

## La protection des consommateurs contre la cyberfraude

**Quelles sont les formes les plus courantes de cyberfraude ?**

**Dans quelle mesure la fraude affecte-t-elle le marché du numérique ?**

**Quelles mesures de prévention faut-il prendre ?**

**Quel est le rôle joué par la mise en œuvre de la législation et les voies de recours ?**

**Que faut-il faire de plus ?**

**Pour en savoir plus**

**Références**

**Où nous contacter ?**

### Introduction

Internet fait désormais partie de la vie quotidienne de millions de personnes dans le monde, que ce soit pour le courrier électronique ou pour les achats en ligne. La multiplication des possibilités d'accès de plus en plus performants via des plates-formes de plus en plus diversifiées, à l'instar des téléphones mobiles et autres appareils portables, a ouvert de nouvelles perspectives pour le commerce électronique. L'achat et la banque en ligne se généralisent et dans les 10 années à venir, le Net devrait devenir aussi commun que le gaz ou l'électricité. À en croire Vinton Cerf, « Évangéliste en chef d'Internet » chez Google, d'ici 2016 « tout, depuis le réfrigérateur familial jusqu'à la cafetière du bureau ... en passant par le chauffage, la climatisation, les systèmes de sécurité ... sera géré via Internet ; ... à cette date, Internet sera devenu tellement omniprésent que le fait de s'y connecter ne sera même plus un acte conscient ».

Cette prévision se vérifiera-t-elle ? Et les consommateurs en tireront-ils pleinement avantage ? Les ministres de l'OCDE qui débattaient du phénomène naissant du commerce électronique en 1998 entrevoyaient l'énorme potentiel du commerce en ligne grand public. Mais ils étaient également conscients de la menace que la fraude pourrait faire peser sur la confiance des consommateurs. L'année suivante, l'OCDE adoptait ses Lignes directrices sur le commerce électronique destinées à promouvoir des pratiques commerciales loyales en ligne. Toutefois, à mesure que le commerce en ligne prenait son essor, il apparaissait de plus en plus clairement que les escrocs pouvaient utiliser le cyberspace pour contourner la loi en s'implantant dans un pays tout en ciblant les consommateurs d'un autre pays. Face à ce problème, l'OCDE a publié en 2003 des Lignes directrices relatives à la coopération internationale entre autorités chargées de la protection du consommateur.

Aujourd'hui, alors qu'Internet offre aux consommateurs du monde entier davantage de choix et de moyens plus commodes pour l'achat de biens et de services, toutes les possibilités du cybermarché ne se sont cependant pas encore concrétisées. Une des raisons fréquemment avancée est la crainte des consommateurs à l'égard de la fraude. La présente Synthèse passe en revue les diverses formes de la cyberfraude, évalue son impact sur l'économie du numérique et examine ce que peuvent faire les pouvoirs publics dès à présent et à l'avenir pour remédier au problème. ■

## Quelles sont les formes les plus courantes de cyberfraude ?

Le cyberspace est le théâtre d'un large éventail d'escroqueries, telles que les loteries frauduleuses, les escroqueries aux voyages ou au crédit, la prise de contrôle de modems et de pages web ou l'usurpation d'identité, pour n'en citer que quelques-unes. Nombre de ces escroqueries, comme la vente pyramidale, ne sont que des variantes en ligne de pratiques frauduleuses qui sévissent depuis longtemps dans l'environnement traditionnel. Internet a cependant offert aux escrocs un accès à une population mondiale de cibles potentielles, ainsi que davantage de possibilités d'échapper à la justice. Les fraudeurs n'ont en effet nul besoin de se trouver dans le même pays, ni même dans le même hémisphère que leurs victimes.

Internet permet aux fraudeurs de se faire passer pour des commerçants légitimes en se dissimulant derrière des sites web à l'apparence professionnelle ou en proposant sur des sites d'enchères électroniques des produits « gratuits » ou « à des prix de rabais », des produits « miracles » ou encore de « bonnes » affaires en matière d'investissement et de commerce. Ces offres trompeuses et mensongères induisent les consommateurs sans méfiance à acheter des biens et services en ligne qui se révèlent être nettement inférieurs à ce qui était promis, ou qui même n'existent pas.

