# Les Arnaques : lançons la contre-attaque

Livret d'information sur les arnaques les plus récurrentes.

**UFC Que Choisir 43**
29, boulevard Chantemesse
43 000 Aiguilhe
**04.71.02.29.45**
**Notre mail** : ufc.quechoisir43@orange.fr
**Notre blog :** http://www.ufcqc43.com/
**Notre site :** http://hauteloire.ufcqchoisir.fr/


# Sommaire

- *Témoignages .....3-4*

- *Différents types d'arnaques avec quelques conseils pour les prévenir au mieux :*
*- Arnaques téléphoniques.....5-6-7*
*- Arnaques sur Internet.....8- 9-10*
*- Arnaques des cartes bancaires .....11-12-13*

- *Conclusion.....14-15*

- *Jeux :*
*Mots croisés.....16-17*
*Quizz.....18-19*

# Prévention des arnaques en Haute-Loire

- **Direction Départementale de la Cohésion Sociale et Protection de la Population**
  **3, chemin du Fieu**
  **43 000, Le Puy-en Velay**

(Nous remercions M. Bernard, Chef de Pôle Concurrence, Consommation et Répression des Fraudes (CCRF) de son témoignage sur l'action de la DDCSPP43)

La DDCSPP 43 est une direction interministérielle, qui sous l'autorité du Préfet, met en œuvre des politiques publiques ministérielles décidées par le gouvernement. *Ses missions principales sont la cohésion sociale (politique de la ville, aide aux sans-abris...) et la protection des populations (protection animale, sécurité sanitaire, protection économique des consommateurs*.

- ***Niveau national :*** *autour de 2 000 enquêteurs de la DGCCRF sont implantés dans les directions départementales*

- ***Niveau départemental :*** *le pôle CCRF compte 5 enquêteurs*
  *- 450 contrôles en 2017 (sécurité des produits et lutte contre les fraudes)*
  *- 30 % de suites à ces contrôles. Parmi ces 30%, 1/3 conduit à des poursuites pénales ou administratives*
  *-120 demandes écrites des consommateurs (signalements ou demandes d'informations)*
  *- 400 demandes téléphoniques*

- **Groupement de Gendarmerie Départementale de la Haute-Loire**
  **Caserne Romeuf, 21 rue du 86ème Régiment d'infanterie**
  **43012, Le Puy-en-Velay**

(Nous remercions Mr. Heyraud Chef d'escadron de la gendarmerie de Haute-Loire pour son témoignage concernant l'action de la gendarmerie contre les arnaques)



*Mr. Heyraud, chef d'escadron à la gendarmerie du Puy-en-Velay déclare que des centaines d'arnaques par an sont enregistrées dans leur base sur tout le département. Ainsi, 20 gendarmes qualifiés CTP (Correspondants Territoriaux de Prévention) interviennent dans des actions de prévention auprès du grand public afin de le sensibiliser sur ce type de risque. Pour lui, la prévention reste nécessaire, il faut poursuivre les efforts. Les délinquants sont en perpétuelle inventivité et malheureusement, les scénarios les plus simples sont ceux qui fonctionnent souvent le mieux. Il rappelle que les arnaques sur Internet restent élevées.*

- **Commissariat de Police du Puy-en-Velay**
  **1, rue de la Passerelle**
  **43 000, Le Puy-en-Velay**

(Nous remercions Mr. Mazière, Capitaine de Police du Puy-en-Velay pour son témoignage sur l'action de la sûreté urbaine contre les arnaques)

*Mr.Mazière, capitaine de police du Puy-en-Velay, nous indique que les arnaques qui reviennent le plus sur le département sont les piratages de carte bleue, les arnaques sur des sites de vente, les arnaques étrangères, les arnaques sur les sites de rencontre ou sur les réseaux sociaux. Le capitaine indique que 99 % des gens ne tombent pas dans le panneau, mais que les 1 % restant, suffisent pour dérober beaucoup d'argent au profit des escrocs. « Les escrocs jouent sur la crédulité des gens » nous dit Mr. Mazière comme nous l'a confirmé aussi Me. Bellut.*

- **Cabinet d'avocats Mtres. Bellut, Pays et Robillard**
  **21 bis Place Michelet**
  **43 000 Le Puy-en-Velay**

(Nous remercions Me. Bellut, avocat partenaire de l'UFC Que Choisir 43 pour son témoignage sur les conséquences des arnaques pour les consommateurs).

