

# Votre Sécurité

Il n'est guère possible, malheureusement, de protéger les adresses électroniques, sur Internet, et celle des Éditions Universelles, comme beaucoup d'autres, est souvent utilisée, par certains, à des fins abusives... **Nous pouvons cependant vous assurer que nous-mêmes n'envoyons aucun virus, spam ou autre courrier délictueux et que nous ne divulguons sous aucun prétexte vos adresses personnelles à des tiers...** Non seulement notre ordinateur est équipé de **2 firewalls** [pare-feux] mais tous les courriers qui sortent et qui rentrent sont automatiquement scannés **par un logiciel antivirus, mis à jour régulièrement et automatiquement**, avant d'être chargés ou expédiés... De plus, toute la gestion de nos services en ligne [**Librairie et autres**] est basée sur la **sécurité +**, grâce à **PayPal Europe** — aujourd'hui en français — **prestataire américain, installé, pour l'Europe, au Luxembourg, et possédant un système de détection de fraudes très élaboré... [Non seulement leur système VOUS protège, mais à nous aussi, contre les fraudes diverses, par une barrière de sécurités tout aussi diverses...]** [voir aussi notre article « **POURQUOI PAYPAL EUROPE** »]

« **Néanmoins, de l'autre côté de la chaîne, vous, lecteur, ou client utilisateur de sites marchands ou bancaires, « devez jouer un rôle actif pour assurer la sécurité complète de la chaîne de transmission des informations échangées. » Les conseils suivants sont basés sur ceux de notre banque, le CCF [aujourd'hui HSBC] et de son site « Sécurité bancaire sur Internet » que nous avons adapté à notre cas, puisque nos préoccupations et défenses sont les mêmes...**

**Cliquez sur chaque point, ci-dessous, pour accéder plus facilement, ou indépendamment, à chaque partie traitée :**

- **[Pour protéger les informations en ligne de nos lecteurs, ou clients](#)**
- **[Les différentes façons, pour vous, lecteur ou client, de vérifier que vos connexions sont sûres et sécurisées](#)**
- **[Comment protéger votre identité en ligne ?](#)**
- **[Comment utiliser votre adresse électronique de façon sécurisée ?](#)**
- **[En cas d'usurpation de votre identité...](#)**



---

## **Pour protéger les informations en ligne de nos lecteurs/clients :**

**La sécurité** de vos informations en ligne est très importante. Pour protéger votre information contre l'accès non autorisé, **PayPal**, notre prestataire de paiement sécurisé, emploie la technologie et les pratiques standards en matière de sécurité qui comprennent :

— **le protocole de sécurité SSL 128 bits (Secure Socket Layer)** [Ce protocole de sécurité existe sous deux niveaux : 40 bits (niveau standard) et 128 bits (niveau très élevé)]

« *Pour crypter toutes les données échangées, PayPal utilise le protocole de sécurité SSL 128 bits (Secure Socket Layer), niveau de chiffrement le plus élevé autorisé en France. Le chiffrement transforme vos informations sous une forme encodée avant l'envoi sur Internet.*

Le **https://** devant l'adresse d'un site ou la présence en icône d'une clé ou d'un cadenas   atteste que le site sur lequel vous naviguez est sécurisé par la technique de l'encodage et que l'information que vous saisissez sur une page est protégée. »

— **Firewall (ou pare-feu)**

**Les Éditions Universelles utilisent depuis longtemps des Firewalls** [un incorporé à notre Routeur et un autre inclus dans le paquet « sécurité sur internet » de Norton anti-virus] « pour empêcher que d'éventuels virus se propagent sur notre ordinateur ainsi que pour interdire l'accès et l'interception d'informations par des personnes non autorisées ». Aujourd'hui, tout système inclus à tout ordinateur en possède un. Vous n'avez pas grand-chose à faire vous-même, sinon à bien paramétrer le dit système selon vos choix et exigences.

