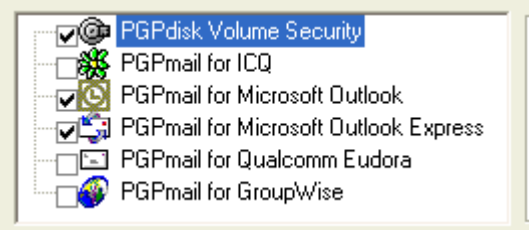
Installer PGP

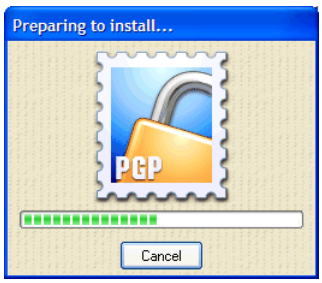
Si vous n'avez jamais installé de logiciel de cryptographie, la procédure peut semble compliquée, mais j'ajouterai des explications en cours de route. Vous rencontrerez de nouveaux concepts, dont :

- Les paires de clés, publiques et privées, et
- les serveurs de clé.

PGP est un produit relativement complexe, et cette section ne présente, très succinctement, que ses fonctions essentielles. Pour une utilisation plus avancée, je vous recommande d'imprimer le manuel et de le lire à tête reposée.

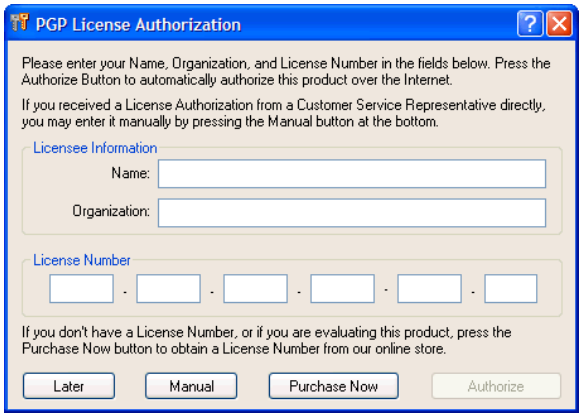
Au cours de l'installation, PGP vous demande quelles options vous voulez installer. Ces options sont des "plug-ins" qui s'intègrent à vos différents logiciels, et votre choix dépend évidemment de ce que vous utilisez. Voici comment j'ai répondu, mais vos choix pourront être différents :





Après l'installation, où PGP vous demande si vous avez déjà définit des clés, vous devez redémarrer votre PC.

Au redémarrage suivant, PGP vous demande votre numéro de licence, en vous encourageant à acheter la version commerciale.



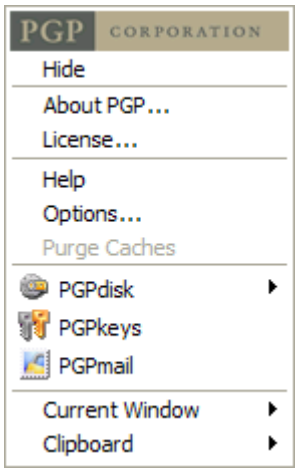
Cliquez simplement sur **Later** si vous ne voulez pas acheter avant d'avoir essayé le produit.

1. PGP passe ensuite à la définition de vos clés de cryptage. Vous devez d'abord donner votre nom et votre adresse email (ceci afin que vos correspondants associent cette adresse à vos clés). Cliquez sur **Suivant**.
2. Vous devez ensuite définir un mot de passe, qui est en fait une phrase entière, et devez la taper une deuxième fois pour confirmation. Cliquez ensuite sur **Suivant**.

   Je vous recommande d'utiliser une phrase entière, que vous connaissez bien, peut-être venue de votre enfance, mais que vous retiendrez facilement. Elle ne doit pas nécessairement être compliquée, mais elle doit vous être entièrement personnelle. Pour plus de sécurité, vous pouvez y mêler des symboles aléatoires, mais facilement mémorisables. N'oubliez pas que, lorsque vous tapez un mot de passe, vous ne pouvez pas voir ce que vous tapez !
3. PGP génère vos clés et vous n'avez pas à intervenir. Cliquez sur **Suivant**.
4. PGP vous annonce que vous avez terminé la définition de vos clés et vous pouvez cliquer sur **Terminer**.

L'installation est terminée.