*Il est facile de monter des scénarios qui décrédibilisent les arnaques. Me. Bellut affirme que de nombreux escrocs ne sont pas poursuivis car il s'agit souvent de sociétés étrangères qui disparaissent. Les gens laissent tomber les poursuites, surtout quand il s'agit de petites sommes car un procès reviendrait plus cher que la somme perdue sans forcément avoir des résultats positifs au final.*

# Arnaques par téléphone

*Depuis un certains nombre d'années en France, la mode est passée à la recherche des bonnes affaires, du bon marché. Ainsi on cherche à acquérir des biens et/ou des services à des prix défiant toute concurrence. Tout ceci au profit parfois de certains escrocs qui ne manquent pas d'imagination. Le problème par téléphone est que l'on ne voit pas la personne et que l'on est plus susceptible de « tomber dans le panneau » des escrocs.*

## Les principales fraudes téléphoniques:

### Rappel d'un numéro surtaxé

Il s'agit d'un appel malhonnête (« ping call » ou spam vocal) ou un SMS indésirable qui incite à rappeler vers un numéro surtaxé.

**- Pour le ping call ou call back :** votre téléphone sonne : soit vous décrochez et personne ne se trouve au bout du fil, soit vous ne décrochez pas et le téléphone continue de sonner, et cela peut s'avérer agaçant. Si vous rappelez ce même numéro, votre appel est surtaxé à 1 ou 2€.

Les numéros commencent fréquemment par : 0899, 0897, 1020.

Mais pour ne pas susciter la méfiance, les escrocs passent désormais par des numéros en 01, 02, 05 etc.



**- Les arnaques par SMS :** on vous indique que vous avez gagné un chèque ou un prix, que l'on a constaté une fraude sur votre compte bancaire, ou bien encore qu'il y a un problème au niveau de votre ligne téléphonique. Vous êtes invité à rappeler un numéro. Le message pour le consommateur est « digne de confiance » car il provient d'organismes officiels **usurpés** comme EDF, les impôts… Hélas le numéro est un numéro surtaxé.

### Les pratiques commerciales agressives

Il s'agit souvent d'appels répétés vous faisant croire que vous êtes l'heureux gagnant d'un jeu ou d'une loterie.

Ne soyez pas trop crédule : sachez que vous pouvez toujours couper la communication sans avoir à vous justifier auprès de votre interlocuteur.

### L'escroquerie pour obtenir des éléments confidentiels par téléphone fixe

Cette arnaque consiste à se faire passer pour un service d'assistance technique (ex. : grande marque d'ordinateur, fournisseur d'accès à internet, etc.). Elle cible les possesseurs d'ordinateurs. Sous le prétexte d'un problème technique, on vous demande d'aller sur un site web pour installer un logiciel qui permettra d'avoir accès à votre ordinateur pour le réparer ou réparer la connexion. Cette escroquerie vise à :

- installer un logiciel malveillant pour capturer vos données confidentielles,
- contrôler à distance votre ordinateur et le rendre vulnérable,
- vous demander à terme votre numéro de carte de crédit ou de compte bancaire,
- vous rediriger vers des sites web frauduleux.

## pour lutter contre les arnaques téléphoniques :

- vous pouvez signaler le **numéro frauduleux au 33700**. Il suffit d'envoyer un SMS au 33700 en inscrivant « spamvocal », suivi du numéro frauduleux.
- **le service Bloctel** : liste d'opposition au démarchage téléphonique. Les consommateurs peuvent s'inscrire gratuitement sur ce registre d'opposition.

bloctel.gouv.fr

- méfiez-vous des numéros inconnus, même ceux commençant par 06, qui peuvent également être erronés ou frauduleux. Pour repérer les numéros frauduleux, il existe le site : *fauxnumeros.fr*
- ne rappelez jamais un numéro inconnu n'ayant laissé aucun message sur votre répondeur et ne jamais communiquer d'informations personnelles
- demandez toujours à votre interlocuteur d'envoyer un courrier afin d'avoir des informations et des preuves



# Arnaques par Internet


*Internet est un espace de liberté où chacun peut communiquer et s'épanouir. Les droits de tous doivent y être respectés, pour que la toile reste un espace d'échanges et de respect.*

### >Escroqueries sans frontière :

Un malfaiteur étranger piège un internaute par un outil de rencontre en ligne (Facebook, Skype…) et lui demande une aide financière sous un prétexte très bien élaboré.

### > Fuites d'informations et victimes d'usurpation d'identité sur Internet :

L'usurpation, c'est quoi ?

- récupérer par divers moyens, toutes informations concernant une personne :
  - Montant d'impôts trop perçus,
  - erreur de facturation sur électricité ou gaz,
  - piratage des comptes de messagerie électronique ou réseaux sociaux,
- utiliser, sans votre accord, des informations personnelles permettant de souscrire, sous votre identité, un crédit, un abonnement ou nuire à votre réputation.