## **Les différentes façons, pour vous, lecteur ou client, de vérifier que vos connexions sont sûres et sécurisées**

« En dehors des mesures de sécurité prises par les Éditions Universelles et PayPal, et par les banques en général, vous devez prêter une attention particulière lors de votre connexion pour vos opérations bancaires sur Internet à l'usage de votre code secret, à la protection de votre ordinateur et de vos données et prendre vous-même quelques précautions. **La protection de votre ordinateur - personnel ou de bureau - est de votre ressort.** Voici quelques conseils pour en assurer la sécurité :

### **Assurez-vous que vos sessions Internet avec PayPal, ou autres banques et services sécurisés, sont sécurisées :**

Saisissez l'adresse du site dans la barre d'adresse ou utilisez les favoris de votre navigateur Internet. Ne donnez pas votre identifiant et votre code secret sur une page s'affichant après un clic sur un lien dans un e-mail reçu.

Avant de saisir votre numéro de compte et votre code secret, assurez-vous que vous êtes bien dans un environnement sécurisé :

- le **https://** devant l'adresse d'un site et la présence en **icône d'une clé ou d'un cadenas** atteste que le site sur lequel vous naviguez est sécurisé par la technique de l'encodage et que l'information que vous saisissez sur une page est protégée.

**Pensez également à installer un firewall et un logiciel antivirus** sur votre ordinateur pour le protéger contre l'accès non autorisé d'un tiers et pour empêcher des virus et vers d'écrire sur votre ordinateur. Dans la mesure du possible, évitez d'utiliser des ordinateurs publics de type "borne publique" ou "cyber café" pour réaliser vos opérations bancaires ou vos achats sur Internet.

**Faites aussi attention aux "espions"** que comprennent certains logiciels gratuits [ou pas], certains sites que vous visitez ou certaines musiques que vous téléchargez : munissez-vous d'un **anti spyware [celui de Microsoft — gratuit — devait sortir en septembre 2005] et scannez votre ordinateur au moins une fois par semaine.**

### **Votre code secret :**

Votre code secret est le seul à donner accès à votre compte. Pour le protéger, suivez les conseils suivants :

- Lorsque vous recevez votre code secret, nous vous recommandons de jeter le courrier sur lequel il est inscrit et de modifier votre code secret dès votre première connexion.
- Créez un code secret composé de chiffres différents.
- Évitez les codes secrets que vous utilisez pour d'autres services en ligne tels que l'e-mail ou la messagerie instantanée.
- Choisissez un code secret que vous seul connaissez et qui ne peut pas être facilement deviné par quelqu'un d'autre
- N'associez pas votre code secret à des données personnelles comme des noms, dates de naissance, numéro de téléphone...
- Retenez votre code secret, ne l'écrivez jamais et ne le communiquez à personne, même si elle se présente comme appartenant au CCF.
- Assurez-vous que personne ne vous observe lorsque vous le saisissez et changez-le si vous croyez que quelqu'un a pu le découvrir.
- Modifiez régulièrement votre code secret.

**Personne dans une banque, ou service de paiement sécurisé, ne vous demandera votre code secret, vous le saisissez toujours vous-même. Si toutefois quelqu'un vous le demande, ne répondez jamais : cette personne ne fait pas partie d'un de ces services !**

**De même, ne répondez jamais à un e-mail vous demandant de donner votre identifiant ou votre code secret. Jamais une banque ou service de paiement sécurisé ne vous enverra un tel message.**

### **Fermeture de session et navigateur :**

Pensez toujours à mettre fin à votre session lorsque vous avez terminé votre consultation ou transaction en ligne et fermez votre navigateur. Cela empêche que d'autres personnes puissent utiliser votre session après que vous ayez quitté votre ordinateur.

Les pages consultées durant votre session ne seront pas stockées et, de ce fait, ne seront consultables sur votre poste informatique par aucune autre personne.

Si vous constatez des opérations anormales sur votre compte, signalez-le immédiatement à votre banque. L'information sur la date et l'heure de votre dernière connexion vous permettent de vérifier que personne d'autre que vous ne s'est connecté à vos comptes.

## L'utilisation de l'e-mail :

Généralement, l'e-mail envoyé ou reçu par une adresse standard (par exemple votrenom@hotmail.com ou votrenom@yahoo.com) n'est ni sécurisé, ni encodé et son contenu n'est pas protégé. Par conséquent, les informations personnelles qui transitent par e-mail peuvent être interceptées par des tiers. Nous vous conseillons donc de ne pas communiquer d'informations sensibles, qu'elles soient personnelles ou financières. En aucun cas, n'envoyez votre code secret par e-mail à personne ; de toute façon, **ne communiquez à personne votre code secret.**

Sur Internet, l'acheminement d'un e-mail n'est pas totalement garanti. N'utilisez donc jamais un e-mail pour transmettre vos coordonnées bancaires ; utilisez le fax, quand vous êtes sûr du numéro de votre correspondant.