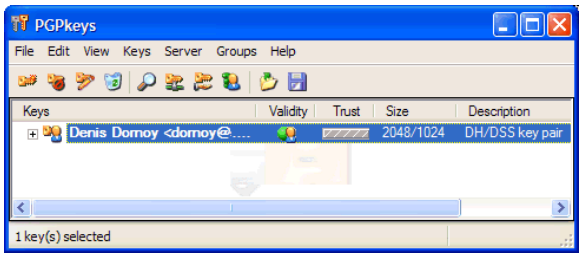
Utiliser PGP 8.0



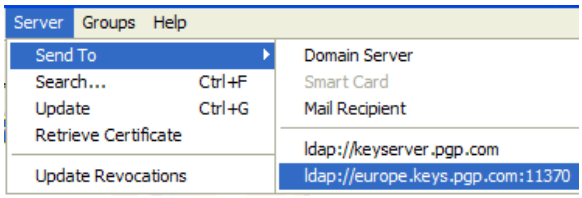
PGP 8.0 dépose sur votre barre des tâches une icône, sur laquelle il suffit de cliquer pour avoir accès aux fonctions du programme.

La première chose à faire, une fois que vous avez défini une clé publique, est de la faire connaître aux autres utilisateurs, afin qu'ils puissent vous envoyer du courrier crypté. Pour cela, sélectionnez **PGPKeys**.

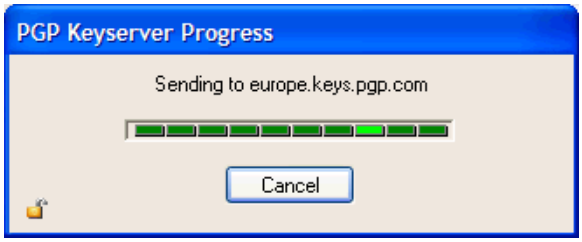
Publier votre clé publique



Si vous n'êtes pas encore connecté à l'Internet, connectez-vous maintenant.



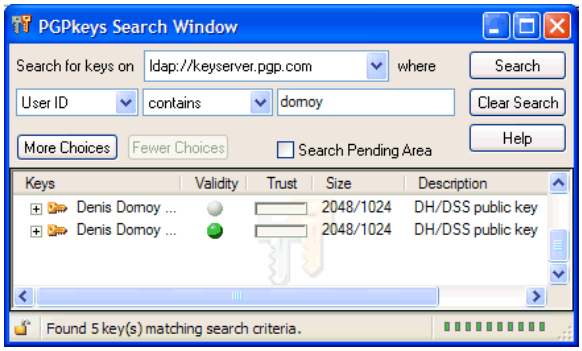
Sélectionnez **Server | Send to**, et sélectionnez un serveur.



Les autres utilisateurs peuvent maintenant trouver votre clé. A l'inverse, vous pouvez trouver les clés d'autres utilisateurs.

Obtenir une clé publique sur un serveur

Sélectionnez la commande **Server | Search**.



Dans cette boîte de dialogue, vous pouvez sélectionner un serveur et y faire des recherches sur un nom.

Passons maintenant à l'action et voyons comment envoyer et recevoir du courrier crypté.

Envoyer du courrier crypté

Quand vous envoyez un courrier par Outlook Express, PGP a automatiquement placé une nouvelle icône sur la barre d'outils d'Outlook Express.

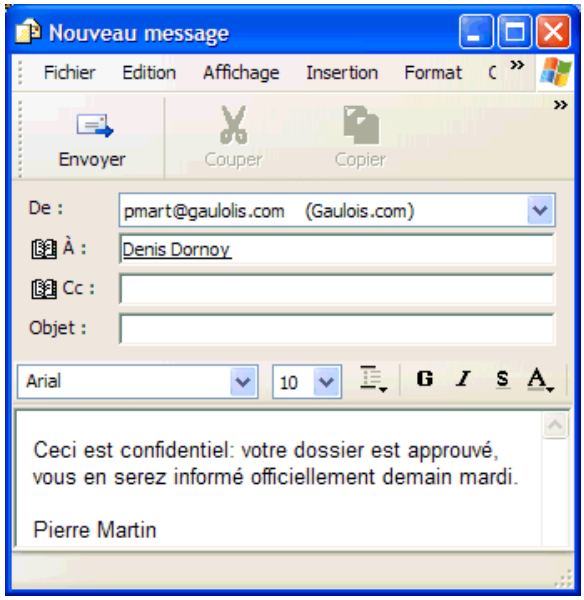
Pour envoyer un message crypté à un correspondant, vous devez avoir sa clé publique. Pour cela, deux possibilités :

1. Le correspondant a placé sa clé sur un serveur public, ou
2. il vous a envoyé sa clé par email. Nous allons examiner cette opération dans les deux cas :