### > Emails malveillants et Hameçonnage ou Phishing :

Le principe du *phishing* est de récupérer des données personnelles sur internet.
L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet.
Des mails à connotation alarmiste ou d'autres alléguant d'un prétendu remboursement en faveur de l'internaute sont ensuite massivement adressés.

Ils semblent provenir d'une source de confiance (banque, CAF, impôts, etc.) et invitent à se rendre sur une page de formulaire afin de fournir des données personnelles et souvent à caractère financier.


| LES INDICES QUI DOIVENT VOUS ALERTER ! | |
|---|---|
| La présentation | Ne vous faites pas abuser par la présence de logos officiels, de liens vers des sites connus ou d'informations vous concernant. La présence de fautes d'orthographe ou de grammaire doit aussi vous mettre la puce à l'oreille. |
| L'expéditeur | Les pirates n'hésitent pas à se faire passer pour une banque, une administration (Caf, service des impôts…), une entreprise (EDF, Orange…) voire une personne de votre connaissance pour gagner votre confiance. |
| Le message | Ils jouent le plus souvent sur l'empathie (une personne a besoin d'aide), l'urgence (votre électricité sera coupée si vous ne réagissez pas vite), la peur (vous risquez d'être poursuivi si vous ne payez pas) ou font miroiter une promesse d'argent ou un remboursement. |
| Le lien hypertexte | Vérifiez que l'adresse du site officiel vers laquelle il est censé renvoyer soit la bonne (www.microsoft.com et pas www.security-microsoft.com ou www.micosoft.com par exemple). |



## Les bons réflexes à adopter

- ✓ Choisissez des mots de passe mélangeant chiffres, lettres, caractères spéciaux (évitez date de naissance ou n° de département)
- ✓ N'utilisez pas le même mot de passe pour plusieurs applications
- ✓ N'enregistrez jamais vos mots de passe dans les ordinateurs accessibles à d'autres personnes
- ✓ Ne cliquez jamais sur les liens contenus dans les messages dont vous n'êtes pas certain de la provenance
- ✓ Ne réagissez jamais dans l'urgence, même si vous recevez un mail alarmiste
- ✓ N'envoyez rien à une personne non parfaitement identifiable.
- ✓ Faites preuve de bon sens : aucun organisme ne vous demandera par e-mail de lui communiquer des informations personnelles.
- ✓ Signalez l'e-mail sur la plateforme gouvernementale : Internet-signalement.gouv.fr.
  Supprimez-le et videz la corbeille

internet-signalement.gouv.fr
Portail officiel de signalement des contenus illicites de l'Internet

*Pour une protection au quotidien, certains éditeurs d'antivirus proposent des suites complètes comprenant diverses fonctions protectrices, dont l'antiphishing.*

*Vous pouvez vous connecter sur le site www.signal-spam.fr, la plateforme nationale de lutte contre le spam.*

# Arnaques par carte bancaire

*Les vols de coordonnées bancaires explosent. L'an dernier, les comptes de 1,1 million de Français ont été piratés. Un braquage virtuel de plus de 400 millions d'€.*

Voici quelques règles afin d'éviter les arnaques par carte bancaire :

Dissimulez le cryptogramme : les trois chiffres au verso de votre carte. Vous pouvez mettre une pastille dessus pour les cacher. Autre solution : s'équiper d'une carte de nouvelle génération dont le cryptogramme change plusieurs fois par heure. Une CB est plus sûre, mais plus chère…

Le code est bien évidemment confidentiel ! Ne communiquez jamais votre code, notamment par courriel et téléphone où les sollicitations d'escrocs sont fréquentes.

Méfiez-vous des faux claviers et des caméras cachées : ils sont souvent installés sur des distributeurs ou des bornes de pompe à essence. Cachez toujours votre code en tapant sur le clavier et mettez la carte en opposition si elle est « avalée ».

Vérifiez régulièrement vos relevés bancaires



Ne téléchargez pas n'importe quoi : ne téléchargez pas d'applications en dehors des boutiques officielles telles que l'App Store ou le Google Store. Ce sont des nids à virus et voies d'accès à vos données bancaires.

