Conférence des évêques de France

Service juridique

Paris, le 21 février 2017

VADEMECUM

N°7 – FEVRIER 2017

LES ARNAQUES

PREAMBULE

Depuis des années les arnaques par internet, SMS, contrat de vente à distance, se multiplient et touchent particuliers, professionnels, collectivités, associations … L'Eglise n'est pas épargnée.

Sur internet, il est facile de se faire escroquer surtout lorsqu'on est « novice ». Fraude à la carte bleue, *phishing* (usurpation d'identité, mot de passe...) sont les pratiques illégales les plus dénombrées.

Ce vademecum a pour but de vous donner les moyens pour éviter de tomber dans de nombreux pièges.

Arnaqueurs, escrocs, qui sont-ils ?

- Généralement, dans les cas d'arnaque par SMS ou internet, les arnaqueurs ont préalablement piraté votre boite mail ou le répertoire de votre téléphone, ceci leur permettant de pouvoir se présenter comme l'une de vos connaissances ou l'un de vos amis.

- Les escrocs créent des profils en utilisant de faux noms de sociétés, de faux logos, de faux document à en-tête, de fausses photos afin de rentrer en contact avec leurs potentielles victimes. La mise en confiance de la « cible » est le préambule indispensable à toute escroquerie.

- Dans les affaires d'arnaques, tout l'art des sociétés commerciales consiste à détecter les personnes foncièrement honnêtes et un peu « candides » afin d'exercer leur savoir-faire. Les vendeurs sont toujours d'une bonne présentation, la documentation et le discours suscitent la confiance.

Où déclarer ces arnaques ?

- Les services de contrôles nationaux.
- Informer la Direction départementale de la concurrence, de la consommation et de la répression de fraude (DDCCRF) ou toute autre administration en précisant la société litigieuse, la date de signature du contrat en cause, la ou les entorses au code de la consommation.
- Douanes : http://www.douane.gouv.fr/
- Police Nationale : http://www.police-nationale.interieur.gouv.fr/
- Ministère de l'intérieur – Direction centrale de la police judiciaire : OCLCTIC (l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication : http://www.interieur.gouv.fr/
- Centre de surveillance du commerce électronique à Morlaix (CSCE)/DGCCRF : http://www.economie.gouv.fr/dgccrf

Une distinction à faire entre pièges dit non contractuels et pièges dit contractuels

Ces arnaques, dont nous avons donné ci-dessus une liste non exhaustive, peuvent être classées en deux groupes présentant chacun des critères propres :

- les pièges dits « non contractuels » d'une part regroupant les arnaques non régies par un contrat, vous ne signez rien, vous ne rencontrez pas de commerciaux qui viennent démarcher pour vendre un produit ou un service … l'arnaque au SMS ou au « *phishing* » en sont des exemples. Dans ce cas c'est vous qui êtes « guidés » par l'escroc à divulguer spontanément, vos coordonnées bancaires, envoyer de l'argent

- et les pièges dits « contractuels » d'autre part qui sont eux régis par un contrat, bon de commande, documents signés qui vous engagent sur un prix, une durée … Exemple : l'arnaque à l'annuaire ou « *scareware* ».

C'est cette articulation qui sera retenue ci-après.

I – Piège dit « non contractuel »

- Les indices qui doivent vous alerter
- Les bons réflexes

II – Piège dit « contractuel »

- Le processus
- Les indices qui doivent vous alerter
- Pour vous aider
- Les bons réflexes

I - PIEGE DIT « NON CONTRACTUEL », QUI NE NECESSITE AUCUNE SIGNATURE

Vous recevez un courrier électronique dont l'en-tête ressemble à celui d'un établissement de confiance : banque, caisse d'allocations familiales, impôts, EDF, site marchand ou opérateur de téléphonie. Cet e-mail, souvent alarmiste, vous demande de communiquer vos données confidentielles, et de façon urgente. Objectif : si vous y répondez, l'escroc en ligne peut réaliser des opérations frauduleuses sur votre compte.