Nombre d'escroqueries en ligne trouvent leur origine dans des messages non sollicités (spam) – généralement via le courrier électronique, mais aussi parfois par SMS, messagerie vocale sur Internet (téléphonie IP) ou autres voies électroniques. Lorsque l'OCDE a mis en place un Groupe de réflexion pour lutter contre le fléau du spam en 2004, le problème était essentiellement celui de la publicité non désirée et irritante qui bloquait les boîtes de courrier électronique. Mais, deux ans plus tard, quand le Groupe de réflexion a conclu ses travaux, le spam était devenu un large vecteur de diffusion de la fraude et autres pratiques abusives en ligne.

Nombreux sont les utilisateurs du courrier électronique qui ont déjà reçu un message émanant d'une personne prétendant être un responsable gouvernemental ou un membre de la famille royale d'un pays étranger (généralement d'Afrique), promettant des sommes d'argent substantielles en échange d'une aide pour effectuer un transfert de fonds à l'étranger. Cette fraude, communément appelée « escroquerie nigériane », « ouest-africaine » ou escroquerie « 419 », consiste, une fois les victimes appâtées, à les convaincre d'effectuer de petits paiements à l'avance pour diverses raisons, telles que des frais de transactions bancaires. Il va sans dire que la victime ne reçoit jamais la forte somme promise. Le spam est aussi utilisé pour propager de nombreuses escroqueries pyramidales ou de travail à domicile consistant à solliciter un paiement ou un investissement par avance contre la promesse de revenus élevés qui ne se matérialisent jamais.

Les consommateurs étant de plus en plus avertis pour déceler et éviter les escroqueries, les fraudeurs ont réagi en s'orientant vers des attaques plus imaginatives et plus inquiétantes basées sur des méthodes astucieuses d'ingénierie sociale et sur une technologie sophistiquée. Ces attaques innovantes consistent à usurper l'identité d'une personne (nom, numéro d'identité nationale et autres informations telles que numéros de cartes de crédit) pour commettre des fraudes ou autres délits. Une fois de plus, le spam est un outil clé pour faciliter le vol d'identité, en incitant les individus à divulguer des informations sensibles telles que numéros de cartes de crédit ou mots de passe. Ainsi, le spam d'hameçonnage (*phishing*) consiste à faire croire frauduleusement que le

message émane d'institutions financières ou de commerçants légitimes et bien connus. Il est demandé aux destinataires de cliquer sur des hyperliens pour vérifier ou mettre à jour leurs comptes en ligne (voir l'exemple ci-dessous). Ces hyperliens dirigent les utilisateurs vers des sites web imitant des sites légitimes pour les amener à divulguer des informations personnelles pouvant être ensuite utilisées pour accéder à leur compte bancaire et effectuer illégalement des retraits d'argent, ouvrir de nouveaux comptes bancaires ou des cartes de crédit au nom de la victime, effectuer des achats en ligne illicites, etc.

Ces attaques deviennent de plus en plus sophistiquées. L'année dernière, une nouvelle pratique appelée « harponnage » (*spear-phishing*) s'est développée, consistant à insérer des informations exactes sur le destinataire, comme son nom complet et son adresse personnelle, afin de rendre le message électronique d'hameçonnage encore plus convaincant. Un autre phénomène nouveau connu sous le nom de *vishing* induit le destinataire à effectuer un appel téléphonique, plutôt que de cliquer sur des liens pointant vers des sites web. Le numéro indiqué est un numéro de téléphone IP qui enregistre les chiffres (tels que les numéros de comptes) saisis sur le téléphone, permettant aux escrocs de voler et d'exploiter l'information.

