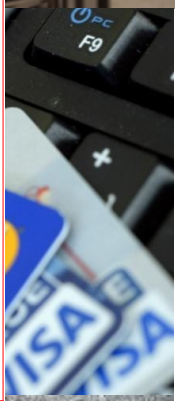



# LES ARNAQUES

## Comment les éviter ?






UFC-Que Choisir Limousin - Edition Mars 2017

# SOMMAIRE

# INTRODUCTION

## Les arnaques : Comment les éviter ?

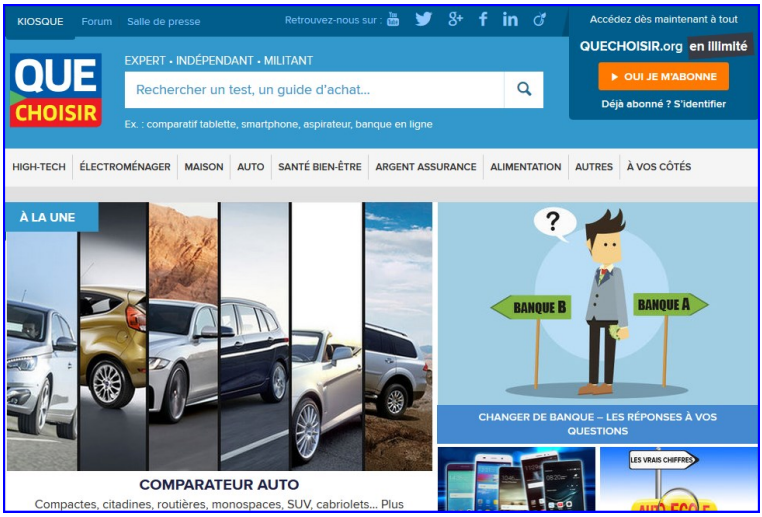
Les arnaques ? Nous aurions plutôt dû dire « Les tromperies », ou les non-respects de la règlementation.

En effet, beaucoup de litiges de consommation sont en fait une ignorance ou un refus d'appliquer les lois et les règlements.

Nous avons voulu attirer votre attention, vous informer sur les principaux domaines où nous constatons des tromperies.

Vous pourrez ainsi vous comporter en consommateurs avertis et responsables, et faire confiance à la très grande majorité de professionnels dans une relation de « Gagnant-Gagnant ».

## L'Union Fédérale des Consommateurs (UFC) Que Choisir du Limousin, Corrèze, Creuse, Haute-Vienne




*Découvrez notre site Internet www.quechoisir.org*

# DÉMARCHAGE À DOMICILE OU CONTRAT HORS ÉTABLISSEMENT

C'est une source inépuisable de tromperies en tout genre.

**Un seul remède : ne faites jamais entrer quelqu'un chez vous.**

Si cela arrive, relever les noms des personnes, de l'entreprise, le numéro d'immatriculation de la voiture.

Sachez aussi qu'un artisan, vraiment professionnel, ne fait que très rarement des opérations de démarchage à domicile ou par téléphone.

Une réglementation très précise existe pour encadrer ces pratiques. Pour éviter tout problème, il vaut mieux la connaître pour mieux la respecter.

## Les différents modes de démarchage

**Ce que dit la loi**

La loi soumet aux règles sur le démarchage les contrats conclus en dehors du lieu où le professionnel exerce son activité en permanence ou de façon habituelle. L'initiative de la conclusion du contrat n'est pas prise en considération.

Elle maintient cette protection pour les consommateurs invités à se rendre dans un magasin ou lors de voyages publicitaires (excursions).

### 1. Le démarchage spontané

C'est la situation la plus commune.

Une personne frappe à votre porte pour vous proposer d'acheter un bien ou une prestation de services.

La plupart du temps c'est à votre domicile que vous rencontrez ces situations. Mais vous pouvez aussi y être confronté(e) au travail, chez des amis…

A chaque fois que l'on vous propose de conclure un contrat en dehors du lieu où le professionnel exerce son activité en permanence ou de façon habituelle : il y a démarchage !

### 2. Le démarchage à la demande du consommateur

C'est le lieu de conclusion du contrat qui est essentiel. Peu importe que le consommateur ait contacté un professionnel pour qu'il vienne, par exemple, à son domicile afin de négocier la conclusion d'un contrat.

Les consommateurs bénéficient alors du régime de protection du démarchage comme le droit de rétractation.

Mais il y a des exceptions, par exemple, pour les ventes à domicile de denrées ou de produits de consommation courante faites au cours de tournées fréquentes (*ex. : vente de surgelés à domicile*).

**Cas particulier de l'urgence** :

Bloqué(e) devant votre porte, vous contactez en urgence un serrurier pour procéder à son ouverture. Vous vous mettez d'accord sur le coût de cette intervention.

Y a-t-il démarchage ? Est-il possible de se rétracter ?

Il s'agit bien d'un contrat hors établissement et ce, même si l'intervention du professionnel est à votre initiative.

Toutefois, dans un pareil cas, le droit de rétractation ne peut être exercé pour les pièces de rechange et les travaux strictement nécessaires pour répondre à la situation d'urgence.

Par contre, pour tous les travaux ou pièces qui ne sont pas strictement nécessaires afin de répondre à la situation d'urgence, les règles sur le démarchage s'appliquent pleinement dont le droit de rétractation, si toutes les conditions d'une opération de démarchage sont remplies.

### 3. Les sollicitations faites aux consommateurs

Afin de contourner la règlementation protectrice du démarchage, les professionnels invitent les consommateurs à se déplacer en magasin, en leur offrant des cadeaux et promotions.

Les juges avaient déjà soumis aux règles sur le démarchage ces pratiques qui ont pour seul objet d'attirer le consommateur dans le magasin afin de provoquer la vente.

La loi sur la consommation du 17/03/2014 confirme cette protection mais en précise les conditions.

**Deux hypothèses doivent maintenant être distinguées :**

A. Vous êtes physiquement sollicité dans un lieu où le professionnel n'exerce pas en permanence ou de manière habituelle son activité. Cette invitation à souscrire un contrat doit avoir été faite « personnellement et individuellement » au consommateur. Enfin, il faut que le contrat soit conclu « immédiatement » **suite à l'invitation dans le magasin du professionnel.**

B. Vous êtes physiquement sollicité dans un lieu où le professionnel n'exerce pas en permanence ou de manière habituelle son activité. Cette invitation à souscrire un contrat, doit avoir été faite « personnellement et individuellement » au consommateur. Enfin, il faut que le contrat soit conclu « immédiatement » **suite à l'invitation, via une technique de communication à distance (par Internet, téléphone).**

### 4. Les excursions

Les contrats conclus pendant une excursion organisée par le professionnel, ayant pour but ou pour effet de promouvoir et de vendre des biens ou des services aux consommateurs, sont soumis aux règles sur le démarchage.

### Et les négociations ?

La règlementation sur le démarchage s'applique lorsqu'un engagement a été conclu en dehors du lieu où le professionnel exerce son activité en permanence ou de façon habituelle.

Tant que vous n'avez pas donné votre accord à la proposition du démarcheur, il ne s'agit que de simples négociations non soumises aux règles sur le démarchage puisqu'aucun engagement n'a encore été conclu.

### En résumé, il y a démarchage quand :

- un consommateur conclut un contrat en dehors du lieu où le professionnel exerce son activité en permanence ou de façon habituelle même à son initiative,

- un consommateur se rend dans le magasin du professionnel suite à une invitation personnelle et individuelle et y conclut un contrat, immédiatement suite à l'invitation,
- un consommateur conclut un contrat, via une technique de communication à distance (ex: par Internet), immédiatement après avoir été personnellement, individuellement et physiquement sollicité dans un lieu où le professionnel n'exerce pas son activité principale en permanence ou de façon habituelle,
- un consommateur conclut un contrat, pendant une excursion organisée par le professionnel, ayant pour but ou pour effet de promouvoir et de vendre des biens ou des services.

## Foires et salons

### 1. L'obligation d'information du professionnel

La loi relative à la consommation du 17 mars 2014 a renforcé, sous peine de sanctions, l'obligation d'information du professionnel.

Ainsi, le consommateur doit être impérativement informé qu'il ne dispose pas de ce droit de rétractation.

Cette information doit être apportée par écrit en termes clairs et lisibles dans un encadré apparent dans les offres de contrat.

**Focus sur les Foires et Salons :**

- si vous avez subi des pressions, fait l'objet d'intimidations ou de chantage lors de la vente, vous pouvez demander la nullité du contrat et déposer plainte pour pratiques commerciales agressives,
- de même, si le commercial a abusé de votre faiblesse ou de votre ignorance, vous pouvez déposer plainte pour ces délits,
- si lors de la vente sur une foire, le paiement demandé est d'un montant supérieur à 200 € et inférieur à 75 000 € et qu'il est échelonné sur plus de trois mois ou sur une durée moindre mais assorti d'intérêts ou de frais non négligeables, cela est assimilé à une opération de crédit à la consommation (*Ex. : paiement d'un abri de piscine d'une valeur de 10 000 € en 5 chèques)*. C'est la règlementation sur le crédit qui s'applique.

### 2. En cas de souscription d'un crédit affecté

En cas de souscription d'un crédit affecté pour l'achat d'un bien ou d'un service conclu dans une foire ou un salon, le consommateur dispose d'un droit de rétractation. Dans ce cas, le contrat de vente ou de prestation de services doit mentionner des informations en des termes clairs et lisibles, dans un encadré apparent.

**Ainsi :**

- l'acheteur doit être informé qu'il dispose d'un droit de rétractation pour le crédit affecté servant à financer son achat,
- si l'emprunteur exerce son droit de rétractation relatif au crédit affecté, dans le délai de quatorze jours, il doit être informé que le contrat de vente ou de prestation de services est résolu de plein droit, sans indemnité,

- en cas de résiliation du contrat de vente ou de prestation de services consécutive à l'exercice du droit de rétractation, le consommateur est informé que le vendeur ou le prestataire de services est tenu de rembourser, sur simple demande, toute somme que l'acheteur aurait versée d'avance sur le prix. A compter du huitième jour suivant la demande de remboursement, cette somme est productrice d'intérêts, de plein droit, au taux de l'intérêt légal majoré de moitié.

**A retenir**
Sur les foires et salons, soyez vigilant sur ce que vous signez.

**Vous ne bénéficiez pas d'un droit de rétractation, votre engagement est donc ferme et définitif.**

**Toutefois, ce qui a changé avec la loi du 17/03/2014 :**

- Le consommateur doit être informé préalablement qu'il ne bénéficie pas d'un délai de rétractation.
- Le contrat doit faire apparaitre l'absence de ce droit, en des termes clairs et lisibles, dans un encadré apparent.

## La forme du contrat

- Le professionnel doit respecter un formalisme précis sous peine de sanctions, que ce soit lors de la délivrance des informations précontractuelles ou dans la rédaction du contrat lui-même.
- Les contrats conclus hors établissement peuvent être fournis sous format papier ou avec l'accord du consommateur, sur tout autre support durable.
- L'absence du formulaire de rétractation prolonge de 12 mois votre droit de rétractation à l'issue du délai de 14 jours initialement prévu.

Avant de vous engager, vérifiez que certaines mentions figurent bien dans le contrat de vente ou de prestation de services. Elles doivent apparaitre de manière lisible et compréhensible.

### Objet du démarchage

Sauf exclusions légales, tous les contrats de prestation de services ou de vente peuvent faire l'objet d'une opération de démarchage.
Le démarchage téléphonique fait l'objet d'une règlementation spécifique.
Certains contrats, strictement déterminés par la loi, ne vont pas être soumis à la règlementation sur le démarchage, du fait de leur objet. Les contrats qui sont conclus, sont alors irrévocables sans faculté de rétractation, et le professionnel peut exiger un paiement immédiat.

**Les exclusions légales :**

- les contrats portant sur les services sociaux, y compris le logement social, l'aide à l'enfance et aux familles, à l'exception des services à la personne,
- les contrats portant sur les services de santé fournis par des professionnels de la santé aux patients pour évaluer, maintenir ou rétablir leur état de santé, y compris la prescription, la délivrance et la fourniture de médicaments et de dispositifs médicaux,
- les contrats portant sur les jeux d'argent, y compris les loteries, les jeux de casino et les transactions portant sur des paris,

- les contrats portant sur les services financiers (*régime juridique spécifique)*,
- les contrats portant sur un forfait touristique, (*ex. : séjour acheté auprès d'une agence de voyages comprenant le transport et l'hébergement*),
- les contrats portant sur les contrats d'utilisation de biens à temps partagé, les contrats de produits de vacances à long terme et les contrats de revente et d'échange *(ex. : il s'agit des opérations de timeshare)*,
- les contrats rédigés par un officier public (*ex. : testament rédigé à domicile par un notaire*),
- les contrats portant sur la fourniture de denrées alimentaires, de boissons ou d'autres biens ménagers de consommation courante, qui sont livrés physiquement par un professionnel lors de tournées fréquentes et régulières au domicile ou au lieu de résidence ou de travail du consommateur,
- les contrats portant sur les services de transport de passagers, *(ex. : réservation d'une place de train, d'avion, de bus…),*
- les contrats conclus au moyen de distributeurs automatiques ou de sites commerciaux automatisés,
- les contrats conclus avec des opérateurs de télécommunications pour l'utilisation des cabines téléphoniques publiques ou aux fins d'une connexion unique par téléphone, Internet ou télécopie, notamment les services et produits à valeur ajoutée accessibles par voie téléphonique ou par message textuel,
- les contrats ayant pour objet la construction, l'acquisition ou le transfert de biens immobiliers, ainsi que ceux relatifs à des droits portant sur des biens immobiliers ou à la location de biens à usage d'habitation principale, conclus hors établissement.

Les placements financiers et assurances-vie font l'objet d'une règlementation spécifique.