**Ne répondez jamais aux mails qui demandent des informations personnelles**, ou qui vous invitent à cliquer sur un lien vers une page vous demandant votre identifiant et votre code secret.

Ne faites des transactions qu'avec des commerçants qui assurent votre sécurité. En cas de doute, contactez la société par téléphone et refusez de fournir par e-mail des informations personnelles.

N'ouvrez pas les e-mails et les pièces jointes dont vous ne connaissez pas la source : ils pourraient inclure un virus qui, une fois ouvert, pourrait endommager votre ordinateur. Vérifiez au préalable votre mail avec votre logiciel antivirus. »

## Comment protéger votre identité en ligne ?

« Nous vous recommandons vivement d'installer un logiciel firewall [[Mc Afee](#), [Symantec](#) et [Computer Associates®](#)] à votre domicile, au bureau et sur les ordinateurs en réseau pour empêcher l'accès non autorisé à votre ordinateur et aux données qui y sont stockées. Pour ceux qui utilisent un accès haut débit (ADSL ou câble), il est particulièrement important d'utiliser un logiciel firewall. Avec un tel accès, vous êtes certainement connecté en permanence à Internet dès que votre ordinateur est allumé, le risque d'intrusion malveillante sur votre ordinateur est donc augmenté.

- Utilisez de manière permanente votre programme antivirus. [Norton — de [Symantec](#) — est pour nous le meilleur, mais il y en a d'autres tels que [Mc Afee](#), [F-Secure](#), [Kaspersky](#) et [Trend Micro](#).] Cela protégera votre ordinateur des virus et des vers et empêchera ainsi toute écriture sur votre système informatique. **Nous vous recommandons d'acheter des programmes qui se mettent à jour régulièrement et automatiquement.**

- Ne partagez pas l'accès de votre ordinateur avec des étrangers. Désactivez le partage de dossier et d'imprimante pour éviter qu'un internaute navigue dans vos fichiers ou les détruise. Suivez attentivement les conseils du manuel de votre ordinateur lors de l'installation ou consultez en ligne les instructions du constructeur.

- Assurez-vous de disposer des dernières mises à jour de votre système d'exploitation et de votre navigateur pour disposer des dernières mises à jour en terme de sécurité.

- Consultez régulièrement le site Internet du logiciel d'exploitation de votre ordinateur (Windows ou Mac) pour les "patches" (compléments) ou mises à jour de votre système ou navigateur : vous disposerez ainsi des dernières mises à jour en terme de sécurité. Windows a un dispositif standard pour vous aider à le faire.

- Soyez attentif aux derniers virus et vers qui pourraient endommager votre ordinateur.

Pour mieux connaître les infections qui peuvent affecter votre ordinateur et vous tenir informé des derniers virus, vers, chevaux de Troie et autres programmes malveillants conçus pour endommager votre ordinateur ou pour accéder à vos informations personnelles, nous vous recommandons notamment les sites des entreprises telles que [Symantec](#) ou [Trend Micro](#)...

N'ouvrez ni les e-mails ni les pièces jointes dont vous ne connaissez pas la source. Parcourez au préalable votre e-mail avec votre logiciel antivirus. La plupart des antivirus peuvent le faire automatiquement.

## **Protégez-vous contre les virus et les e-mails frauduleux :**

La meilleure des défenses contre les virus est l'apprentissage et la discipline, car c'est avec un comportement averti et discipliné que vous réduirez vos risques. Aujourd'hui, les messageries sont pourvu d'un système de tri « anti-spam », plutôt efficace. Il suffit de cocher les bons paramètres.

Lancez régulièrement et fréquemment sur votre ordinateur votre programme antivirus soigneusement mis à jour. Le logiciel peut également scanner vos e-mails et leurs pièces jointes, qu'ils soient reçus ou envoyés et vous protéger contre des virus, vers, chevaux de Troie et autres programmes malveillants conçus pour endommager les dossiers et programmes de votre ordinateur.