D'autres variantes de fraude exploitent le vol d'identité réalisé par des moyens techniques. Ainsi, le *pharming* perturbe le processus d'interrogation du système de nom de domaine (DNS) pour rediriger les utilisateurs souhaitant se connecter sur un site web particulier vers un site « pirate » où ils divulguent des informations personnelles aux escrocs. Les consommateurs peuvent aussi télécharger à leur insu des logiciels malveillants lorsqu'ils ouvrent des pièces jointes à des messages non sollicités ou lorsqu'ils naviguent en ligne. Ces programmes malveillants, qui, outre les ordinateurs, ciblent de plus en plus fréquemment les téléphones mobiles et autres appareils portables, peuvent installer des enregistreurs de frappe au clavier et autres programmes conçus pour voler les informations stockées, saisies ou reçues au moyen de ces appareils. L'information ainsi recueillie par

**Graphique 1.**  
**COURRIER ÉLECTRONIQUE**  
**D'HAMEÇONNAGE QUE**  
**POURRAIENT RECEVOIR**  
**LES CLIENTS D'UNE**  
**BANQUE**  
(exemple inventé  
par l'OCDE)

Auteur : Le service de sécurité de votre banque <securite@votrebanque.com>  
Date : 19 septembre, 2006 5h13 PM  
Destinataire : Moi-même  
**Objet : Vérification des informations concernant votre compte**

## Ma banque

Cher client,

Dans le cadre de nos procédures courantes de contrôle de sécurité, nous avons noté plusieurs tentatives suspectes de connexion à votre compte. Par précaution, nous avons temporairement suspendu votre accès à nos services bancaires en ligne. Pour nous permettre de rétablir votre accès à ces services, nous vous invitons à cliquer sur le lien ci-dessous et à compléter toutes les étapes de vérification des informations concernant votre compte.

### [Informations concernant votre compte](#)

La sécurité de votre compte est l'une de nos préoccupations majeures. Nous vous remercions de l'attention que vous porterez à cette question.

Veuillez ne pas répondre à ce message. Les courriers électroniques adressés à ce compte resteront sans réponse. Si vous avez besoin d'aide, connectez-vous à votre compte et cliquez sur le lien « Aide » figurant dans le haut de chaque page.

ces moyens d'attaque technologiques, comme par exemple des mots de passe et autres données sensibles, peut ensuite être utilisée pour commettre des fraudes.

Selon une idée fautive pourtant très répandue, seuls les consommateurs naïfs sont victimes de la cyberfraude. Or, avec la sophistication croissante des escrocs en ligne, même les internautes les plus avertis peuvent se laisser prendre. Comme le concluait un rapport de l'OCDE de 2005 : « On peut être victime d'une escroquerie quel que soit son degré d'instruction, son âge ou son expérience. » ■

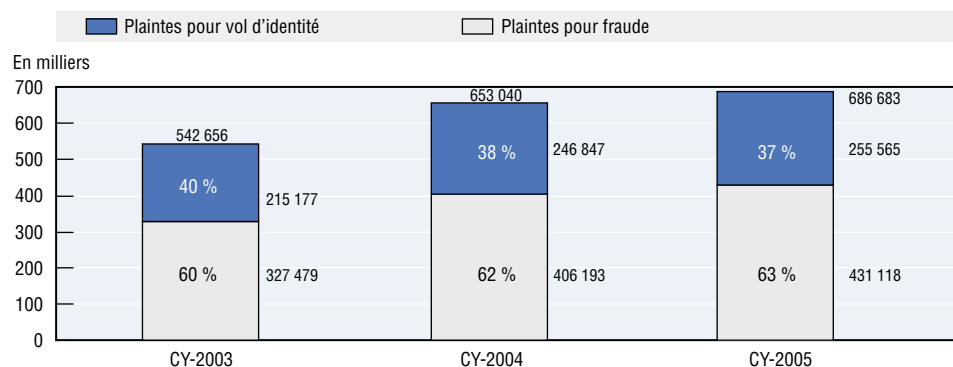
### Dans quelle mesure la fraude affecte-t-elle le marché du numérique ?

À en juger par l'augmentation constante des plaintes des consommateurs, la fraude transfrontière semble incontestablement progresser. Un rapport de 2006 du Réseau des centres européens des consommateurs montre que les plaintes relatives au commerce électronique, notamment les cas de fraude, ont plus que doublé entre 2004 et 2005. De la même manière, un rapport de 2006 de la Federal Trade Commission (FTC) des États-Unis montre que les plaintes pour fraude transfrontière ont bondi de 16 % de l'ensemble des plaintes en 2004 à 20 % de l'ensemble des plaintes en 2005. Sur les 685 000 plaintes reçues en 2005, 63 % constituaient des plaintes pour fraude et 37 % des plaintes pour vol d'identité.