### Ce que dit la loi

**La loi s'applique :**

- quels que soit le service concerné ou la valeur du bien,
- pour des biens soldés ou déstockés,
- pour du mobilier et partiellement pour les opérations portant sur des immeubles (construction, acquisition, location...).

Ainsi, il peut y avoir, par exemple, démarchage :

- pour un contrat de vente et de pose de panneaux photovoltaïques,
- pour les contrats de vente de portes et fenêtres/volets roulants,
- pour la vente d'un adoucisseur d'eau,
- pour des contrats de ramonage, de ravalement…

## DÉMARCHAGE TELEPHONIQUE

## Ce que dit la loi

### 1. Le régime d'opposition au démarchage téléphonique

Dorénavant, vous avez la possibilité de vous inscrire gratuitement sur une liste d'opposition qui sera **opposable à tous les professionnels**. Néanmoins, cette opposition n'a pas d'effet à l'égard des professionnels avec lesquels vous avez déjà un contrat.

En pratique, lorsque le professionnel est amené à recueillir vos coordonnées téléphoniques, **il doit vous informer de la possibilité de vous inscrire sur cette liste**.

Si c'est par le biais d'un formulaire que vos coordonnées sont demandées, vous devez retrouver cette information de manière claire et compréhensible

L'inscription sur cette liste entraîne l'interdiction de louer ou vendre tout fichier comportant vos coordonnées.

### 2. Interdiction des numéros masqués et présentation lors de l'appel

Désormais l'utilisation d'un numéro masqué est interdite par le professionnel lors d'un démarchage téléphonique.

Si vous êtes démarché par téléphone, votre interlocuteur doit, en début de conversation, vous communiquer son identité et celle de la personne pour le compte de laquelle il effectue cet appel, puis la nature commerciale de cet appel.

Ensuite, il doit vous communiquer les informations précontractuelles s'agissant des caractéristiques essentielles des biens ou des services, du prix, de la durée du contrat et de son droit de rétractation.

### 3. Quand et comment suis-je engagé ?

Le professionnel doit adresser une **confirmation par écrit ou sur un support durable** (*ex. : mail*) de l'offre qu'il a faite.

Cette confirmation doit reprendre, comme pour les contrats conclus hors établissement, les mentions suivantes :

- les informations liées à la possibilité de se rétracter ou pas,
- les frais de renvoi de la marchandise suite à cette rétractation,
- les informations relatives aux professionnels ainsi que les conditions générales et garanties applicables au contrat.

Si le professionnel a omis de vous communiquer ces informations, d'une part par téléphone puis sur tout support durable (papier, mail, ...), vous pouvez demander la nullité du contrat. Vous ne serez engagé que par votre signature et votre acceptation écrite.

La loi du 17/03/2014 ajoute à ces dispositions que **votre consentement peut être donné par voie électronique.**

Les règles, s'agissant du démarchage téléphonique, s'appliquent aussi bien à l'occasion **de la souscription d'un contrat qu'à la modification d'un contrat en cours.**

**Exemple :** vous êtes contacté par téléphone par votre opérateur mobile actuel, qui vous propose un nouveau téléphone assorti d'un réengagement de 24 mois.

Votre opérateur doit vous envoyer une confirmation de l'offre mais surtout vous ne serez engagé que par votre signature manuscrite ou électronique.

Si vous avez souscrit votre **contrat avant le 14 juin 2014**, il est peu probable que vous puissiez bénéficier des règles applicables au démarchage.

En effet, les tribunaux ont parfois estimé que le démarchage ne visait que la prospection de nouveaux clients, qu'en conséquence, la modification d'un contrat existant même signé à domicile ne permettait pas de bénéficier des dispositions relatives au démarchage.

Dans cette hypothèse, votre simple acceptation par téléphone était suffisante et ce sont les règles de la vente à distance qui s'appliquaient, votre signature n'étant pas une condition nécessaire.

**A retenir**
C'est au professionnel de prouver, d'une part, que les informations précontractuelles vous ont été communiquées et, d'autre part, de prouver votre engagement par l'apposition de votre signature sur le contrat ou par voie électronique.

## Le financement du contrat

*« Vous pouvez choisir de financer ce contrat de 2 manières : soit en réglant au comptant (espèces, chèque, carte bancaire…), soit à crédit ».*
*« Monsieur, je vous demande de me verser un acompte pour valider le dossier auprès de mon directeur... ».*

Voici des phrases que vous avez peut-être déjà entendue de la part d'un professionnel venu chez vous pour conclure un contrat de vente ou de prestation de services.

Quelque soit le mode de paiement choisi, est-ce qu'un démarcheur peut légalement vous demander un règlement immédiat ?

### Ce qui dit la loi

**Paiement au comptant**
La loi a posé un principe d'interdiction : le professionnel ne peut pas recevoir un paiement ou une contrepartie, sous quelque forme que ce soit, de la part du consommateur avant l'expiration d'un délai de sept jours à compter de la conclusion du contrat hors établissement.

Cependant il existe des exceptions légales à ce principe d'interdiction qui concernent :

- les contrats d'abonnement à une publication quotidienne et assimilée,
- les ventes organisées au domicile d'un consommateur ayant accepté cette opération *(ventes « Tupperware »),*
- les contrats à exécution successive proposés par un organisme agréé ayant pour objet la fourniture de services à la personne (*garde d'enfant, assistance aux personnes âgées…*),

- les travaux de réparation et d'entretien réalisés en urgence au domicile du consommateur et expressément sollicités par lui, mais dans la limite des pièces de rechange et travaux strictement liés à l'urgence.

### Quelles contreparties sont interdites par la loi ?

Pour répondre à cette question, la jurisprudence antérieure à la loi relative à la consommation aura certainement vocation à s'appliquer.

En effet, le nouvel article L121-18-2 du Code de la consommation reprend la même interdiction qui figurait déjà dans l'ancien article L121-21 du même Code.

**Ainsi, le professionnel ne peut pas vous demander de lui remettre :**

- un paiement en espèces,
- la remise d'un chèque y compris de réservation, même non encaissé ou antidaté. Vous ne pouvez faire opposition sur un chèque qu'en cas de perte ou de vol,
- une autorisation de prélèvement, peu importe que celle-ci puisse être révoquée par la suite par le signataire (*Cour d'appel de Saint-Denis de la Réunion du 01/02/2013 n°11/00276*),

La preuve que l'autorisation de prélèvement a été signée après et non avant la fin du délai de rétractation incombe au démarcheur (*Cour d'appel de Grenoble du 03/03/2009 n°07/00003*).

### Quelles sont les sanctions en cas de paiement malgré son interdiction ?

Outre les sanctions pénales, la demande illégale de paiement entraîne la nullité du contrat.

En effet, cette sanction, résultant du non-respect d'une disposition d'ordre public a été retenue par la jurisprudence établie avant la loi du 17/03/2014. Sachez que la nullité du contrat peut être soulevée d'office par un juge saisi du litige.

**A retenir**

Une demande de paiement comptant avant l'expiration d'un délai de 7 jours est, en principe, interdite.

Le recours au crédit doit être mentionné sur le contrat.
En cas de souscription d'un crédit affecté, aucun paiement comptant ne peut intervenir avant l'expiration du délai de 14 jours calendaires, correspondant au délai de rétractation du crédit.

### Financement du contrat avec un crédit

Un autre mode de financement du contrat est possible : la souscription d'un crédit à la consommation.

Il s'agit d'un prêt consenti par un établissement de crédit d'un montant supérieur à 200€ et inférieur à 75000€. Son remboursement doit être prévu sur une période de plus de 3 mois ou sur une durée moindre si les intérêts ou les frais ne sont pas négligeables.

La Cour de cassation a déjà jugé qu'il est possible d'accepter une offre de crédit à la consommation pendant le délai de renonciation dès lors qu'elle n'est pas accompagnée d'une autorisation de prélèvement.

**Conseil** : Certains démarcheurs font pression pour faire accepter aux clients une livraison anticipée, voire immédiate.

D'autres proposent, avec de faux arguments, d'anticiper le contrat dans le but de faire échec à votre droit de renonciation et être payés rapidement par l'organisme de crédit.

N'acceptez pas de souscrire à de telles manœuvres.

Au contraire, veillez bien à ce que soient bien indiqués sur le contrat la date et le lieu de sa signature pour bénéficier des dispositions protectrices du démarchage. Refusez une livraison anticipée et ne signez pas un bon de livraison alors que celle-ci n'est pas effective.

## Le droit de rétractation.

### L'obligation d'information du professionnel

Le professionnel doit, avant la conclusion du contrat, vous communiquer les conditions, délai et modalités d'exercice de ce droit de rétractation lorsqu'il existe.

Le professionnel doit **aussi informer le consommateur clairement lorsque ce droit ne peut être exercé** ou, le cas échéant, des circonstances dans lesquelles le consommateur perd cette faculté.

L'information précontractuelle s'agissant du droit de rétractation doit se faire sur papier ou, sous réserve de l'accord du consommateur, sur un support durable (*ex. : mail*).

Outre la faculté de se rétracter (ou pas), **ce support devra comprendre toutes les informations précontractuelles sous peine de nullité**.

Dans tous les cas, ces informations doivent être rédigées de manière lisible et compréhensible.

### Comment faire pour se rétracter

Votre contrat doit reprendre toutes les informations précontractuelles dont **le formulaire type de rétractation**, sous peine de nullité.

Le contrat remis doit mentionner cette faculté de rétractation et comporter un formulaire détachable destiné à en faciliter l'exercice sur support papier ou support durable.

Mais le consommateur reste libre d'exercer ce droit par courrier, dénué d'ambiguïté, exprimant sa volonté de se rétracter.

La seule exigence est de **renvoyer le formulaire et d'envoyer le courrier en LRAR dans le délai de 14 jours**.

La loi relative à la consommation permet dorénavant au consommateur, en plus de sa rétractation « postale », de remplir et transmettre en ligne sur le site du professionnel, le formulaire ou la déclaration permettant sa rétractation.

Dans ce cas, le professionnel devra lui communiquer sans délai un accusé de réception.

**Néanmoins, deux précisions s'imposent :**

- le professionnel **peut** prévoir sur son site la « **rétractation numérique** », mais il ne s'agit pas d'une obligation,

- en cas de contestation, c'est au consommateur de prouver qu'il a bien exercé sa rétractation dans les délais, qu'elle soit postale ou numérique.

La **rétractation par courrier** est faîte en LRAR : c'est l'accusé de réception qui permettra au consommateur d'établir la réalité de l'envoi et sa date.

S'agissant de la **rétractation numérique,** la question est plus délicate. Le consommateur doit prendre soin de faire une impression écran si la rétractation se fait via un formulaire sur le site du professionnel.

Si le professionnel a prévu une rétractation par mail, il est recommandé de demander un accusé de réception.

### Le point de départ du délai de rétractation

Le Code de la consommation prévoit que le consommateur dispose d'un délai de 14 jours pour exercer son droit de rétractation.

Ces dispositions sont d'ordre public, ce qui signifie qu'aucune clause du contrat ne peut y déroger.

Le délai commence à courir **le jour de la conclusion du contrat ou le jour de la réception des biens**.

La loi du 17/03/2014 ne prévoit aucune prorogation de ce délai s'il s'achève un samedi, un dimanche ou un jour férié.

Si le professionnel a omis de communiquer les informations relatives au droit de rétractation pendant 14 jours, ce délai est prolongé de 12 mois à compter de l'expiration du délai initial.

Toutefois, si ces informations sont fournies pendant cette prolongation de 12 mois, le délai expire au terme d'une période de 14 jours à compter du jour où le consommateur a reçu ces informations.

### Les effets de la rétractation

L'exercice du droit de rétractation entraîne un certain nombre d'obligations pour les parties, s'agissant du renvoi de la marchandise, de ses modalités et du remboursement par le professionnel.

**Le renvoi des biens.**

Une fois la rétractation envoyée, le consommateur doit renvoyer la marchandise dans un délai maximal de 14 jours suivant la communication de sa décision de se rétracter.

Les conditions générales du professionnel peuvent prévoir que c'est le professionnel lui-même qui se chargera de récupérer le(s) bien(s).

**Les frais liés à ce renvoi.**

Les coûts directs de renvoi des biens, et uniquement ceux-là, restent à la charge de l'acheteur sauf dispositions plus favorables dans le contrat ou si le consommateur n'a pas été informé que ces frais étaient à sa charge.

Une seule exception est prévue : s'agissant des marchandises qui par leur nature (*ex. : imposante*) ne peuvent être renvoyées par voie postale, lorsqu'ils ont été livrés au domicile du consommateur au moment de la conclusion du contrat. Dans ce cas, le professionnel les récupère à ses frais.

**Le remboursement du prix.**
En principe, que le contrat porte sur la vente de biens ou la réalisation de prestations de services, le professionnel doit rembourser le consommateur dans un délai maximal de 14 jours à compter de la date à laquelle il a été informé de sa décision de se rétracter. Il s'agit donc de la date à laquelle il reçoit la rétractation et non de la date d'envoi de celle-ci.

Néanmoins, cette nouvelle loi donne la faculté au professionnel, pour les contrats de vente de biens, de différer ce remboursement jusqu'à récupération des biens ou jusqu'à ce que le consommateur ait fourni une preuve de l'expédition de ces biens.

L'article précise que la date retenue pour le point de départ du délai de 14 jours sera la date du premier de ces faits.

En pratique, ce sera la date de réception des biens par le professionnel si, à cette date, il n'a pas reçu l'avis d'envoi du colis contenant les marchandises par le consommateur.

**A retenir**
Le délai commence à courir **le jour de la conclusion du contrat ou le jour de la réception des biens**.

Si le professionnel a omis de communiquer les informations relatives au droit de rétractation pendant 14 jours, ce délai est prolongé de 12 mois à compter de l'expiration du délai initial.