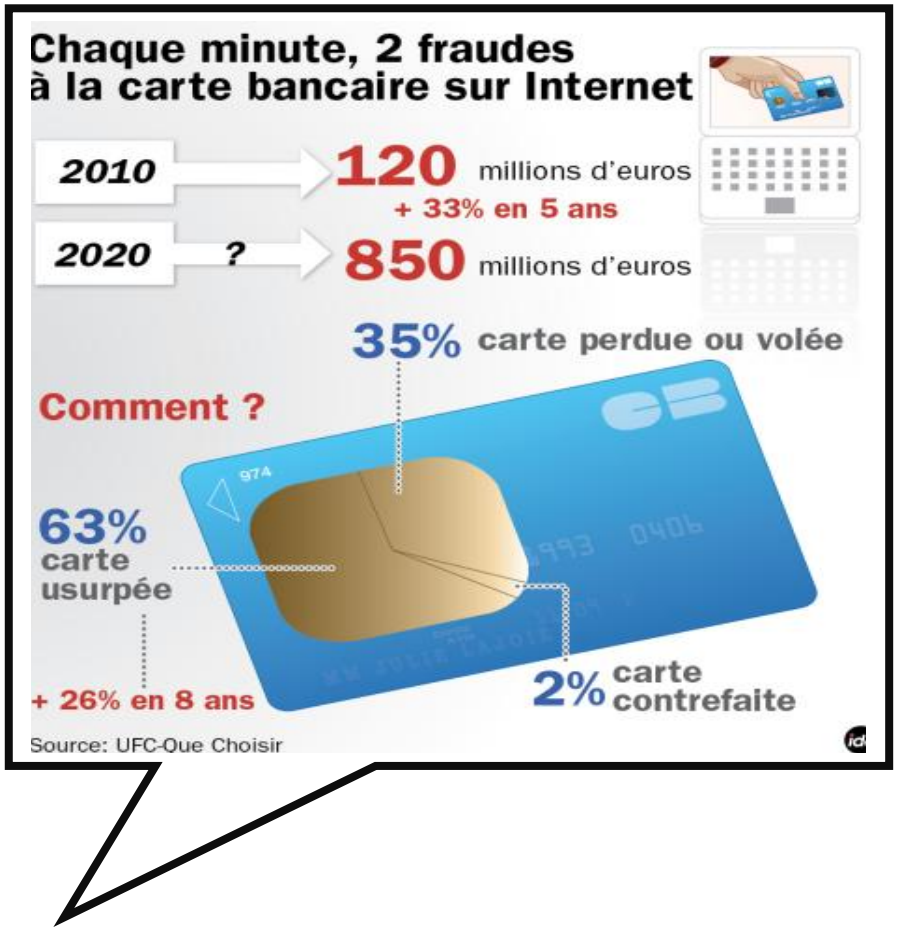
Evitez les sites web non sécurisés : si vous payez un achat en ligne, vérifiez que le site est sécurisé. Comment ? Un petit cadenas doit s'afficher à côté de l'adresse du site indiquée en « https » (avec le « s » de sécurité). Mieux vaut aussi privilégier les sites français, souvent plus protégés.

Pensez à l'antivirus : de plus en plus de ventes se font avec un portable. Equipez-le d'un antivirus en sachant que même gratuits, ils sont performants.

Ne quittez jamais votre carte des yeux lors d'un paiement chez un commerçant : n'acceptez pas que l'employé parte avec, il s'agit ici de la principale fraude de détournement de carte bancaire.

A la banque, exigez des contrôles : assurez-vous que votre banque propose bien le code 3D Secure (un code envoyé par SMS par votre banque) qui permet de confirmer un paiement en ligne.

La loi impose aux établissements de rembourser immédiatement leurs clients en cas de fraude constatée. En général, lorsque la fraude dépasse 4000 €, il vaut mieux prendre un avocat.




**Ceci mêle donc à la fois les arnaques sur Internet et les arnaques par carte bancaire !**



# Pour conclure…

Avec des scénarios très affinés et très bien rodés, les fraudeurs sont aujourd'hui prêts à tout pour tromper les gens et gagner de l'argent « sur leur dos ». Ils sont à l'affût des meilleures idées afin d'arnaquer des personnes de manière détournée pour que ces derniers ne se rendent compte de rien.

De nombreux autres types d'arnaques existent comme certains démarchages à domicile, certaines arnaques à l'emploi, certaines arnaques automobiles, certaines offres de voyance, de nombreux autres détournements sur Internet …

Les personnes les plus touchées sont les personnes âgées, plus vulnérables donc plus susceptibles de tomber dans les pièges des arnaqueurs.

Différents organismes existent pour aider les personnes arnaquées mais il est certain que ces personnes ne récupèrent pas toujours leur dû car les traces disparaissent et les escrocs avec.

Il est donc important d'avoir quelques connaissances sur le sujet pour se prémunir au mieux de ces tromperies mensongères.