Cette explosion de la fraude à la consommation pourrait expliquer pourquoi les transactions entre consommateurs et professionnels demeurent à ce jour inférieures en nombre à celles effectuées entre professionnels. L'Observatoire européen des technologies de l'information relevait en 2004 que les transactions interentreprises constituaient près de 90 % du marché du commerce électronique. La situation n'a guère changé depuis.

Selon des estimations récentes, l'hameçonnage et les autres fraudes sur Internet représentent, pour les consommateurs américains, un coût de quelque 1.2 milliard de dollars par an, tandis qu'en Allemagne, les chiffres officiels font état de pertes supérieures à 4.5 millions d'euros pour les consommateurs, ce chiffre ne couvrant que les cas signalés à la police et faisant l'objet d'une enquête. De plus, une étude de 2006 publiée par le Better Business Bureau des États-Unis fait ressortir que le temps que les victimes de fraude à l'identité doivent consacrer à la régularisation de leur situation est passé de 33 heures en 2003 à 40 heures en 2006. Le risque qui en découle est que les consommateurs pourraient moins dépenser en ligne pour éviter non seulement les coûts financiers de la cyberfraude mais aussi les pertes de temps pour résoudre les problèmes rencontrés. Les entreprises subissent également un préjudice considérable du fait

**Graphique 2.**  
**PLAINTES POUR**  
**USURPATION D'IDENTITÉ**  
**ET POUR FRAUDE**  
**PAR ANNÉE CIVILE**



Source : US FTC, Rapport 2006 sur les données relatives aux plaintes pour vol d'identité ou pour fraude.

de la fraude, notamment en termes de productivité perdue et de coûts directs liés à la mise en place d'un soutien technique et de solutions logicielles pour contrer celle-ci (par exemple au moyen de filtres). Les sociétés de cartes de paiement ont mis en place des politiques (que ce soit à titre volontaire ou pour se conformer à la réglementation) pour limiter la responsabilité des consommateurs et prendre en charge la majeure partie de leur préjudice en cas de retraits non autorisés. Au Royaume-Uni, l'Association des services de compensation a noté que les pertes des banques du fait des fraudes aux services bancaires sur Internet ont plus que triplé pour atteindre 14.5 millions de livres pour le premier semestre 2005. Selon le Rapport annuel sur la fraude publié par CyberSource, fournisseur mondial de logiciels de paiements électroniques sécurisés, de gestion des fraudes à la carte de crédit et de vérification, les opérateurs de commerce électronique devaient perdre jusqu'à 2.8 milliards de dollars du fait de fraudes aux paiements en 2005, soit une progression de 8 % par rapport à l'année précédente. ■

### Quelles mesures de prévention faut-il prendre ?

La première ligne de défense pour empêcher les consommateurs de devenir des victimes du cyberspace est celle de l'éducation. Des fiches sur les principales formes de fraude sur Internet et sur la façon de les combattre ont été préparées par les autorités publiques, les autorités de contrôle et le secteur privé sur divers supports tels que des sites web gouvernementaux, brochures, affiches, vidéo, rapports, etc. Le Réseau international de contrôle et de protection des consommateurs (RICPC), un réseau informel regroupant les autorités chargées de faire appliquer la législation dans les pays de l'OCDE et autres pays non membres, a ainsi lancé le *Mois de Prévention de la Fraude*, campagne de sensibilisation organisée chaque année pendant un mois spécifique. Dans le cadre de cette campagne, les membres organisent des activités pour apprendre aux consommateurs à reconnaître, signaler et faire cesser la fraude. En 2006, 25 membres du RICPC ont participé à la manifestation. De même, à travers le Plan d'Action de Londres, 34 organismes et 24 représentants du secteur privé de plus de 24 pays explorent des stratégies d'information pour lutter contre le spam.