## DÉPANNAGE A DOMICILE : NE VOUS FAITES PLUS AVOIR !

Clé oubliée à l'intérieur ou perdue, lavabo bouché ou tuyau qui fuit ? Vous devenez la proie idéale pour les entreprises de dépannage à domicile, facture exorbitante garantie. Alors, que faire ?

## Les bonnes pratiques et les vrais prix (2012)

### SERRURERIE

50 % des plaintes enregistrées sur le dépannage à domicile en 2011 concernaient l'ouverture de porte. C'est une mine d'or inépuisable pour les professionnels sans scrupule.

**La porte est simplement claquée**
C'est la situation la plus courante. On oublie ses clés en sortant ou un courant d'air referme la porte alors qu'on est à deux pas.

**Que faire ?**
Pas de panique, gardez la tête froide. Il est inutile de recourir au dépannage d'urgence, ouvrir une porte fermée du moment qu'elle n'est pas verrouillée est à la portée d'à peu près tout le monde.

Il suffit d'un cliché de radiographie médicale et, bien entendu, d'un peu de persévérance quand on n'est pas spécialiste.

Plutôt que de chercher frénétiquement un serrurier sur les Pages Jaunes ou sur Internet, mettez-vous en quête d'une radiographie.

Sollicitez vos voisins et vos proches, il est rare que personne n'ait jamais passé d'examen radiologique dans une famille. Si la porte vous résiste, faites appel à un bricoleur de votre entourage.

Nous avons fait l'expérience, l'ouverture ne prend que quelques minutes, le temps de bien positionner le cliché et de pousser au bon instant.

**Et si les clés sont à l'intérieur sur la porte ?**
Ça ne change strictement rien pour l'ouverture avec une radiographie.

En revanche, si vous comptiez sur le double des clés confié à un voisin ou un proche pour entrer, il ne sera d'aucun secours.

**Et si la porte est blindée ?**
*« Votre porte est blindée, elle est impossible à ouvrir sans toucher à la serrure »*, c'est une des grosses ficelles des dépanneurs indélicats pour justifier de la casser et de la remplacer !
En réalité, ça ne change rien, une porte blindée avec serrure multipoints s'ouvre de la même façon qu'une porte standard tant qu'elle n'est pas verrouillée.

*« Toutes les portes s'ouvrent à la radiographie ou au fil de fer, on ne touche jamais au cylindre »*, confirme un serrurier, 34 ans de métier.

Prix 2012 à Paris : Ouverture porte claquée : 80 à 100 € en journée, 110 à 140 € le soir ou le week-end.

**La porte est fermée à clé, vous avez perdu vos clés**
L'intervention d'un serrurier est indispensable. Les dépanneurs sans scrupule cassent pour changer toute la serrure ; en réalité, ce n'est pas nécessaire.

Tout se passe au niveau du cylindre, les serruriers très aguerris peuvent même ouvrir avec délicatesse sans l'abîmer. Mais inutile de rêver, ils sont peu nombreux et ce travail minutieux demande du temps.

Dans la pratique, le serrurier perce le cylindre, c'est plus rapide. Ensuite, il faut le remplacer mais les clés étant perdues, c'était de toute façon nécessaire.

Il arrive qu'un serrurier soit contraint de remplacer la serrure mais c'est rare. *« Neuf fois sur dix, il faut détruire le cylindre,* explique un serrurier depuis plus de 30 ans, *mais je remplace seulement le cylindre, jamais le bloc serrure. Il y a une seule exception, c'est la marque Picard, là on n'a pas le choix. Mais s'en tenir au remplacement du cylindre est possible sur les autres marques ».*

**Bon à savoir.**
Un vrai serrurier n'abîme jamais la porte, il ne la perce pas. Dans le pire des cas, il détruit le cylindre.

Prix 2012 à Paris : Porte fermée à clé : 90 à 140 € pour l'ouverture ; 150 à 350 € pour le changement de cylindre, selon gamme et marque.

**Pour votre sécurité, enfermez-vous**
Une porte non verrouillée peut s'ouvrir avec une radiographie.

Du coup, on comprend mieux la mise en garde qui figure sur le site Internet de Fichet, spécialiste de la serrure de sécurité et de la porte blindée : *« Une porte simplement claquée, même s'il n'y a pas de poignée mobile extérieure, n'est pas une porte fermée. Sans être experte, une personne peut ouvrir votre porte en quelques secondes et sans aucun bruit ».*

Pour éliminer tout risque d'intrusion par la porte d'entrée et se sentir en sécurité, *Que Choisir* recommande donc de fermer à clé dès qu'on rentre chez soi, même si la porte n'a pas de poignée côté extérieur.

## PLOMBERIE

Après l'ouverture de porte, le dépannage en plomberie occupe la deuxième place en matière d'arnaques. Pourtant, fermer un robinet suffirait bien souvent.

**Une fuite d'eau**
Pas d'urgence. D'après le Président de la CAPEB (Confédération de l'Artisanat et des Petites Entreprises du Bâtiment) Grand Paris.

*« L'urgence n'existe pas en plomberie, quand il y a une fuite, la seule chose à faire c'est de fermer le robinet d'arrivée d'eau, au niveau de l'appareil en cause ou du logement selon l'origine, mais la réparation peut toujours attendre le lendemain ou le lundi matin.*

*Si je me déplace un soir ou un week-end chez un client, c'est pour fermer le robinet d'arrivée d'eau parce qu'il ne l'a pas trouvé. La seule urgence, c'est l'inondation. Mais dans ce cas on appelle les pompiers, pas un service de dépannage ».*

**Les WC bouchés**
C'est sans doute la seule véritable urgence en plomberie mais elle se produit rarement par hasard.

Bloc désodorisant ou serviette hygiénique qui tombe dans la cuvette, tuyau ancien qui n'a jamais été curé, ce sont les causes les plus fréquentes.

Pour un bloc désodorisant, inutile d'attendre. *« Faites bouillir de l'eau et versez-la aussitôt pour ramollir le plastique, parfois ça suffit pour l'évacuer. Sinon, il faut intervenir avec une pompe »,* conseille un plombier.

Quand la pompe manuelle ou la tringle ne suffisent pas, ou s'il y a un dégorgement important, les plombiers recourent au camion pompe, c'est rapide, efficace, mais cher.

**Le chauffe-eau électrique fuit**
C'est une cause fréquente de surfacturations, alors qu'on peut facilement parer au plus pressé. *« Quand un client m'appelle en urgence pour ce type de problème, je le dépanne par téléphone. Je lui dis de fermer le robinet d'arrivée d'eau et de chercher le fusible sur le tableau électrique pour mettre son ballon en sécurité. S'il faut vidanger le ballon, je l'explique aussi par téléphone, ça lui permet de patienter ».*

Prix 2012 à Paris : WC bouchés : 300 € maximum, nuit ou week-end ; 350 € à 600 € pour le camion pompe (Montant parfois supérieur en assainissement non collectif, intervention sur demande du syndic en immeuble).

## Dépannage à domicile : Comment éviter les arnaques

Les erreurs à éviter et les conseils à suivre avant de faire appel à un spécialiste du dépannage à domicile.

### Les règles incontournables pour se protéger

- Jeter tous les cartons publicitaires ou soi-disant « officiels » trouvés dans sa boîte aux lettres.
- Éviter d'aller sur Internet pour chercher un pro du dépannage. En tapant dépannage, serrurier ou plombier, on tombe rarement sur les professionnels honnêtes.
- Entrer les coordonnées de son plombier et d'un vrai serrurier compétent dans son téléphone portable pour savoir qui appeler en cas de catastrophe.
- Passer la nuit chez des proches ou à l'hôtel plutôt qu'appeler un serrurier au hasard.
- Fermer le robinet d'arrivée d'eau de son logement si son plombier n'est pas disponible aussitôt au lieu de faire intervenir n'importe qui.

Une nouvelle règlementation est entrée en vigueur : obligation de donner ses tarifs sur le site Internet du professionnel.

### Les 7 erreurs à éviter

**Consulter les Pages Jaunes**.
Tout se paie, en particulier une place bien visible et une publicité sur les Pages Jaunes, en version papier ou sur Internet.

Les professionnels sérieux n'ont pas les moyens de financer cette visibilité. Seule la surfacturation des prestations le permet.

Une entreprise a ainsi consacré plus de 3 millions d'euros à la publicité Pages jaunes sur un an.

**Chercher sur Internet**
Quand on tape les mots : artisan, serrurier, plombier, dépannage, et tout ce qui s'en approche, ce ne sont jamais les artisans sérieux qui apparaissent.

Là encore, tout est question d'argent. Arriver en bonne place quand un internaute lance une recherche, cela se paye. Pour une bonne visibilité sur Google, c'est plus de 300 000 €.

Votre plombier ou votre serrurier de quartier n'en a pas les moyens, même s'il assure un service de dépannage en urgence.

**Appeler un des numéros d'urgence du carton trouvé dans votre boîte aux lettres**

En voyant cette carte, on pense à une information officielle de la Mairie ou de la Préfecture. Faux ! Au verso, en caractères minuscules, voire comment elle est signée.

La stratégie des dépanneurs est toujours la même. On fournit tous les numéros utiles des services de la ville, les numéros d'urgence, Samu, pompiers…

On donne au carton l'aspect d'un document officiel, on insère son numéro en gros caractères pour faire penser qu'il en fait partie, ou on multiplie les numéros par type de dépannage pour faire croire à des services différents.

En réalité, c'est toujours la même entreprise. Les Mairies (comme les services d'urgence) et les Préfectures ne cautionnent jamais ces cartes.

Il s'agit d'une utilisation frauduleuse de leur nom, de leur blason. Mais on se fait facilement avoir tant la présentation est trompeuse. Comme cette carte postale d'une Mairie avec la mention *« informations utiles et numéro de téléphone »*.

**Aller au commissariat**

Diriger les consommateurs vers une entreprise ou une autre ne fait pas partie des missions de la police.

Plutôt que de vous voir désemparé, certains vous tendent une carte ou un numéro de téléphone d'urgence.

Attention, c'est un de ces cartons qui inondent les boîtes aux lettres, les commissariats n'échappent pas à la distribution de masse.

**Vouloir le prix le plus bas**

*« Quand une personne à la porte de son logement appelle, la première question qu'elle nous pose, c'est toujours : combien prenez vous ? »*

*« Commencer comme ça, c'est se jeter dans la gueule du loup. Un serrurier honnête n'est jamais compétitif à ce petit jeu-là »*, témoigne un professionnel.

De fait, des promesses telles que *« ouverture de porte : 26 € TTC »*, *« ouverture de porte claquée 39 € tarif agréé »*, sont impossibles à tenir.

Tarif agréé par qui d'ailleurs ? Au téléphone, face à notre question insistante, on a fini par nous lâcher : *« Par nous-mêmes ! »*

**Faire confiance à l'AFDCE**

C'est l'Association Française de Défense des Consommateurs Européens. Le nom est pompeux, il inspire confiance.

Pourtant, il n'a strictement rien à voir avec une association de protection des consommateurs, c'est une trouvaille de dépanneurs à domicile pour mieux ferrer les clients.

On y retrouve du beau monde dans le collimateur de la justice.

**Se fier à la mention « agréé par les grandes marques ».** Ça ne veut rien dire, c'est abusif.

Ce n'est pas parce qu'on commercialise des serrures ou des produits de différentes marques qu'on est agréé par elles.

## Les 7 conseils à suivre

**Dormez plutôt chez un proche ou à l'hôtel**
Tant qu'on n'a pas vécu de dépannage cauchemardesque, on trouve le conseil farfelu. Mais si on s'attendait à payer 2 000 à 4 000 € pour faire ouvrir sa porte, on choisirait certainement d'aller coucher ailleurs.

Alors, plutôt que courir ce risque très élevé, faites-vous héberger par un proche ou passez la nuit à l'hôtel.

**Coupez l'eau**
S'il y a une fuite d'eau, coupez le robinet d'arrivée et écopez. C'est le plus sûr moyen d'éviter la facture démentielle et les travaux inutiles.

Et si l'eau vous manque trop, allez dormir ailleurs. Appeler votre plombier le lendemain ou le lundi vous coûtera moins cher.

**Exigez un devis écrit**
Les dépanneurs sont malins, ils annoncent souvent le montant du devis tout en dévissant ou en perçant.

Ils sont si concentrés que vous n'exigez pas de trace écrite. C'est gagné, la facture délirante est en marche.

Malgré l'urgence, exigez un devis écrit dès que le problème est identifié, avant que la réparation ne débute.

**Conservez toutes les pièces remplacées**
Sur les nombreuses factures aux montants malhonnêtes reçues à l'UFC-Que Choisir, la case « enlèvement du matériel » est souvent cochée « oui ».

C'est un beau cadeau fait au dépanneur, cela lui évite le risque d'être poursuivi pour avoir changé des pièces en parfait état.

Les éléments remplacés vous appartiennent, exigez de les conserver quand la facture est lourde.

**Alertez les autorités compétentes**
Envoyez un courrier, en y joignant la facture, à votre DDPP (Direction Départementale de la Protection des Populations), ou la DDCSPP (Direction Départementale de la Cohésion Sociale et de la Protection des Populations).

Les DDPP et DDCSPP engagent des procédures judiciaires quand elles ont suffisamment de plaintes. S'il y a procès, vous toucherez des dommages et intérêts.

**Trouvez un professionnel honnête**
Bien sûr, en dénicher un qui soit disponible le soir ou le week-end n'a rien d'évident.

**Pour la serrurerie**.
À titre préventif, faites le tour de votre quartier ou de votre commune pour repérer un vrai serrurier.

Demandez-lui s'il lui arrive de faire des dépannages à domicile. Si c'est le cas, enregistrez son numéro sur votre portable, cela peut un jour vous éviter de débourser 4 000 €.