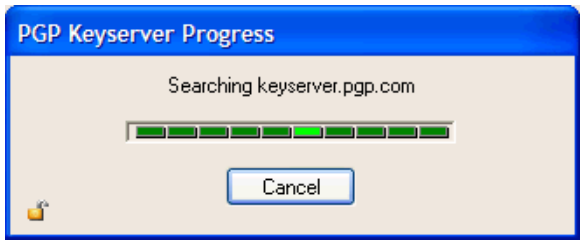
La clé publique est sur un serveur

Cette option n'est possible que si vous avez acheté une licence pour la version *PGP 8.0 Personal* (disponible pour $39 sur www.pgp.com) mais elle est si pratique que je vous la montre ici. Nous supposons que votre ami Pierre Martin vous envoie un message :

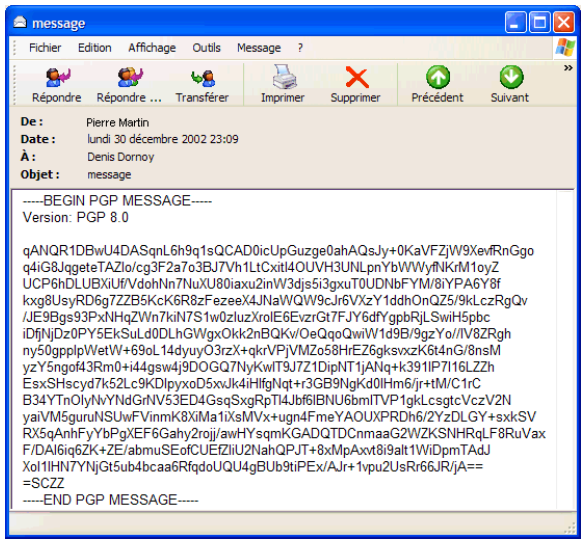
1. Il lance Outlook Express.



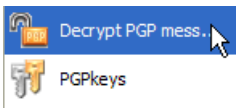
2. Il compose son message.
3. Sur la barre d'outils, il clique sur **Encrypt Message (PGP)**.



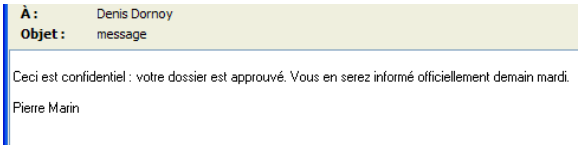
4. Dès qu'il clique sur **Envoyer**, PGP va chercher votre clé publique, s'il ne l'a pas déjà dans son trousseau de clés (voyez plus loin).



5. Vous recevez le message crypté, qui est beaucoup plus long que l'original.
6. Sur la barre d'outils, vous cliquez sur **Decrypt PGP Message**.



7. Le message est sélectionné, et vous devez taper votre **clé privée** dans une boîte de dialogue.



8. Le message est immédiatement décrypté.

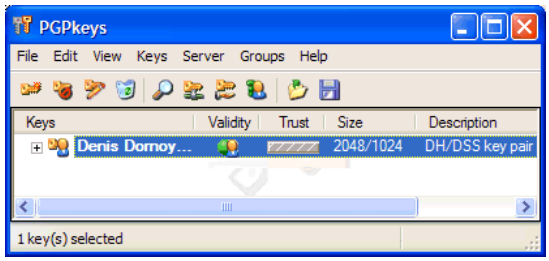
Cette méthode est très simple, mais elle exige que l'adresse email que vous utilisez soit présente sur un serveur de clés. N'y mettez pas votre vraie adresse, mais utilisez une adresse factice pour cela. N'oubliez pas que votre vraie adresse email doit rester confidentielle, et ne doit pas être placée sur un serveur public !

Vous avez reçu la clé publique en email

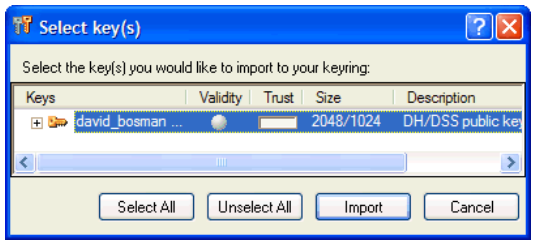
Cette méthode peut être nécessaire si vous utilisez un logiciel de courrier où PGP ne peut pas s'intégrer, ou si votre correspondant n'a pas placé sa clé publique sur un serveur.

Supposons que vous avez reçu par email la clé publique d'un de vos collègues :

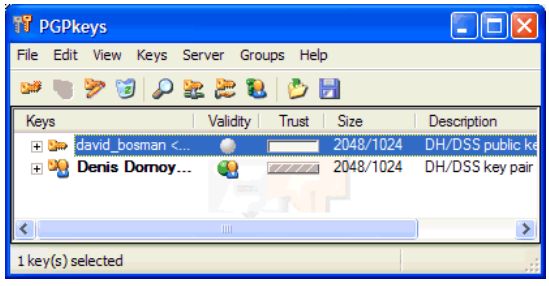
1. Sur la barre d'outil, cliquez sur **PGPKeys**.