N'opérez jamais de double click sur la pièce jointe d'un e-mail qui contient un dossier exécutable ou des fichiers avec l'extension .exe ou .com ou .vbs à moins d'être absolument confiant de la source. Si un dossier infecté est ouvert, le virus peut endommager votre disque dur, les fichiers programmes et le fichier d'e-mail. Activez votre **antivirus** pour détecter les infections **avant** d'ouvrir quelque fichier que ce soit.

Concernant les données personnelles, lisez attentivement les informations émises par les sociétés et les sites Internet que vous utilisez. Les mentions sur les données personnelles fournissent aux clients les détails sur la protection de leurs informations personnelles, le partage de ces informations et le but de leur collecte. Prenez l'habitude de lire ces mentions sur les sites des sociétés qui détiennent vos comptes ou avec qui vous réalisez des transactions (sites commerciaux par exemple). La plupart des mentions sur les données personnelles vous offriront un accès et les droits de modifications de vos données."

## **Comment utiliser votre adresse électronique de façon sécurisée ?**

**"L'utilisation frauduleuse d'e-mail [très, très IMPORTANT]"**

### **• Les sites d'e-mail ou techniques du Phishing**

Certains e-mails frauduleux sont utilisés pour envoyer de fausses informations en se faisant passer pour des sociétés connues. Dans le mail, on vous demande des informations personnelles pour "mettre à jour les données vous concernant". Le but est de duper les consommateurs qui téléchargent un virus ou sont invités à consulter un site frauduleux leur demandant des informations personnelles. Le risque encouru est la fraude, l'usurpation d'identité ou l'infection de l'ordinateur. **[Si vous recevez un e-mail ou un lien vers une page demandant des informations personnelles, ne répondez pas, même si la page ressemble à celle du prétendu site. Aucune société à la réputation établie ne vous demandera d'informations personnelles par e-mail.]**

### **• Les alertes de sécurité**

Récemment, plusieurs fraudeurs ont envoyé de faux e-mails informant les clients que, à cause d'une alerte de sécurité, ils devaient cliquer sur un lien de l'e-mail et aller sur un site pour changer leur code secret. Sur un site illicite, les clients sont invités à saisir leur nom et leur code secret avant de changer leur code secret. Le fraudeur espère ainsi obtenir en ligne les noms et codes secrets des clients non méfiants et les utiliser pour accéder à leurs comptes. Comme nous l'avons précédemment mentionné, nous vous recommandons de ne jamais fournir d'information personnelle en réponse à de telles demandes et de contacter la société en question si vous soupçonnez que l'e-mail est frauduleux.

### **• Fraudes à la loterie**

Le principe consiste à envoyer des lettres ou e-mails qui laissent croire au destinataire qu'il a gagné un prix dans une loterie à laquelle il n'a jamais participé. Généralement, le destinataire prétend représenter une société de vente. Pour obtenir les fonds, le destinataire doit répondre à une adresse e-mail ou à un numéro de fax spécifique. On lui demande alors de retourner ses coordonnées bancaires afin que les fonds soient transférés par virement et que soient prélevés des frais de traitement de l'opération. Une fois réglés, ces frais sont perdus ; de plus, les informations fournies seront probablement utilisées pour d'autres fraudes. »

## **En cas d'usurpation de votre identité :**

« Si vous suspectez que vous êtes victime d'une fraude :

- informez immédiatement votre agence bancaire si vous suspectez une fraude sur vos comptes ;
- déposez plainte auprès des instances de police et fournissez une copie de la plainte à votre agence.

Pour plus d'information sur la sécurité de votre ordinateur, pour vous protéger et compléter l'installation de votre ordinateur, nous vous invitons à consulter les sites présentés ci-dessus et ci-dessous. Si vous avez des questions concernant la sécurité de votre banque sur Internet ou sur la sécurité de vos informations, contactez l'assistance technique de votre banque. »

**Informations fournies à titre indicatif seulement. D'autres sources, évidemment, sont disponibles sur Internet, soit sur le site du CCF, aujourd'hui [HSBC](#), [Security Seer](#), [Spybot](#), [Hoax Buster](#), [Symantex Security response](#)... etc.**

Evelyne Lapouge  
[Éditions Universelles](#)  
25 août 2005/ 23 janvier 2009

Lire aussi notre article « [POURQUOI PAYPAL EUROPE](#) »