*Abonnez-vous et recevez tous les trimestres notre magazine Spécial*

**Pour la plomberie**.
Il n'existe pas de réseau d'urgence constitué de vrais professionnels en plomberie.

À titre préventif, demandez à votre plombier chauffagiste son numéro de portable. Le soir ou le week-end où vous serez en rade, il acceptera peut-être de venir ou au moins de vous conseiller la marche à suivre par téléphone.

Si vous ne connaissez pas de plombier, consultez votre entourage et vos voisins. Ils ont peut-être une bonne adresse à vous communiquer, prenez le numéro au cas où.

Sinon, contactez la CAPEB (Confédération de l'Artisanat et des Petites Entreprises du Bâtiment) de votre département, les adhérents sont tous artisans, ce n'est pas une garantie absolue mais ce sont de vrais professionnels, contrairement à la plupart des dépanneurs, et leur entreprise est là pour durer. Ils ont tout intérêt à satisfaire et fidéliser la clientèle.

**A noter** : avoir le réflexe de fermer l'eau si le problème intervient le week-end et d'appeler le lundi matin !

**Bon à savoir**
Les contrats d'assurance multirisques habitation comportent parfois une clause sur les dépannages d'urgence à domicile.
Mais les contrats ne mettent pas à l'abri des dépanneurs indélicats. Le risque est à priori moindre avec un contrat d'assistance si vous pouvez joindre un numéro d'urgence 24 h/24 qui vous dirige vers un professionnel référencé.


*Abonnez-vous et recevez tous les mois notre magazine*


***Les livres de Que Choisir Edition :***
*une série de guides à commander sur notre site Internet www.quechoisir.org*

# TELEPHONE

Les principales fraudes : rappel N° surtaxé, renseignements téléphoniques surtaxés, SMS indésirables et appels frauduleux, harcèlement téléphonique, arnaque au colis en attente à retirer.

## Rappel N° surtaxé

Un appel malhonnête (« ping call » ou **spam vocal**) ou un **SMS indésirable** sont des fraudes utilisant comme combine le rappel vers un numéro surtaxé.

Le message reçu comporte soit une demande d'un organisme officiel (EDF, Impôts, etc…) soit une demande de la part d'une relation ou d'une parenté. Il incite le consommateur à appeler un numéro surtaxé.

Pour ne pas susciter la méfiance de leurs victimes, les escrocs passent désormais leurs appels depuis des numéros en 01, 02, 05 etc..., plutôt que des 0 892 ou 0 899 trop visible.

### Conseils :

Un système de signalement permet de lutter contre les SMS indésirables et appels frauduleux : le numéro téléphonique « **33700** » est mis en place par la Fédération Française des Télécoms (FFT). Il permet aux consommateurs d'alerter gratuitement les opérateurs sur des SMS ou appels téléphoniques qu'ils jugent suspects.

**Sur les smartphones, pour les SMS indésirables.**

Vous pouvez transférer systématiquement le SMS indésirable vers le 33700 (SMS gratuit).

Cette plateforme envoie un accusé de réception et demande au consommateur de transmettre le numéro d'envoi de l'émetteur.

Le consommateur envoie un second SMS avec le numéro de l'émetteur (SMS gratuit).

Le 33700 envoie un SMS de remerciement afin de clore le signalement.
La plateforme 33700 informe les opérateurs mobiles et fixes concernés par les numéros signalés.

Les opérateurs télécoms, sur la base de ces signalements, en fonction de leur récurrence et de leur gravité, peuvent prendre des sanctions contre les expéditeurs de messages, allant jusqu'à la fermeture des numéros surtaxés. Se méfier des invitations lancées sur Facebook ou autres sites communautaires par de soi-disant amis (la plupart du temps des profils d'amis réels usurpés) et qui incitent à rappeler des numéros surtaxés.

## Renseignements téléphoniques : les mauvais coûts des 118

Dix ans après le remplacement du « 12 » par des numéros en 118, le marché des renseignements téléphoniques est devenu complètement fou.

Entre règlementation non respectée et tarifs prohibitifs, l'ouverture à la concurrence de ce service a tourné au fiasco.

S'il est un secteur où la libéralisation n'a pas permis de faire baisser les prix, c'est bien celui des renseignements téléphoniques.

**Les tarifs des numéros en 118 XYZ n'ont cessé d'augmenter depuis dix ans, jusqu'à atteindre des sommets.**
Aujourd'hui, le moindre appel vers l'un de ces services coûte au minimum 2 €, auxquels s'ajoutent entre 50 centimes et 2,99 € par minute passée en ligne.

Une fortune, surtout quand on sait que le temps qui s'écoule après la mise en relation est facturé au même prix que les premières minutes.

Résultat : le fait de rester en ligne dix minutes avec son interlocuteur après avoir été mis en relation par un 118 peut générer une facture dépassant les 30 €, alors que la même communication aurait eu de grandes chances d'être gratuite si l'appelant avait composé lui-même le numéro.

Longtemps en décroissance, le marché des 118 connaît un certain regain d'intérêt ces derniers mois avec le lancement de nouveaux services qui vont au-delà de la simple recherche de numéro.

Certains se vantent de pouvoir remplacer les services clients des grandes marques, d'autres proposent de réserver un billet d'avion à votre place ou de faire venir chez vous un plombier.

**Des services plus ou moins utiles qui ont pour point commun de coûter cher !**
Attention au service de renseignements par téléphone d'un nouveau genre, où les conseillers cherchent à résoudre eux-mêmes les problèmes des personnes qui les appellent, avant de les diriger si nécessaire vers le bon interlocuteur.

Ce service est facturé au prix fort : plus de 2 € l'appel, puis x € la minute, y compris après l'éventuelle mise en relation.

## Pour les appels frauduleux « spam vocal » ou « ping call »

Ce système consiste, dès lors qu'il y a un appel en absence jugé suspect, à le signaler via l'envoi d'un SMS au numéro « 33700 », en inscrivant, dans le corps du message :
La mention « ***Spam vocal*** » suivie du ***numéro de téléphone incriminé***.

Exemple : « **spam vocal 089X XX XX XX** »
La plateforme 33700 envoie au consommateur un accusé de réception spécifique :
« *Service 33700. Merci pour ce signalement. Votre coopération va nous permettre de lutter contre ces appels indésirables* ».

Un site Internet permet de signaler un spam vocal en remplissant un formulaire en ligne sur : www.33700.fr/

De même, si vous avez été victime de cette escroquerie, vous pouvez contacter le numéro sur le site du Ministère de l'Intérieur « Info escroquerie » ou au 0805 805 217.

**Conseils :**
Dans tous les cas, **éviter de répondre à certains numéros téléphoniques inconnus ou surtaxés.**

Pour vérifier un faux numéro téléphonique, voir aussi « fauxnumeros.fr »

## Cas particulier : harcèlement téléphonique

### Ne pas confondre harcèlement téléphonique et démarchage commercial abusif.

Le harcèlement téléphonique se caractérise par des appels répétés et malveillants émis dans le but d'importuner une personne.

Ce comportement peut être caractérisé lorsque l'auteur des faits se contente de laisser des messages vocaux ou des appels en absence à la victime.

L'envoi répété de SMS ou de courriers électroniques malveillants est également assimilé à du harcèlement téléphonique.

Ces agissements ont pour objectif ou pour effet de dégrader les conditions de vie de la victime (sonneries intempestives, anxiété, peur…).

Ils constituent également un délit. En effet, l'article L.222-16 du Code pénal dispose que « les appels téléphoniques malveillants réitérés, les envois réitérés de messages malveillants émis par la voie des communications électroniques ou les agressions sonores en vue de troubler la tranquillité d'autrui, sont punis d'un an d'emprisonnement et de 15000 € d'amende ».

### Quels sont vos droits dans ces deux cas ?

Si vous estimez être victime de l'un de ces délits, vous pouvez vous adresser au commissariat de police ou à la gendarmerie de votre domicile, qui sont seuls compétents pour enregistrer votre plainte et y donner les suites appropriées.

Seules les juridictions pénales sont compétentes pour prononcer des sanctions à l'encontre des auteurs de ces infractions.
Pour plus d'informations, vous pouvez consulter l'adresse suivante : « http://vosdroits.service-public.fr/particuliers/F32235.xhtml »

### Le démarchage commercial par des moyens de communications électroniques ne relève pas du harcèlement téléphonique.

Si vous estimez être sollicités par un commerçant par le biais d'appels de prospections commerciales non-désirés, gênants ou abusifs, vous avez la possibilité de signaler ces appels par le biais d'un télé-service. Vous trouverez les informations nécessaires à ce signalement en consultant le site suivant : www.bloctel.gouv.fr

### Le service Bloctel : la nouvelle liste d'opposition au démarchage téléphonique depuis le 1er juin 2016

Depuis le 1er juin 2016, la nouvelle liste d'opposition au démarchage téléphonique a été effectivement ouverte.

**Les consommateurs peuvent s'inscrire gratuitement sur ce registre d'opposition.** Pour cela, sur le site **www.bloctel.gouv.fr**, ils doivent entrer leur(s) numéro(s) de téléphone fixe(s) et/ou portable(s).

Ils recevront alors un récépissé précisant la date à laquelle leur inscription sera effective. L'inscription sera effective au maximum 30 jours après la réception du récépissé.

Le récépissé mentionnera également la durée d'inscription sur la liste d'opposition, à savoir 3 ans. Et 3 mois avant l'expiration de ce délai de 3 ans, les consommateurs seront contactés par courriel ou courrier postal pour renouveler, s'ils le souhaitent, l'inscription de leur(s) numéro(s) sur le registre d'opposition.

Si les appels continuent, les consommateurs pourront s'identifier sur le site **www.bloctel.gouv.fr** afin de remplir le formulaire de réclamation.

Les services de la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) mèneront les enquêtes nécessaires.

**Toutefois, le démarchage restera autorisé dans les situations suivantes :**

- en cas de relations contractuelles préexistantes (par exemple, votre banque pourra continuer à vous appeler pour vous formuler des offres),
- en vue de la fourniture de journaux, de périodiques ou de magazines,
- de la part d'instituts de sondage ou d'associations à but non lucratif, dès lors qu'il ne s'agira pas de prospection commerciale.

Les spams vocaux et les SMS, pour lesquels il existe déjà un numéro de signalement, ne sont pas concernés par Bloctel.

Ils doivent être renvoyés par SMS au 33700. En outre, sachez que tous les opérateurs de téléphonie proposent à leurs abonnés de s'inscrire gratuitement sur une liste d'opposition.

**Il existe 2 types de listes d'opposition :**

- **la liste rouge** : les coordonnées téléphoniques de la personne inscrite sur cette liste ne sont pas mentionnées sur les listes d'abonnés ou d'utilisateurs,
- **la liste orange** : les coordonnées téléphoniques de la personne inscrite sur cette liste orange ne sont plus communiquées à des entreprises commerciales en vue d'une utilisation à des fins de prospection directe. Mais elle continue de figurer dans l'annuaire universel.

## Arnaque au Colis en attente à retirer

Après les avis de passage dans les boîtes aux lettres, les messages par téléphone et les SMS, les arnaques au colis en attente passent désormais de plus en plus souvent par e-mail.

Apprenez à repérer ces escroqueries qui n'ont d'autre but que de vous faire appeler un numéro surtaxé.

La technique de fraude au colis n'a cessé d'évoluer. Certaines victimes ont été contactées par le biais de messages laissés sur leur répondeur ou par des SMS reçus sur leur smartphone.

Mais aujourd'hui, c'est par e-mail que ces arnaques transitent en majorité.

**Si le mode de communication change, le principe, lui, reste globalement le même.**

Censé émaner d'un transporteur connu (Chronopost et Colissimo sont les noms les plus fréquemment utilisés), **le message invite le destinataire à composer un numéro surtaxé commençant par 0892 ou 0899 afin de récupérer son colis**.

Dans la plupart des cas, la victime qui appelle tombera sur un répondeur qui lui demandera de patienter ou de rappeler.

Parfois, elle sera invitée à récupérer un code qu'elle devra envoyer par mail à une fausse adresse figurant dans le message.

Une fois récupéré par l'escroc, ce code sera utilisé pour accéder à des contenus en ligne (jeux, loteries, etc.).

Bien entendu, aucun colis n'arrivera. En revanche, le coût des communications, lui, apparaîtra bien sur la facture de téléphone de la personne qui a appelé.

**À raison de 0,80 € la minute ou 3 € l'appel, les montants peuvent vite grimper.**

Méfiance donc si vous recevez un e-mail vous indiquant qu'un colis vous attend. Il s'agit très certainement d'une arnaque.

Vous pouvez la signaler à l'Association Française du Multimédia Mobile (AFMM) à l'adresse suivante : deontologie@afmm.fr, accompagnée du message incriminé.

Si vous avez le moindre doute, appelez le transporteur en cherchant son numéro dans l'annuaire ou bien consultez son site Internet.

Dans le cas où vous avez déjà appelé le numéro surtaxé, tout n'est pas perdu.

**Conseils :**

Rendez-vous sur le site Internet Infosva.org et entrez le numéro en 08 que vous avez composé.

Vous verrez apparaître le nom de l'éditeur ou d'un prestataire technique. C'est à lui qu'il faut adresser sa demande de remboursement.

Même si aucune loi ne les y oblige, ils acceptent, dans la plupart des cas, de rendre de bonne foi, les sommes versées .


*Abonnez-vous et recevez tous les mois notre magazine Santé*

# INTERNET

Principales fraudes : escroqueries africaines, fuites d'information et victimes d'usurpation d'identité, emails malveillants et Phishing, surfacturation et « micro-paiements » en ligne.

## Escroqueries Africaines ou à la Nigériane

Un malfaiteur piège un internaute souvent sous Skype, Facebook ou autres outils de rencontre et lui demande une aide financière sous un prétexte très élaboré.

Escroquerie classique : une demande financière pour aider un ami de la victime en difficultés à l'étranger par exemple.