2. La boîte de dialogue **PGPKeys** s'affiche à l'écran. Sélectionnez la clé publique, de la ligne :
   -----BEGIN PGP PUBLIC KEY BLOCK-----
   à la ligne :
   -----END PGP PUBLIC KEY BLOCK-----
3. Avec la souris, tirez la sélection dans la boîte de dialogue.



4. La clé de votre correspondant apparaît immédiatement dans une fenêtre séparée. Notez qu'elle correspond à une adresse précise. Sélectionnez la clé, et cliquez sur **Import**.



5. La clé de votre correspondant est maintenant dans votre trousseau de clé, et vous pourrez à l'avenir la réutiliser pour lui envoyer de nouveaux messages.

Les autres fonctions de PGP

PGP peut faire encore plus pour vous que chiffrer et déchiffrer des emails. Avec PGP, vous pouvez aussi :

- Signer des messages,
- Crypter des fichiers,
- Détruire des fichiers, c'est-à-dire les effacer complètement de votre disque, sans possibilité de récupération,
- Nettoyer votre disque.

Conclusion sur PGP

PGP est un produit qui peut accomplir énormément de choses. Il peut non seulement sécuriser votre courrier (du moins jusqu'à ce qu'un décryptage soit possible), mais encore assurer votre disque dur contre les curieux..

Ceci dit, rien n'est parfait en matière de sécurité, et vous devrez rester constamment en alerte : les techniques de déchiffrement progressent, et il sera possible demain de décrypter un message qui est sécurisé aujourd'hui. Il vous faudra alors vous procurer une version plus avancée, qui sera à son tour dépassé un jour, et ainsi de suite.

PGP a l'avantage d'être régulièrement mis à jour, et vous y trouverez toujours des outils utiles. La description que j'en ai donnée dans ce manuel ne fait qu'effleurer ses fonctions. Si vous voulez vraiment entrer dans les détails de la cryptographie, téléchargez un manuel et étudiez-le à tête reposée.

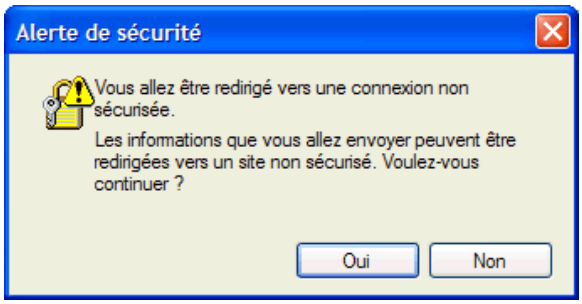
N'oubliez pas non plus, si vous êtes en France, que la législation concernant le chiffrement du courrier évolue pratiquement de mois en mois.

Le commerce électronique

Dans un manuel sur la sécurité Internet, il était inévitable que nous abordions le sujet du commerce électronique.

L'Internet ne cesse de colporter des rumeurs diverses, dont les plus persistantes veulent que les données transmises lors des paiements par carte de crédit soient mal sécurisées et à la disposition du premier pirate venu.

Quand vous effectuez un paiement sur le Web, vous êtes en *connexion sécurisée*. Autrement dit, *toutes vos données sont cryptées*. Vous vous en apercevez généralement quand Internet Explorer vous avertit du passage d'un type de connexion à l'autre :



Il est d'ailleurs facile de vérifier le niveau de cryptage. Dans Internet Explorer, sélectionnez la commande **? | A propos de Internet Explorer** et d'examiner le **Niveau de cryptage** :

Le niveau de cryptage est de 128 bits dans les dernières versions d'Internet Explorer. Dans les versions plus anciennes, il peut être de 40 bits.

Si c'est le cas, il est temps de mettre à jour votre version d'Internet Explorer.

Un cryptage de 128 bits n'est pas facile à décrypter. C'est possible, mais cela exige des ressources considérables, qui coûte bien plus cher qu'une transaction de quelques centaines d'Euros.

Les transactions en ligne sont donc très bien sécurisées.

Cette sécurité est-elle parfaite ? **NON** ! La sécurité parfaite n'existe pas. Cette question recevra toujours une réponse négative.

La vraie question est la suivante : payer par carte de crédit sur Internet comporte-t-il plus de risque que chez un commerçant.

Là aussi, la réponse est NON. Vous courez sans doute plus de risques à payer par carte chez un commerçant qu'en donnant votre numéro de carte sur un site Internet.

Chaque fois que vous réglez par carte de crédit chez un commerçant, il y a une petite chance de vol de votre numéro. De même, vous pouvez vous faire agresser dans la rue et vous faire voler vos cartes.

Les risques de l'Internet ne sont pas plus élevés. En fait, si vous prenez des précautions élémentaires, ils sont bien moins élevés.