Le secteur privé propose également un certain nombre d'outils techniques permettant d'assurer la protection en temps réel des consommateurs contre la cyberfraude. Ainsi, pour lutter contre les messages non sollicités, lesquels sont une source importante de fraude, les professionnels ont mis au point des moyens basés sur des mécanismes d'authentification, des filtres et des listes. De la même manière, des systèmes anti-hameçonnage ont été mis en place permettant aux internautes de signaler les sites d'hameçonnage et de les bloquer.

Toutefois, peu d'initiatives ont été entreprises jusqu'à présent pour mesurer l'impact de ces actions sur le comportement des consommateurs sur le cybermarché. Seul un nombre limité d'études ont tenté de savoir dans quelle mesure les consommateurs gèrent effectivement l'information et utilisent les outils mis à leur disposition pour éviter la fraude en ligne. Et les résultats peuvent être surprenants. Une enquête réalisée en 2005 par le Momentum Research Group aux États-Unis, en France, au Royaume-Uni et en Allemagne a, par exemple, montré que les consommateurs européens étaient moins informés du vol d'identité que les consommateurs américains. L'enquête note que 9 consommateurs américains sur 10 sont conscients du risque de vol d'identité, alors qu'un consommateur sur trois connaît encore mal la question en France et en Allemagne. Bien que cette estimation permette de se faire une idée de l'ampleur du problème, davantage de données sont encore nécessaires pour comprendre les raisons d'un tel décalage et la manière dont il pourrait être comblé. ■

**Quel est le rôle joué par la mise en œuvre de la législation et les voies de recours ?**

Si la prévention est essentielle, le renforcement de la coopération internationale est également vital pour identifier les activités frauduleuses en ligne et y mettre un terme. Comme le cyberspace ignore les frontières nationales, les autorités chargées de l'application des lois doivent œuvrer ensemble pour appréhender les escrocs sur le marché du Net. Suite aux recommandations des Lignes directrices de 1999 sur le commerce électronique et celles de 2003 sur la fraude transfrontière, les pays membres de l'OCDE ont mis en place des cadres plus appropriés et adaptés pour faire respecter l'application des lois, tant au niveau national qu'international.

Un rapport récent de l'OCDE sur la mise en œuvre des Lignes directrices de 2003 conclut que les pays membres ont d'ores et déjà déployé des efforts considérables pour moderniser leurs législations et leurs mécanismes de coopération pour l'application des lois (voir encadré ci-dessous).

Cependant, pour que les consommateurs prennent confiance dans le cybermarché, ils doivent pouvoir se faire indemniser par les auteurs des délits pour les préjudices qu'ils ont subis. Le fait de priver les auteurs de délits de leurs gains illicites pour indemniser leurs victimes peut également contribuer à dissuader d'éventuels futurs fraudeurs.

Il est cependant très difficile pour les consommateurs d'engager des poursuites à titre personnel pour obtenir réparation dans les affaires de cyberfraude. En premier lieu, les consommateurs n'ont pas les pouvoirs d'investigation et de sanction nécessaires pour identifier l'auteur et établir la preuve suffisante du délit. En second lieu, les difficultés pratiques et coûts financiers de la saisie d'un tribunal sont souvent bien supérieurs au préjudice subi par les consommateurs, surtout si la fraude provient d'un autre pays.

Les autorités chargées de la protection des consommateurs, en s'appuyant sur leur pouvoir de sanctions et leurs réseaux de coopération internationale, sont mieux à même d'obtenir l'indemnisation des consommateurs dans les affaires

**Encadré.  
ACTIONS PRINCIPALES  
DE MISE EN ŒUVRE  
DES LIGNES  
DIRECTRICES DE 2003  
RÉGISSANT LA FRAUDE  
TRANSFRONTALIÈRE**