Il existe d'autres pièges beaucoup plus élaborés, le scénario de l'escroquerie est le même au départ mais le cyber-malfaiteur envoie souvent un chèque X volé à d'autres personnes d'un montant supérieur à la somme demandée précédemment et demande le remboursement de la différence par Western union, Money Gram ou rechargement PCS Mastercard.

La banque prend souvent une dizaine de jours pour informer la victime de la non validité dudit chèque X. La victime a donc perdu son argent.

## QUE FAIRE ?

**1 – Téléphoner à son ami** « soi-disant à l'étranger » et selon le cas intervenir ou non !

**2 – Ne rien envoyer à une personne non parfaitement identifiable** et surtout ne pas accepter un chèque ou un virement bancaire d'une personne inconnue pour ce type de transaction !

**3 - Demander à sa banque de faire une vérification immédiate du chèque.**

Dans le cas d'un virement bancaire, demander à la banque la provenance des fonds avant tout retrait d'espèces.

Si malgré tous vous souhaitez aider cet ami, faites une reconnaissance de dette ! Les victimes sont nombreuses et souvent manipulées. Allez voir sur le site : http://www.avenfrance.org/

## Fuites d'information et Victimes d'usurpation d'identité sur Internet.

L'usurpation d'identité consiste dans un premier temps :

- à récupérer par divers moyens (visite de poubelle, demande frauduleuse par Internet sous divers faux prétextes : montant d'impôts trop perçus, erreur de facturation sur électricité ou gaz, piratage des comptes de messagerie électronique ou Facebook), toutes informations concernant une personne,
- puis à utiliser, sans votre accord, des informations (nom, prénom, adresse, e-mail, photographie personnelle, numéro de compte, etc.) permettant de souscrire sous votre identité un crédit, un abonnement, ou nuire à votre réputation.

Les photos ou vidéos que vous avez transmises ou qui circulent sur le Net, peuvent être utilisées par un individu peu scrupuleux.

Pour vérifier la présence de photos, vous pouvez utiliser un moteur de recherche inversée d'images (http://tineye.com/, http://www.cydral.fr/ ).

Ce moteur de recherche spécialisé se chargera d'identifier tous les sites qui réutilisent publiquement votre image. Vous pouvez conserver une trace de cette manipulation.

**Sur Internet, on distingue deux types d'usurpation d'identité.**
**Nuire à la réputation de la victime** dont il a volé les données personnelles en rédigeant des commentaires sous l'identité de sa victime ou en créant de faux profils (Twitter, Facebook, blog web, ou autres).

**Utiliser des informations personnelles** de particuliers comme support pour effectuer des opérations sous l'identité de la victime.

## Conseils :

### QUE FAIRE AVANT usurpation ?

- **Soyez vigilant lorsque vous jetez des documents personnels à la poubelle,** ou saisissez des données sur Internet ou lorsque vous recevez des courriels vous demandant de fournir ou de mettre à jour des données vous concernant.
- **Ne répondez pas aux courriels** qui vous paraissent suspects et détruisez les immédiatement.
- **Ne cliquez jamais sur les liens contenus dans les messages** dont vous n'êtes pas certain de la provenance.

**Précautions à prendre avec vos identifiants de comptes en ligne :**

- choisissez des mots de passe mélangeant chiffres, lettres, caractères spéciaux, pas de 123456 ou date de naissance ou numéro de département !
- n'utilisez pas le même mot de passe pour plusieurs applications,
- ne transmettez, ni partagez vos mots de passe avec personne,
- sur un ordinateur accessible à d'autres personnes, n'enregistrez jamais les mots de passe dans votre navigateur, effacez ses cookies et son historique de navigation régulièrement,
- enfin, **vérifiez vos relevés bancaires régulièrement** pour repérer tout prélèvement anormal.

### QUE FAIRE APRES usurpation ?

- vérifiez avant toute intervention que le compte n'appartient pas à un homonyme,
- si l'usurpation vous semble avérée, vous pourrez constituer un dossier comprenant les éléments permettant de déterminer qu'il s'agit bien de vos propres informations et non celles d'un homonyme,
- conservez les adresses URL des pages/profils concernés,
- faites des captures d'écran du faux profil et de ses publications ou d'autres justificatifs qui vous semblent pertinents.

- Venez nous voir à l'UFC, ou demandez, en tant que victime, au responsable (webmaster) du site incriminé, d'interrompre la diffusion des informations personnelles en ligne et/ou d'exiger la suppression de ces informations.

## Emails malveillants et Hameçonnage ou Phishing

**Exemple :** Dernier en date signalé par MSA Bourgogne
Vous recevez un e-mail avec le logo de l'Assurance maladie, sur votre messagerie personnelle et/ou professionnelle faisant la promotion de la *« nouvelle carte Vitale V4 » proposée par Ameli.*

Ce document invite les assurés à demander leur pseudo nouvelle carte qui *« garantit le remboursement de vos soins sous 24 h »* et assure que la démarche est « très simple » et ne prendra *« qu'une minute »*.

Pour cela, ils doivent fournir, sur une boîte email **pirate** (exemple d'adresse mail : vitale@amelidirection.com, documents@assurance-maladie.be), la photocopie de 2 pièces d'identité, un justificatif de domicile et un relevé d'identité bancaire.

**CONSEIL :**
Pour les campagnes d'hameçonnage ciblées : **Ne répondez JAMAIS à ces e-mails**.

## Les 5 règles d'or anti-hameçonnage

**Afin d'éviter d'être victime d'une opération d'hameçonnage ou de phishing, voilà cinq règles d'or :**

- vérifiez régulièrement les opérations effectuées sur votre compte bancaire. Si vous détectez une anomalie, signalez-la immédiatement à votre banque et contestez le débit,
- si vous recevez un message d'un tiers professionnel (banque, impôt, EDF, fournisseur Internet ou mobile…), qui vous réclame un
- « reliquat de paiement de facture », vous prévient d'un « bon de remboursement » ou vous demande de confirmer vos codes et identifiants « suite à une tentative de piratage », **ne cliquez jamais sur le lien fourni dans le mail**,
- ne réagissez jamais dans l'urgence, même si le mail est alarmiste. Prenez toujours le temps de vérifier,
- ne rentrez jamais vos coordonnées bancaires au complet sur un site, ni votre mot de passe qui donne accès aux services en ligne, ni votre code secret de carte bancaire, personne n'a le droit de vous le demander,
- en cas de doute ou si vous pensez avoir été victime d'hameçonnage, prévenez immédiatement votre conseiller bancaire pour qu'il bloque en amont toutes les opérations suspectes sur votre compte.

## Abonnement Internet caché

Les surfacturations avec le « micro-paiements » en ligne.

Un exemple classique : vous laissez votre smartphone à vos petits enfants.

Ils jouent à des jeux éducatifs en ligne mais n'ont pas conscience que certains jeux sont payants et vous vous retrouvez à payer des prestations de plusieurs dizaines d'euros qui seront débités en même temps que votre abonnement mensuel.

**« Micro-paiements » : quels systèmes !**

Il s'agit de systèmes de paiement qui permettent de réaliser des achats de petits montants en ligne sans carte bancaire, le montant étant ensuite reporté sur la facture du fournisseur d'accès à Internet.

Votre facture de téléphonie est plus élevée que d'ordinaire ? Celle de votre fournisseur d'accès à Internet affiche de surprenants dépassements ? Peut-être avez-vous utilisé sans le savoir des services payants.

Nombre d'éditeurs recourent à des systèmes de « micro-paiement » pour vendre leurs contenus.

Des jeux aux sonneries pour portables en passant par des informations sportives ou des services d'assistance, tout se monnaye par ce biais, à l'unité ou par l'intermédiaire d'un abonnement.

Le montant de l'achat est automatiquement reporté sur la facture de son opérateur de téléphonie mobile ou de son fournisseur d'accès à Internet.

### Les 4 principaux systèmes de « micro-paiement »

**INTERNET +**

L'utilisateur est dirigé automatiquement vers une page de paiement gérée par son opérateur. Il n'a plus qu'à confirmer l'achat.

Internet+ autorise des achats jusqu'à 30 €, à l'unité ou sur abonnement. Il est accessible aux clients Orange, SFR, Bouygues, Free et Alice.

**SMS +**

Idéal pour acheter des jeux, télécharger des titres de musique ou recevoir les résultats sportifs, pour faire participer les téléspectateurs à des jeux ou les faire voter.

**CONTACT +**

Ce système est destiné à facturer des services à la durée sur Internet : assistance en ligne, accès à certaines informations, jeux, tests de QI, etc.

Contact+, lui, permet une facturation en fonction du temps passé sur des pages Internet ou auprès de services (assistance, etc.). Il est réservé aux clients d'Orange.

**LES NUMÉROS SURTAXÉS**

Dans ce cas, le paiement se fait en composant un numéro surtaxé depuis son téléphone. Les numéros surtaxés les plus chers commencent par 0892 ou 0899.

**Le problème, c'est que ces services sont souvent activés par défaut** et ne nécessitent parfois aucune authentification.

Il est donc possible qu'un membre de votre famille ait procédé à ces achats, sans avoir forcément conscience de leur caractère payant.

Si vous estimez avoir été lésé, retournez-vous vers l'éditeur du service. Votre opérateur peut vous donner ses coordonnées.

Dans tous les cas, prenez garde à ne pas faciliter l'accès à ces modes de paiement à un tiers (évitez par exemple d'enregistrer le mot de passe de votre compte client).
Attention certaines options dont « Google Play - Paiement sur facture » peuvent être activé par défaut.

## Conseils : Que faire en cas de surfacturation ?

**Contacter son opérateur** pour obtenir le nom de l'éditeur du service et, le cas échéant, résilier l'abonnement. Pour plus d'informations pour Internet + et SMS +, consulter le site infoconso-multimedia.fr ou pour les paiements des numéros surtaxés, le site infosva.org.

**Appeler l'éditeur du service** pour obtenir le remboursement des sommes prélevées (il n'est pas forcément tenu de le faire, mais la plupart acceptent lorsque la victime est de bonne foi).

**Bloquer l'utilisation des services** de paiement Internet et/ou mobile sans carte bancaire.

### Vous souhaitez bloquer l'utilisation des services de paiement (Internet+ box, Internet+ mobile, Contact+ et SMS+ et autres)

**Conseil :** Rendez-vous dans votre espace client, puis désactiver les options de paiement par mobile ou par Internet.

Le principe reste le même quelque soit le fournisseur mobile et/ou Internet.

Pour plus de détails voir sur http://infoconso-multimedia.fr qui vous accompagne pas à pas dans votre démarche.

## Conseils de sécurité sur Internet

Maintenez votre ordinateur à jour :

- applications fixes ou mobiles frauduleuses. Utiliser essentiellement un antivirus mis à jour régulièrement,
- utilisez un réseau sécurisé (se méfier des connexions WIFI publiques),
- préférez les achats sur des sites reconnus, et vérifiez l'identité des sites marchands et bancaires (le HTTPS obligatoire sinon ne pas acheter),
- n'utilisez pas de mot de passe simple, ni partout le même,
- ne tombez pas dans le piège des offres frauduleuses, restez vigilant sur des sites comme Ebay, Facebook, Leboncoin ou les sites étrangers.

Votre navigateur web (Chrome, Firefox, Opera, Microsoft Edge, Safari...) intègre un filtre anti hameçonnage, généralement assez pertinent, mais là encore deux précautions de sécurité valent mieux qu'une, et un bon antivirus viendra renforcer vos défenses.

Utilisez les outils de protection de votre banque, et payez en toute sécurité par l'intermédiaire de numéro de carte bancaire virtuel, ou une confirmation de paiement via votre téléphone.

Des systèmes de paiement intégrés aux smartphones, de type Apple Pay, Android Pay (bientôt en France) ou PayPal peuvent être une alternative sécurisée.

Consultez la politique de confidentialité des sites marchands. Ces informations se trouvent souvent en bas de page, dans la section Informations légales.

Vérifiez les retraits sur vos comptes bancaires régulièrement afin de détecter d'éventuelles transactions frauduleuses.




## CARTE BANCAIRE

### Carte bancaire : Des règles de prudence pour éviter l'arnaque.

Plus de 400M€ ont été débités frauduleusement plus par vols des données bancaires que par vols de la carte.

**Comme son nom l'indique le code est confidentiel**

Ne l'écrivez nulle part, ne le communiquez à personne (banque, police, administration) notamment par téléphone ou par courriel où les sollicitations d'escrocs sont fréquentes.

**Attention aux faux claviers et aux cameras cachées**

Ils sont souvent installés sur des distributeurs ou des bornes de pompe à essence.

**Conseil :** Ne pas hésiter à saisir son code en cachant le clavier et mettre la carte en opposition si elle est avalée.

**Cacher le cryptogramme : les 3 chiffres du verso**

Lors d'un paiement, il nous est demandé de les communiquer. Entre temps rien n'empêche d'y mettre un cache autocollant et de conserver toujours un œil sur sa carte si un commerçant a besoin de la prendre.

**Conseil :** il existe de nouvelles cartes avec un cryptogramme dynamique (mini écran intégré à la carte).

Il peut donc changer plusieurs fois par jour.

**Surveiller l'existence d'un S et d'un cadenas dans l'adresse du site.**
On est sûr que le site est sécurisé si l'adresse « https » indique un S (comme sécurité) à la fin avec le symbole d'un cadenas à côté.

Pour les sites basés à l'étranger, attention leurs règles de gestion des données peuvent être différentes des nôtres.

«Mieux vaut privilégier les sites français souvent plus protégés », assure Olivia de Suza juriste à UFC-Que Choisir.

**Paiement avec 3D Secure**
Après l'étape où vous avez été reconnu en saisissant le numéro, la date de validité, le cryptogramme, et le code 3D Secure à usage unique est envoyé par votre banque (si elle est adhérente au système) par SMS.

Vous devez le saisir pour authentifier et sécuriser votre paiement en ligne.

**Conseil :** attention aux mails frauduleux portant la mention « Verified by visa ».

**Vérifier ses relevés de banques**
Regarder régulièrement vos relevés bancaires et signaler immédiatement une anomalie.

**Penser à l'Antivirus**
De plus en plus de ventes se font avec un portable. Équipez-le d'un antivirus en sachant que ceux, même gratuits, sont assez performants.

**Si fraude avérée : remboursement sans pénalité**
Toujours en poche, votre carte a été utilisée frauduleusement pour des achats à distance.

L'article L133-24 du Code monétaire et financier dispose que la banque doit créditer les sommes litigieuses dès réception de la notification (lettre recommandée avec AR) qui doit intervenir dans les 13 mois (70 jours et parfois 120 au plus pour les paiements hors Union Européenne).

**Disparition de la carte**

Il faut en informer le plus rapidement sa banque et selon l'article L133-20 du Code monétaire et financier, elle doit rembourser l'intégralité des frais liés à l'opposition.

En pratique, les banques mettent entre deux et trois semaines pour le faire, sinon il faut les mettre en demeure devant la juridiction compétente.

*« En général, si la fraude dépasse 4000€, il vaut mieux prendre un avocat »,* explique Olivia De Suza juriste à UFC-Que Choisir.

## Éviter les fraudes à la carte bancaire : Les conseils de la police

Comparé au nombre d'achats ou débits effectués en France, 560 milliards d'euros environ, le taux de **fraudes à la carte bancaire** paraît très faible : 0,080 % en 2012 (contre 0,077 %, l'année précédente), chiffres de l'Observatoire de la sécurité des cartes de paiement.

Mais, en valeur, cela représente tout de même 450 millions d'euros, soit une hausse de 9 %, alors que, dans le même temps, le montant des transactions n'a crû que de 5 %.

Il y a trois ans, policiers et gendarmes ont reçu pour instruction de ne plus prendre les plaintes liées à de tels faits. Tout juste les porteurs légitimes peuvent-ils déposer une main courante et se voir remettre un document leur expliquant la marche à suivre à l'égard de leur banque.

Problème, il arrive que certaines d'entre elles exigent encore un dépôt de plainte préalable avant de régulariser la situation.

Le Ministère de la Justice entend clarifier les choses. Pour l'heure, la police indique n'intervenir que sur sollicitation des banques ou des commerçants. Elle tente de remonter filières et réseaux (qui mènent souvent à l'étranger) ou d'appréhender des escrocs « plus artisanaux ». Mais il est difficile de connaître le taux d'élucidation, probablement assez faible par rapport au nombre d'arnaques.

**Face à la menace, la police distille quelques conseils de bon sens aux consommateurs.**

Quelques gestes simples peuvent prémunir le porteur légitime d'une utilisation frauduleuse de sa carte bancaire.

**Chez les commerçants**

Magasins d'habillement, restaurants, stations-service… les détournements de cartes dans les commerces restent la principale source de fraudes.

Si le numéro inscrit au recto (les 16 chiffres, ndlr) est amputé sur le reçu remis au client, en revanche, il est intégralement imprimé sur celui conservé par le commerçant où figure aussi la date d'expiration.

Lors du paiement, un salarié malveillant peut rapidement retourner la carte et mémoriser le cryptogramme à trois chiffres inscrit au verso.

Il aura alors en sa possession les coordonnées complètes, ce qui permettra ensuite la réalisation d'achats à distance sur le compte du porteur légitime.

Ayant toujours sa carte, ce dernier n'a aucune raison de se méfier. Et ce n'est que lors de la vérification de ses comptes qu'il constatera la fraude.

Souvent, ces salariés indélicats détournent les coordonnées des cartes bancaires au profit de réseaux structurés.

Les produits ensuite commandés grâce à cette fraude sont acheminés à une adresse fictive, avec parfois la complicité du livreur, qui ferme les yeux en échange d'un billet.

**Conseil :** Ne quittez jamais votre carte des yeux lors d'un paiement chez un commerçant.

N'acceptez pas que l'employé parte avec.
Cas typique : au restaurant, le serveur vous prend la carte puis revient, pour que vous validiez la transaction, avec le Terminal de Paiement Électronique (TPE) dans lequel il l'aura entretemps introduite. Il aura eu tout loisir pour mémoriser les trois chiffres du pictogramme.

Méfiance aussi lorsque l'employé frotte votre carte sur la manche au prétexte que le terminal ne peut pas la lire.

Cela peut être une technique afin de vite jeter un œil au dos.

Face à ce risque, une mesure radicale existe : apprendre par cœur ou inscrire (loin de la carte, bien sûr) les trois chiffres du cryptogramme que l'on occulte ensuite par un petit autocollant. (Attention à ne pas bloquer la carte bancaire dans le DAB avec l'autocollant mis sur la carte).

**La Brigade des Fraudes aux Moyens de Paiement (BFMP) a édité un autocollant pour masquer les trois chiffres du cryptogramme.**
La BFMP a créé une gommette avec le blason de la préfecture de police. Elle est distribuée gracieusement lors d'actions de prévention. Les banques rappellent, quant à elles, que la carte reste leur propriété et qu'elle ne doit pas être altérée.

**Au distributeur de billets**
Les escrocs ont de l'imagination et sont très à l'aise avec la technologie : fausses façades ou faux claviers, mécanismes de retenue des billets, mini caméras quasiment indétectables… un concentré d'ingéniosité et de haute technologie pour piéger les distributeurs automatiques de billets (DAB).

L'objectif, capter les données de la carte (informations contenues sur la piste magnétique et code confidentiel) à l'insu de l'usager venu retirer de l'argent.

À partir de là, des réseaux encodent des cartes vierges, qu'ils utilisent ensuite pour retirer de l'argent aux distributeurs (généralement 200 à 300 €) ou dans l'un des très nombreux pays où la puce de nos cartes bancaires n'est pas active (par exemple, aux États-Unis).

Ce sont les distributeurs des quartiers huppés et/ou très fréquentés qui sont a priori les plus piégés.

Il y a davantage de chances pour que l'usager du DAB soit en possession d'une carte haut de gamme avec des plafonds de retrait plus élevés.

Pour "rentabiliser" l'investissement avant que le pot aux roses ne soit découvert, il faut qu'il y ait de nombreux passages.

**Conseil :** Pour compliquer la tâche des « piégeurs » de cartes, n'hésitez pas à cacher avec une main le clavier quand vous tapez votre code confidentiel.

Une précaution qui vaut pour les DAB mais également pour les automates de paiement (billets SNCF ou de transports urbains, pompes à essence, etc.), de plus en plus ciblés.

**Sur Internet**
Une bonne nouvelle… relative. Le taux de fraudes concernant les paiements sur Internet serait en baisse. Mais, en valeur, la fraude continue de progresser, en même temps que le commerce en ligne monte en puissance. Le paiement s'y fait presque exclusivement par carte bancaire, dont les données peuvent être récupérées par des pirates férus d'informatique ou des employés complices.

**Pour l'usager, difficile de se protéger.**
Une délinquance qui est l'apanage de réseaux très structurés (une spécialité des pays de l'Est mais plus seulement) ou d'escrocs à la petite semaine.

Sans compter que ce sont parfois la totalité des données bancaires conservées par des sociétés d'e-commerce qui peuvent avoir été aspirées par des pirates (hackers).

**Conseil :** Privilégiez les sites équipés de dispositifs de sécurité qui permettent de garantir une meilleure authentification du porteur de la carte (systèmes dits 3D Secure). Avant paiement définitif, celui-ci doit en effet fournir une information supplémentaire qu'il est le seul à détenir. Exemple, un code envoyé par SMS sur son mobile par sa banque.

### Se faire rembourser en cas de fraude à la carte bancaire

Dès que le porteur légitime d'une carte bancaire se rend compte d'une opération irrégulière, il doit faire opposition pour ne plus être tenu par les paiements qui surviendraient par la suite. La banque doit, de son côté, régulariser la situation pour tous les débits effectués avant l'opposition.

**Si la carte a été utilisée frauduleusement ou a été contrefaite sans emploi du code confidentiel** (achat sur Internet, par exemple), la banque rembourse intégralement le porteur légitime des sommes débitées, sans que celui-ci ait à payer de franchise.

Le client a, en principe, 13 mois pour déposer une réclamation à compter de la réalisation de l'opération contestée. La banque doit recréditer le compte dans le mois qui suit cette réclamation.

**Si la carte a été perdue ou volée et qu'il y a eu frappe du code confidentiel**, le titulaire est remboursé des sommes débitées, déduction faite d'une franchise de 150 € pour les retraits ou débits effectués avant opposition. La banque peut cependant refuser ce remboursement si elle prouve une faute ou une négligence du porteur légitime.

### Phishing : La preuve de la négligence doit être apportée par la banque

Dans un arrêt récent, la Cour de cassation précise qu'un établissement bancaire ne peut pas affirmer qu'une victime de phishing (hameçonnage) a fait preuve de négligence sans le prouver. Faute d'éléments concrets, elle est tenue de rembourser la victime.

En août 2013, Franck, un habitant du département du Nord, découvre sur son compte trois débits pour un montant total de 838 €.
Lorsqu'il se tourne vers sa banque, pour en demander le remboursement, celle-ci refuse au motif que Franck aurait transmis ses données bancaires à un inconnu suite à la réception d'un e-mail qu'il pensait provenir de sa banque.

**C'est ce qu'on appelle le phishing (hameçonnage).**
Mais dans un arrêt du 18 janvier 2017, la Cour de cassation ne l'a pas entendu de cette oreille.

Certes, le Code monétaire et financier dispose que la banque n'a pas à rembourser des prélèvements dès lors que le client a fait preuve de *« négligence »*.

Or, dans ce cas précis, rien ne prouve que Franck a été négligent. *« La banque se borne à évoquer l'hypothèse du phishing [...] mais n'en apporte aucunement la démonstration »*, précisent les magistrats.

Les doutes sont d'autant plus permis qu'au moment des faits, Franck était en vacances dans le Var alors que les opérations contestées se sont produites en région parisienne.

Autre fait troublant : l'adresse mail de Franck a été remplacée par une autre adresse, inconnue. De toute évidence, l'escroc s'est servi de cette adresse mail pour recevoir de la banque les codes de confirmation nécessaires pour procéder aux prélèvements.

En envoyant ces codes à une personne qui n'était pas le titulaire du compte, les magistrats estiment que la banque a aussi commis une *« faute contractuelle »*.

Cet arrêt est intéressant dans la mesure où, pour la première fois, il précise qu'un établissement bancaire ne peut se contenter d'affirmer que les victimes de Phishing ont été négligentes. Encore doit-il le prouver. Et le fait d'affirmer qu'il ne peut en être autrement compte tenu des systèmes de sécurité mis en place ne suffit pas à le démontrer.

Grâce à cet arrêt, de nombreuses victimes de Phishing devraient à l'avenir pouvoir obtenir plus facilement un remboursement de la part de leur banque.

**Pour autant, le meilleur moyen, c'est encore la prévention.** Jamais une banque ni aucun autre professionnel ou administration (Orange, EDF, Fisc, CAF ou autre) n'enverrait un mail pour demander des coordonnées bancaires.

Alors, à chaque fois que vous recevez un e-mail de ce genre, demandez-vous d'où il vient et, en cas de doute, contactez directement le soi-disant expéditeur avant de transmettre des informations personnelles.

## Sécurité des banques : Bilan du paysage bancaire en ligne

Internet s'est immiscé dans notre environnement, jusqu'à devenir quasi incontournable. Pionniers en la matière, les établissements bancaires ont rapidement développé et proposé des services en ligne à leurs clients.

Au départ simple prolongement du Minitel, leurs sites permettaient de consulter le solde de son compte courant et d'investir en Bourse.

Mais, petit à petit, les établissements financiers ont étoffé leurs palettes de services et désormais, les clients peuvent réaliser en quelques clics toutes leurs opérations courantes de base : virements automatiques, transfert d'argent, impression de RIB/Iban (coordonnées bancaires), commande de chéquiers, changement de carte bancaire…

Et les grands réseaux bancaires ne sont pas les seuls à développer leur offre sur Internet. Les banques en ligne, établissements à distance sans aucune agence « en dur », séduisent de plus en plus.

D'après une étude Audirep, en octobre 2014, environ 7 % de la population détenaient un compte dans l'un de ces établissements. Un nouveau compte sur trois serait aujourd'hui souscrit dans une banque en ligne. La plupart d'entre elles sont des filiales de banques traditionnelles.

## Revers de la médaille

Mais cet engouement a ouvert un large champ des possibles aux personnes malveillantes. Désormais, plutôt que de dérober chéquiers ou cartes bancaires, les « pirates » s'en prennent directement aux données des clients sur le Web.

Selon l'enquête 2014 de l'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP), 840000 Français auraient subi une cyber-attaque en 2013 et ils étaient quasiment 900000 un an plus tard.

**« En 2014, la fraude à la carte bancaire a représenté, en valeur, 500 millions d'euros ».** Toujours selon l'ONDRP, le nombre de ménages victimes de débits bancaires frauduleux croît de façon régulière depuis 2010.

## Encore trop de failles

Les données bancaires des clients sont souvent frauduleusement récupérées dans les serveurs de sites de e-commerçants.

Mais comme la sécurité informatique des professionnels se renforce, les pirates se tournent vers des cibles potentiellement moins protégées : les particuliers.

Et, depuis quelques années, les techniques d'hameçonnage ou la propagation des virus espions de type « cheval de Troie » sont les pratiques privilégiées des réseaux de malfaiteurs.

L'engouement du grand public pour le téléphone mobile et le développement d'applications bancaires dédiées, dans chaque réseau bancaire, risque de permettre l'augmentation de ce type de fraudes.

Car, même si globalement les applications présentent moins de failles que les sites Internet des banques, leur utilisation par les clients est parfois peu prudente (accès depuis une connexion Wi-Fi non sécurisée, par exemple), inutile pour autant de bouder leurs services connectés.