<p>Modernisation au plan national</p>	<ul style="list-style-type: none"> <li>• De nouvelles autorités chargées de l'application des lois ont été créées.</li> <li>• Celles déjà en place ont été dotées de pouvoirs renforcés pour dissuader les commerçants indécents de récidiver.</li> <li>• Les peines à l'égard des fraudeurs ont été sensiblement alourdies.</li> <li>• Des partenariats public-privé ont aidé à appréhender les auteurs d'infractions dans le monde entier.</li> </ul>
<p>Coopération internationale renforcée pour l'application de la législation protégeant les consommateurs</p>	<ul style="list-style-type: none"> <li>• Notifications des activités illégales observées dans un pays.</li> <li>• Développement accru des échanges d'informations sur les activités illégales en cours et sur les fraudeurs.</li> <li>• Assistance dans le cadre d'enquêtes.</li> <li>• Décisions judiciaires exemplaires en matière de fraude transfrontière.</li> </ul>

de fraude. Actuellement, cependant, les capacités et expériences à cet égard des autorités chargées de la protection des consommateurs dans les pays de l'OCDE sont toujours très contrastées. Dans certains pays, les autorités n'ont absolument aucun pouvoir pour compenser les préjudices des consommateurs alors que dans d'autres pays, les autorités peuvent demander réparation au nom aussi bien des consommateurs étrangers que des consommateurs nationaux. L'élaboration de principes d'action communs dans ce domaine est une priorité évidente de l'action future de l'OCDE. ■

### Que faut-il faire de plus ?

Incontestablement, des progrès significatifs ont été accomplis dans l'édification d'une stratégie efficace contre la cyberfraude – les campagnes d'information, les mesures techniques de prévention et les moyens et la coopération pour l'application des lois sont autant de domaines dans lesquels des progrès sont à noter. Néanmoins, des éléments clés de cette stratégie doivent être encore améliorés pour endiguer le flot toujours plus important des cas de cyberfraude et des pertes financières qu'ils provoquent.

Une première mesure simple serait de collecter des statistiques comparables au plan international sur l'ampleur des plaintes des consommateurs et des préjudices financiers dus à la fraude. Cela aiderait à apprécier l'importance des obstacles actuels au développement du cybermarché grand public et à fixer les priorités en matière de répression. Actuellement, les activités de collecte et d'analyse de statistiques varient considérablement d'un pays à l'autre.

La mesure de l'impact de l'éducation des consommateurs pourrait améliorer les méthodologies pour la conception et la conduite des futures campagnes. L'analyse des différentes catégories d'initiatives menées dans les pays membres et de leur impact sur la compréhension et le comportement des consommateurs pourrait offrir une base utile pour dégager des pratiques exemplaires.

Dans certains pays, des aménagements législatifs sont encore nécessaires pour permettre aux autorités d'enquêter avec succès et de réprimer la fraude, notamment dans le contexte transfrontière. De façon plus générale, davantage de ressources et de moyens de formation devraient être alloués pour remédier à certains problèmes pratiques que les autorités rencontrent dans leurs actions de coopération.

Les pays membres de l'OCDE sont résolus à accomplir de nouveaux progrès significatifs contre la cyberfraude pour éviter que, sur Internet, les risques ne l'emportent sur les avantages offerts aux consommateurs, et pour promouvoir de façon générale le développement économique et social. Des projets sont en cours en vue d'une réunion ministérielle sur les questions relatives aux politiques concernant Internet qui se tiendrait en 2008, soit dix ans après la précédente réunion à haut niveau de l'OCDE sur la question. La période conduisant à cette prochaine ministérielle est l'occasion idéale pour essayer de remédier aux lacunes actuelles dans la lutte contre la fraude. ■

### Pour en savoir plus

Pour plus d'informations sur les travaux de l'OCDE sur la lutte contre la fraude à la consommation, veuillez contacter : Brigitte Acoca, [brigitte.acoca@oecd.org](mailto:brigitte.acoca@oecd.org), tél. : +33 1 45 24 93 65 ou Sarah Andrews, [sarah.andrews@oecd.org](mailto:sarah.andrews@oecd.org), tél. : +33 1 45 24 90 05, ou visitez le site [www.oecd.org/sti/consumer-policy](http://www.oecd.org/sti/consumer-policy).