## Les principaux modes de piratage

- **Le keylogger :** ce programme pirate enregistre toutes les saisies que vous effectuez au clavier et/ou à l'aide de la souris de votre ordinateur. Le pirate qui l'a installé peut donc récupérer toutes vos données sensibles.

- **Le malware** : il s'agit des programmes pirates parmi les plus sophistiqués, qui s'installent sur votre ordinateur à votre insu. Ils se lancent lorsque vous consultez une page Internet officielle et vous demandent, par exemple, des informations confidentielles à remplir sur un formulaire vierge qui apparaît sur l'écran.

Le plus connu d'entre eux s'appelle Zeus et vise surtout les clients des banques.

• **Le Phishing ou hameçonnage** : cette technique consiste, pour un voleur, à vous attirer vers un faux site Internet qui imite l'apparence du vrai pour récupérer vos coordonnées bancaires.

En général, vous recevez comme appât un e-mail vous demandant de vous connecter d'urgence au site de votre banque, des impôts, de votre fournisseur de téléphone…

Vous êtes informé qu'il faut remettre vos données personnelles à jour ou entrer vos coordonnées bancaires pour recevoir un virement. Si vous vous exécutez, l'escroc a alors accès à votre compte bancaire et peut le vider en quelques clics.

• **Le pharming :** cette fois ce n'est pas le site, mais l'adresse qui est falsifiée. Ainsi, vous pensez vous retrouver sur la page de paiement du site d'un commerçant en ligne ou sur celui de votre banque, mais en réalité, vous êtes transféré sur celui d'un pirate.

Pour éviter ce type de désagrément, assurez-vous, pour chaque transaction, que le site est sécurisé : l'adresse qui apparaît dans votre barre de navigateur doit démarrer par « https » (HyperText Transfer Protocol Security – protocole de transfert hypertexte sécurisé) et être accompagné d'un dessin de cadenas.

Dans le cas contraire, vous risquez de transmettre vos coordonnées bancaires à une personne mal intentionnée, avec les mêmes risques que pour le phishing.

•**Le spyware :** contrairement au virus, dont le but est de se propager, le spyware est un logiciel malveillant qui s'installe sur votre ordinateur à votre insu. Selon son type, il peut capturer les frappes de votre clavier et donc connaître vos mots de passe, copier ce qu'il y a sur votre écran d'ordinateur.

• **Le virus :** il se loge dans votre ordinateur à votre insu et se propage dans le but de saturer les fonctionnalités de votre ordinateur, voire de le rendre hors d'usage.

Certains virus contiennent des programmes qui désactivent les pare-feu et antivirus pour diminuer le niveau de protection de votre ordinateur.

Parmi les plus dangereux, ceux qui contiennent un « cheval de Troie », qui permet au pirate de prendre la main, à distance, sur votre ordinateur.


*Abonnez-vous et recevez tous les mois notre magazine*

## Sécurité des banques : Une protection sûre à 100 % n'existe pas

Selon l'Observatoire national de la délinquance et des réponses pénales (Ondrp), la part des ménages victimes d'escroqueries bancaires est en nette progression.

Les enquêtes réalisées entre 2011 et 2014 révèlent que 35 % d'entre eux ont subi un préjudice d'un montant inférieur ou égal à 100 €, de 23 % à 25 % entre 101 et 1000 € et 17 % supérieur à 1000 €.

La sécurité des comptes bancaires accessibles en ligne est encore loin d'être optimale. **Une protection à 100% n'existe pas.**

La preuve : sur tous les sites bancaires, il est possible de récupérer le mot de passe du compte via un logiciel pirate de type « keylogger », qui installe un virus sur l'ordinateur sans que ce dernier ne s'en aperçoive. Certaines opérations ne sont pas toujours sécurisées.

### Mot de passe, un choix clé

Lors de l'ouverture d'un compte, les banques ont toutes de bons réflexes : elles n'envoient jamais l'identifiant (code à plusieurs chiffres) et le mot de passe sur un même document, par SMS ou par courrier postal.

Si certaines banques vous communiquent vos identifiants en agence – ce qui est plus sûr –, d'autres les envoient par e-mail (banques en ligne) ou par courrier postal. Pour certaines banques, ce code est temporaire et il faut le modifier lors de la première connexion.

Néanmoins, quelque soit l'établissement bancaire, changer de mot de passe en ligne est toujours possible à n'importe quel moment.

Concernant la difficulté de cryptage, des progrès restent aussi à faire, car peu de sites exigent un mot de passe élaboré.

Enfin, pour les clients néophytes, le niveau d'information concernant les mots de passe est peu satisfaisant.

Certaines banques se contentent de préciser qu'il faut éviter les dates de naissance ou les suites de chiffres.

D'autres suggèrent de modifier régulièrement le mot de passe.

### Clavier physique ou virtuel

Une fois le compte ouvert et le mot de passe choisi, tous les sites bancaires proposent un protocole sécurisé sur la page de connexion (« https » et cadenas présent sur la barre).

Certains proposent, en option, une sécurité renforcée lors de la connexion ou à l'aide d'une carte de sécurité.

Pour vous connecter à votre espace bancaire sur Internet, vous devez tout d'abord entrer votre identifiant et votre mot de passe.

Ce dernier doit être saisi directement sur votre clavier d'ordinateur, ou à l'aide de votre souris sur un clavier virtuel qui modifie automatiquement et de façon aléatoire l'emplacement des chiffres à chaque connexion.

Ce système, plus sécurisé, permet de tromper certains logiciels de type « keylogger » qui enregistrent et transmettent à des pirates les frappes au clavier et les boutons sur lesquels l'utilisateur a cliqué.

### La mémoire du navigateur.

Plus grave, selon nos tests, la connexion aux comptes est mal protégée pour certaines banques. Le navigateur Internet (Chrome) a pu enregistrer les identifiants de connexion.

Pire, pour trois autres banques, le navigateur Internet a aussi mémorisé les mots de passe ! Ce qui est potentiellement très dangereux si votre ordinateur est dérobé ou utilisé à votre insu.
**D'une manière générale, il ne faut jamais permettre au navigateur Internet de mémoriser ses identifiants ou mots de passe lors d'une connexion,** que ce soit sur un ordinateur privé ou pire, sur un ordinateur public en libre accès.

### Déconnexion automatique

Une sécurité absolue reste illusoire. Sur tous les sites bancaires testés, il est possible de capturer le mot de passe via un logiciel pirate de type « keylogger », qui installe un virus sur votre ordinateur et récupère les données à votre insu.

**Quelle réaction du site de la banque face à plusieurs tentatives de connexion avec un code erroné ?**
Elles ont entraîné le blocage de tous les sites, de façon temporaire, jusqu'à un blocage complet nécessitant une restauration du code en agence où le blocage s'est activé au bout d'une dizaine de tentatives, ce qui est peu rassurant.

Enfin, en cas de session non utilisée, la durée de déconnection automatique du site est plus ou moins variable selon les banques : supérieure à quinze minutes, ce qui laisse le temps à un autre utilisateur de se connecter sans difficulté derrière votre dos, ou pour d'autres établissements, ce délai s'élève entre cinq et quinze minutes, laps de temps plus raisonnable et qui permet de réaliser certaines opérations sur l'ordinateur sans avoir à se reconnecter de façon trop répétée.

### Choisir un mot de passe sécurisé

La plupart des banques recommandent de modifier régulièrement votre mot de passe. Mais, dans la pratique, mieux vaut opter pour un code sécurisé, que vous n'aurez pas à écrire quelque part (bureau, ordinateur, mobile...) pour vous en rappeler.

En effet, en changeant trop souvent de code, vous risquez de choisir un mot de passe trop simple à retenir ou de l'écrire dans vos notes, ce qui est finalement plus risqué.

**Pour choisir un mot de passe sécurisé, il faut privilégier au moins douze caractères composés de majuscules, de minuscules, de chiffres et de caractères spéciaux.**

Il existe des astuces permettant de vous en souvenir plus facilement comme la méthode des premières lettres (« Un tiens vaut mieux que deux tu l'auras » donne, par exemple, « 1tvmQ2tl'A ») ou encore la méthode phonétique.

Bannissez une bonne fois pour toutes les mots trop simples (« password » et « football » sont les plus utilisés), les informations personnelles (les prénoms de vos enfants, votre date de naissance...) ou encore les suites de chiffres (123456...).

## Sécurité des banques : Comment sécuriser vos moyens de paiement ?

En France, d'après la dernière étude de la Banque de France datant de 2013, 48 % des paiements étaient effectués par carte bancaire, 19 % par prélèvements, 17 % par virement, 14 % par chèque et 2 % par d'autres moyens (*Titre interbancaire de paiement : Tip*…).

Cela fait des Français les champions européens des utilisateurs de carte bancaire (les paiements par ce biais représentent en moyenne 37 % dans la zone euro) et les leaders de l'utilisation de chèques (employés pour seulement 4 % des transactions en zone euro). Dommage, car la carte bancaire et le chèque restent les cibles privilégiées des escrocs.

« *Pour sécuriser au maximum ses transactions, mieux vaut régler par virement, télépaiement ou Tip, ce sont les moyens de paiement qui offrent le moins de possibilités de falsification* », confie un avocat spécialisé dans la défense des épargnants.

### La sécurisation des chèques

En France, plus de neuf particuliers sur dix disposent encore d'un carnet de chèques : ils en émettent en moyenne 4,9 par mois et en reçoivent un par mois.

Dès lors, les risques de perte ou de vol de chèques envoyés par La Poste sont importants.

Premier bon réflexe pour sécuriser au maximum ce moyen de paiement : « *il faut conserver son chéquier dans un endroit sûr et ne pas laisser sa signature à l'intérieur ou dans des documents à proximité* ».

Sinon, en cas de vol, l'escroc pourra très facilement rédiger des chèques en sa faveur et les encaisser avant votre dépôt de plainte.

Lorsque vous rédigez un chèque, notez toujours sur le talon le montant et l'ordre de celui-ci. Ce qui vous permettra de vérifier, en pointant vos relevés bancaires, qu'il n'y a pas de problème lors de l'encaissement.

Comme un chèque a une durée de validité de 6 mois, sans cette précaution, vous aurez du mal à vous souvenir de tout votre historique.

Pensez également à toujours utiliser un stylo indélébile et occupez tout l'espace lorsque vous écrivez le montant en chiffres et lettres. « *Il ne faut pas hésiter à tirer un trait après les lettres et les chiffres pour s'assurer que le chèque soit débité du bon montant, sans qu'un escroc puisse modifier les données* ».

Enfin, si le montant du chèque est très important, « *collez une bande de scotch sur le montant rédigé et envoyez-le par courrier avec accusé de réception* » (vérifiez auprès de la banque qu'elle acceptera ce chèque).

Ainsi, un fraudeur ne pourra pas changer le montant ou l'ordre, au risque de rendre le chèque impossible à encaisser.

### Prudence avec votre carte bancaire

Pour sécuriser votre carte, protégez l'accès à ses données (numéro, date de validité et cryptogramme à trois chiffres au dos). Si par hasard un pirate s'en empare, il pourra régler des achats à distance avec.

Et comme la carte sera toujours en votre possession, vous ne soupçonnerez rien. Conservez-la sur vous dans un étui qui masque les données inscrites dessus.

**Des personnes laissent parfois traîner leur carte sur leur bureau après l'avoir utilisée, n'importe qui peut alors avoir accès aux numéros et les utiliser ensuite frauduleusement.**

Dans la même logique, ne la laissez pas sans surveillance dans votre veste ou votre sac à main dans un endroit public, il est très facile pour un voleur aguerri de retenir par cœur un numéro.

Ne la confiez pas non plus à un commerçant que vous ne connaissez pas, mais suivez-le jusqu'au terminal pour régler votre achat.

Enfin, ne notez pas votre code secret, tapez-le toujours à l'abri des regards indiscrets et ne le communiquez à personne. Sinon, en cas de vol, votre banque pourrait mettre en cause votre négligence et ne pas vous rembourser.

## 7 CONSEILS POUR ÉVITER LE PIRATAGE

La meilleure protection contre les fraudes bancaires consiste à ne jamais vous faire pirater vos données personnelles.

Pour cela, adoptez de bons réflexes lorsque vous utilisez les services en ligne de votre banque.

**Voici les sept principaux conseils que nous vous engageons à suivre.**

### A. Mettez vos coordonnées à jour

Si vous changez de numéro de portable, déménagez ou utilisez une autre adresse e-mail, demandez à votre conseiller bancaire de mettre vos coordonnées à jour.

En cas de suspicion de fraude, il pourra ainsi vous joindre pour vérification.

Si vous partez en vacances, emportez avec vous les numéros de téléphone vous permettant de faire opposition, la ligne directe de votre conseiller et son e-mail pour le prévenir rapidement en cas de souci.

### B. Protégez votre ordinateur

Protégez l'accès à l'ordinateur auquel vous vous connectez pour consulter vos comptes en ligne. Installez un mot de passe pour y accéder, cela n'empêchera pas un pirate d'y accéder, mais cela lui compliquera la tâche.

Si vous utilisez également une tablette et un téléphone mobile, multipliez les mots de passe. Et ne les notez pas sur un post-it collé à l'écran, au dos de l'ordinateur ou dans le premier tiroir de votre bureau...

Ensuite, installez un antivirus et téléchargez régulièrement ses mises à jour « officielles », provenant du site de l'éditeur du logiciel.

Certains pirates rusés lancent en effet des « offres promotionnelles » pour des antivirus infectés.

Acceptez également toutes les mises à jour des programmes installés sur votre ordinateur, elles réparent des vulnérabilités détectées par les éditeurs.

Enfin, exécutez régulièrement le scan (ou analyse régulière) de votre ordinateur en lançant votre antivirus. Cela lui permet de vous signaler un fichier infecté et d'éviter la propagation du virus.