## Références

- OCDE (2006), **Rapport sur la mise en œuvre des Lignes directrices de 2003 régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses**, [www.oecd.org/dataoecd/2/5/37133090.pdf](http://www.oecd.org/dataoecd/2/5/37133090.pdf).
- OCDE (2006), **Boîte à outils anti-spam : Politiques et pratiques recommandées**, [www.oecd-antispam.org/IMG/pdf/Toolkit\\_2005\\_3\\_FINAL\\_FRE-2.pdf](http://www.oecd-antispam.org/IMG/pdf/Toolkit_2005_3_FINAL_FRE-2.pdf).
- OCDE (2005), **Rapport sur les campagnes d'information des consommateurs relatives aux escroqueries (« Scams »)**, [www.oecd.org/olis/2005doc.nsf/linkto/dsti-cp\(2005\)12-final](http://www.oecd.org/olis/2005doc.nsf/linkto/dsti-cp(2005)12-final).
- OCDE (2005), **Rapport général sur le règlement des litiges avec les consommateurs et la réparation sur le marché mondial**, [www.oecd.org/dataoecd/54/49/35201271.pdf](http://www.oecd.org/dataoecd/54/49/35201271.pdf).
- OCDE (2003), **Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses**, [www.oecd.org/dataoecd/24/33/2956464.pdf](http://www.oecd.org/dataoecd/24/33/2956464.pdf).
- OCDE (1999), **Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique**, [www.oecd.org/dataoecd/17/59/34023530.pdf](http://www.oecd.org/dataoecd/17/59/34023530.pdf).

---

Les publications de l'OCDE sont en vente sur notre librairie en ligne :  
[www.oecd.org/librairie](http://www.oecd.org/librairie)

Les publications et les bases de données statistiques de l'OCDE sont aussi disponibles sur notre bibliothèque en ligne : [www.SourceOCDE.org](http://www.SourceOCDE.org)

---

## Où nous contacter ?

### SIÈGE DE L'OCDE DE PARIS

2, rue André-Pascal  
75775 PARIS Cedex 16  
Tél. : (33) 01 45 24 81 67  
Fax : (33) 01 45 24 19 50  
E-mail : [sales@oecd.org](mailto:sales@oecd.org)  
Internet : [www.oecd.org](http://www.oecd.org)

### ALLEMAGNE

Centre de l'OCDE de Berlin  
Schumannstrasse 10  
D-10117 BERLIN  
Tél. : (49-30) 288 8353  
Fax : (49-30) 288 83545  
E-mail :  
[berlin.contact@oecd.org](mailto:berlin.contact@oecd.org)  
Internet : [www.oecd.org/deutschland](http://www.oecd.org/deutschland)

### ÉTATS-UNIS

Centre de l'OCDE  
de Washington  
2001 L Street N.W., Suite 650  
WASHINGTON DC 20036-4922  
Tél. : (1-202) 785 6323  
Fax : (1-202) 785 0350  
E-mail : [washington.contact@oecd.org](mailto:washington.contact@oecd.org)  
Internet : [www.oecdwash.org](http://www.oecdwash.org)  
Toll free : (1-800) 456 6323

### JAPON

Centre de l'OCDE de Tokyo  
Nippon Press Center Bldg  
2-2-1 Uchisaiwaicho,  
Chiyoda-ku  
TOKYO 100-0011  
Tél. : (81-3) 5532 0021  
Fax : (81-3) 5532 0035  
E-mail : [center@oecdtokyo.org](mailto:center@oecdtokyo.org)  
Internet : [www.oecdtokyo.org](http://www.oecdtokyo.org)

### MEXIQUE

Centre de l'OCDE du Mexique  
Av. Presidente Mazaryk 526  
Colonia: Polanco  
C.P. 11560 MEXICO, D.F.  
Tél. : (00 52 55) 9138 6233  
Fax : (00 52 55) 5280 0480  
E-mail :  
[mexico.contact@oecd.org](mailto:mexico.contact@oecd.org)  
Internet :  
[www.oecd.org/centrodemexico](http://www.oecd.org/centrodemexico)

Les Synthèses de l'OCDE sont préparées par la Division des relations publiques de la Direction des relations publiques et de la communication. Elles sont publiées sous la responsabilité du Secrétaire général de l'OCDE.