### C. Protégez votre connexion Internet

Il faut aussi protéger votre connexion Wi-Fi, sur votre Box, avec un mot de passe complexe. Si vous utilisez du Wi-Fi en libre accès pour vous connecter sur des sites sensibles, cela revient à blinder votre porte et laisser toutes vos fenêtres ouvertes.

Si vous recevez régulièrement des personnes chez vous, pensez à modifier le code de votre Wi-Fi après leur passage.

Évitez d'utiliser un accès Wi-Fi ouvert à tous (aéroport, gare) ou un ordinateur en libre accès (bibliothèque…) pour vous connecter sur les services en ligne de votre banque : si des pirates se trouvent à proximité, ils n'auront aucun mal à récupérer vos données personnelles.

### D. Gérez votre session

Prenez l'habitude de vous déconnecter systématiquement à la fin de vos opérations, que ce soit sur ordinateur ou via un téléphone portable.

Il est dangereux de laisser une session ouverte trop longtemps, car un escroc peut profiter de ce laps de temps pour entrer sur votre compte.

De la même façon, n'enregistrez pas votre identifiant sur les sites et refusez cette option, en général proposée en début de connexion. Si un voleur prend la main sur votre ordinateur, il accèdera bien plus facilement à vos comptes.

Même réflexe à prendre sur les sites de e-commerce : refusez d'enregistrer les coordonnées bancaires de votre carte (l'option est proposée pour vous éviter de les retaper à chaque achat).

Sinon, en cas de piratage du serveur de l'entreprise, les voleurs auront accès à votre numéro de carte.

### E. Multipliez les adresses e-mail

Ouvrez plusieurs adresses Internet à votre nom, ce procédé est gratuit. Servez-vous d'une adresse spécifique et sécurisée pour vos transactions importantes.

Ne la communiquez qu'à des tiers de confiance : banque, service des impôts… et ne l'inscrivez sur aucun document susceptible d'être piraté.

Ouvrez une deuxième adresse pour vos communications courantes. Enfin, un troisième e-mail sera lié à un compte « poubelle », vous l'utiliserez pour recevoir vos newsletters et offres promotionnelles et réaliser vos achats sur Internet…

Comme cette adresse circulera sur le Net, elle a plus de chances d'être piratée. Mais les escrocs ne pourront rien en faire, puisqu'elle ne sera reliée à aucune donnée sensible. Bien entendu, chacune de vos adresses doit avoir un mot de passe différent.

## F. Soyez méfiant

Les pirates utilisent souvent des informations trouvées sur les réseaux sociaux pour vous piéger. Si, par exemple, un membre de votre famille est parti en vacances dans les Caraïbes, il postera sur Internet des photos de lui devant une eau turquoise.

Peu de temps après, vous recevrez un e-mail angoissé de sa part vous demandant de lui virer des fonds parce qu'il s'est fait voler son portefeuille.

**Alerte !** Prenez le temps de vérifier que c'est bien le cas et non que son carnet d'adresses a été piraté à son insu.

N'ouvrez jamais des documents en pièces jointes si vous ne connaissez pas l'expéditeur. Et faites preuve de méfiance si l'e-mail provient d'un membre de votre famille, des impôts ou d'un commerçant. Les pièces jointes peuvent transporter des virus, de type « cheval de Troie ».

**De manière générale, n'ouvrez pas de fichier en *.exe, .com, .msi, .scr, .hta, .cpl, .cmd, .bat…*** Si vous avez un doute sur un e-mail, supprimez-le et videz votre poubelle, sinon le fichier restera sur votre ordinateur.

## H. Sécurisez votre téléphone

Si vous utilisez un smartphone avec un accès Internet et consultez vos comptes dessus, mêmes conseils.

Protégez son accès par un code secret. En cas de vol ou de perte, l'escroc aura du mal à accéder à votre application bancaire et à vos données personnelles.

Dès que vous constatez le vol ou la perte de votre portable, changez les mots de passe de vos boîtes mails si elles sont synchronisées sur votre mobile.

Modifiez également le mot de passe d'accès à votre site bancaire. Enfin, prévenez votre opérateur pour qu'il déconnecte votre carte Sim et empêche le voleur de recevoir des codes de confirmation d'achat par SMS.

Si vous utilisez la fonction Bluetooth ou Wi-Fi chez un ami ou dans un lieu public, désactivez-la après utilisation pour éviter les intrusions à distance dans votre appareil.

Enfin, sachez que les derniers systèmes d'exploitation intègrent une fonction « effacer les données du téléphone à distance ».

## Banques en ligne : Adoptez les bons réflexes

En matière de services, les banques en ligne offrent davantage de possibilités « online » que les banques de réseaux.

Pour les banques de réseaux, de nombreuses fonctionnalités doivent encore être réalisées par le conseiller financier. « *C'est un manque de souplesse, mais les opérations ont aussi l'avantage d'être plus sécurisées* ».

Autre enseignement : les banques ont très peu recours aux e-mails et privilégient, comme moyen de double authentification, les SMS et les courriers postaux. D'autant qu'elles ont toutes une messagerie interne, qui permet d'échanger, une fois connecté, de façon nettement plus sécurisée que sur un mail extérieur.

**Ainsi, si vous recevez un e-mail d'une banque vous demandant des informations personnelles, vous devez clairement vous méfier.** Il peut en effet s'agir de « Phishing » ou « hameçonnage ».

### Virez plus ou moins dans les règles...

Dans toutes les banques, il est possible d'effectuer des virements en ligne. Mais seule une banque sécurise ses virements par une double authentification (SMS).

Les autres établissements ne demandent rien ou juste de retaper votre mot de passe, ce qui laisse tout loisir à un voleur qui aurait piraté votre code d'effectuer des virements en sa faveur depuis votre compte en banque.

Les établissements permettent tous d'ajouter un bénéficiaire en ligne. Opération sécurisée par une double authentification (souvent votre mot de passe puis un code envoyé par SMS sur votre smartphone).

Certaines banques demandent en ligne l'autorisation d'ajouter des destinataires. Vous recevez ensuite un code de validation sur votre téléphone mobile.

### Modifiez vos coordonnées personnelles

Dans votre espace personnel, accessible sur votre site bancaire, vous retrouvez vos coordonnées personnelles communiquées au moment de l'ouverture de votre compte.

Ces données peuvent être modifiées plus ou moins facilement en ligne : le changement de numéro de téléphone en ligne s'effectue sans aucune sécurité, ou vous devez passer par votre conseiller bancaire, envoyer un courrier ou un SMS (payant pour certain établissement).

Modifier votre adresse mail est aussi souvent possible en ligne, mais « *cela est moins problématique car les banques utilisent très peu les e-mails* ».

Enfin, en cas de déménagement, seule la moitié des banques permettent de préciser votre nouvelle adresse en ligne, cette formalité doit se faire par courrier ou via un conseiller par téléphone pour les autres.

## Pour les conseils, on repassera...

Autre enseignement : tous les sites bancaires proposent une aide, plus ou moins pertinente et détaillée, sur les questions liées à la sécurité. Certaines banques ont fait de réels efforts de pédagogie. En revanche, les conseils sont un peu limités chez d'autres.

**Mais carton rouge pour presque tous les établissements :** ces conseils ne sont pas toujours faciles à trouver sur leurs pages d'accueil. En outre, l'utilisateur n'est jamais obligé de les lire avant d'utiliser les services en ligne de son établissement.

D'ailleurs, pour éviter les piratages, des logiciels de sécurité existent, parfois gratuits, parfois payants. Aucune banque ne les mentionne sur ses pages.

Seules deux banques proposent un antivirus, développé par IBM. D'autres offrent une barre de confiance destinée à lutter contre le risque de piratage (« phishing ») en vous indiquant de façon visible que vous vous trouvez bien sur leur site. Certaines vous permettent de configurer des alertes. Ainsi, en cas de mouvements importants ou inhabituels sur votre compte, votre banque vous envoie un SMS pour vous prévenir. Un bon moyen de déceler rapidement une fraude.

Enfin, d'une manière générale, les banques vous inciteront à utiliser leurs applications sur mobiles, ceux-ci n'étant quasiment jamais infestés par un virus.

## Les règles à suivre pour limiter les risques

Si un pirate veut vraiment accéder à vos comptes bancaires, il est probable qu'il trouvera la solution. Mais en adoptant certains comportements à risque, vous lui faciliterez grandement la tâche.

**Voici ceux que vous devez éviter :**

- ne dévoilez pas trop d'informations personnelles sur les réseaux sociaux (date de naissance, numéro de téléphone, adresse postale…), elles sont en libre accès,
- n'écrivez pas votre mot de passe. Mémorisez-le !
- servez-vous d'un mot de passe sécurisé,
- n'utilisez pas un ordinateur « à risque » (faille/pas de protection, libre-accès à différentes personnes),
- évitez de passer par les réseaux Wi-Fi non protégés pour consulter vos comptes bancaires sur Internet (hot spot d'un aéroport, d'une gare, d'un parc, d'une bibliothèque…),
- n'oubliez pas de toujours vous déconnecter avant de quitter la page Internet de la banque ou son application mobile (ou forcez la fermeture),

# VOLS À LA FAUSSE QUALITÉ

## Se protéger des vols à la fausse qualité

Des voleurs se font passer pour des plombiers, des employés EDF ou même des policiers pour entrer chez leurs victimes. Comment réagir ?

En 2016, une forte hausse des vols à la fausse qualité (par exemple : + 67 % en Seine-et-Marne) a été enregistrée, notamment dans les grandes agglomérations. Les personnes âgées sont particulièrement visées.

Et les chiffres officiels sont certainement sous-évalués, car de nombreuses victimes ne portent pas plainte par honte d'avoir été mystifiées.

## Les méthodes des voleurs

Les variantes des vols à la fausse qualité sont nombreuses. Mais le mode opératoire est souvent très ressemblant. Un faux plombier, employé EDF, coursier ou encore agent de l'assurance maladie se présente au domicile d'un particulier qui le laisse entrer chez lui.

Le visiteur profite d'un moment d'inattention de son hôte pour lui dérober deux ou trois objets puis prend congé.

Quelques instants plus tard, de faux policiers (avec brassard, blouson et/ou carte) se présentent. Ils indiquent à la victime que la personne reçue était un voleur (ils montrent d'ailleurs les objets récupérés sur celui-ci).

Ensuite, ces individus demandent au particulier de vérifier que sa carte bancaire ou des valeurs (liquide, bijoux, or…) n'ont pas été dérobées.

Ils vont avec lui… et tentent de s'emparer du butin qui leur est montré. Dans la majorité des cas, ces vols se déroulent heureusement sans violence. Tout est dans la ruse et la persuasion !

## Les conseils à suivre

Lorsque l'on sonne, avant d'ouvrir, vérifiez qui se présente puis discutez avec la personne en laissant la porte fermée avec l'entrebâilleur.

Exigez qu'elle vous montre la carte attestant de son statut si elle fait état d'une qualification professionnelle. Examinez le document avec attention (il s'agit parfois d'imitations grossières).

Effectuez également des vérifications auprès de son « employeur ».
Par exemple, si votre visiteur dit être policier, contactez le commissariat.

Enfin, si le voleur à la fausse qualité est entré chez vous, suivez-le à la trace et ne lui indiquez jamais où vous avez rangé argent, bijoux, cartes bancaires…

**Bon à savoir**

Il faut éviter d'indiquer sur sa boîte aux lettres ou sa sonnette que l'on vit seul(e) (exemple, Mme X). Cela renforce la vulnérabilité face à ce type de voleurs.

# Les arnaques : Comment les éviter ?

Nous pourrions continuer encore sur de nombreuses pages et traiter beaucoup d'autres sujets, comme par exemple les loteries, la publicité, les locations de vacances et autres, les agences matrimoniales, etc …

Notre but n'était pas d'être exhaustif, mais d'attirer votre attention sur les principaux genres de tromperies et de vous donner le maximum d'informations pour les éviter ou y faire face.

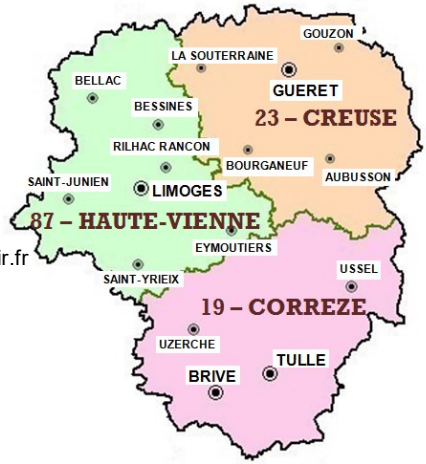
Pour le reste, n'hésitez pas à nous consulter dans les nombreuses permanences de la région Limousin (voir carte ci-dessous), sur nos sites Internet départementaux ou national (quechoisir.org).

Vous pouvez aussi nous lire et vous informer avec les revues Que Choisir, Que Choisir Argent, Que Choisir Santé et les spéciaux Que Choisir.

***Rappelez-vous que, vous les consommateurs, vous êtes à la fois notre seule force et notre seule ressource.***
***Votre soutien nous est indispensable.***

## Rejoignez-nous
## Adhérez et devenez bénévoles

UFC-Que Choisir
Haute Vienne
4 Cité Casimir Ranson
**87000 LIMOGES**
☎ : 05 55 33 37 32
Site Internet :
hautevienne.ufcquechoisir.fr




UFC-Que Choisir
Creuse
25, Ave Pierre Leroux
BP 242
**23005 GUERET cedex**
☎: 05 55 52 82 83
Site Internet :
creuse.ufcquechoisir.fr

UFC-Que Choisir
Corrèze
Maison du bénévolat
10 Bd Marx Dormoy
**19100 BRIVE**
☎: 05 55 23 19 37
Site Internet :
correze.ufcquechoisir.fr

## L'Union Fédérale des Consommateurs (UFC) Que Choisir du Limousin, Corrèze, Creuse, Haute-Vienne