Il s'agit avant tout de questions de bon sens. Vous devez toujours vérifier la manière dont est rédigé le SMS ou le message internet, y-a-t-il des fautes d'orthographes ? L'ami qui peut vous demander votre aide agirait-il de cette façon ?

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

Il joue 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 fait 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

- Pour se protéger, il faut commencer par protéger son ordinateur : antivirus performant, pare-feu, logiciel anti espion... N'hésitez pas à vous faire accompagner ou conseiller.
- Ne jamais répondre au message, ne cliquez sur aucun lien y compris celui censé permettre de se désabonner, n'ouvrez pas de pièce jointe et ne remplissez aucun formulaire. en répondant vous permettez l'accès à votre boîte mail et par conséquent à tous vos contacts.
- Lors d'un appel téléphonique, il vaut mieux mettre fin à la conversation et appeler soi-même le service client concerné.
- Ne jamais communiquer de coordonnées bancaires avant d'avoir vérifié l'identité de l'interlocuteur et le bien-fondé de sa demande et ce quel que soit le contenu du courriel.
- Faites preuve de bon sens : aucun organisme ne vous demandera par e-mail de lui communiquer des informations personnelles.
- En cas de doute, contactez l'organisme censé vous avoir envoyé l'e-mail par téléphone ou en passant par la page d'accueil de son site Internet et non par le lien proposé dans l'e-mail. Supprimez-le et videz la corbeille.
- Pour une protection au quotidien, certains éditeurs d'antivirus proposent des suites complètes comprenant diverses fonctions protectrices, dont l' « *antiphishing* ».
- Signalez l'e-mail sur la plateforme gouvernementale Internet-signalement.gouv.fr ou signalez ces messages aux autorités nationales Il suffit d'envoyer un SMS au 33 700 avec le texte *"Spam vocal"*

suivi du numéro de l'arnaque. Si vous avez déjà rappelé l'escroc, vous pouvez vous tourner vers le service "Info escroquerie" au 0811 02 02 17. Surtout ne versez pas d'argent.

II - PIEGE DIT « CONTRACTUEL », QUI NECESSITE UNE SIGNATURE

LE PROCESSUS

Première partie du processus

L'important pour le vendeur est d'arracher une signature authentifiée par un cachet sur un document qui engage irrévocablement le signataire. Ce document est généralement incomplet, il comporte aussi des conditions générales de vente de rédaction obscure et en petits caractères. Souvent, le vendeur peut ne pas laisser de copie du document signé, prétextant un envoi de confirmation par retour du courrier, ce qui peut permettre de le compléter hors la vue du signataire… Enfin, le vendeur peut aussi solliciter le paiement immédiat d'un acompte, ce qui est strictement interdit.

Par la suite, l'escroc envoie rapidement un courrier de confirmation de visite et l'accord pour enregistrer la commande aux conditions convenues… qui ne sont d'ailleurs pas toujours détaillées… ou qui font apparaître des conditions non remarquées sur le document d'origine.

Enfin, une facture est adressée, alors même que le contrat souscrit n'a encore subi aucun début d'exécution et qu'aucune date de mise à disposition du guide, du journal ou plus généralement du support sur lequel doit paraître l'information, n'est avancée.

Si le paiement ne suit pas, un processus funeste s'enclenche :

- Envoi de la première lettre de relance 4 à 6 semaines plus tard par courrier simple.
- Envoi d'une seconde lettre de relance par courrier simple sous le même délai en précisant cette fois que le dossier est transmis au service contentieux en cas de non-paiement sous un certain délai, en général une quinzaine de jours.

Cette première partie du processus peut prendre de 4 à 6 mois.

Deuxième partie du processus

Le service contentieux, ou baptisé comme tel, confirme la lettre précédente par un ou deux courriers. Après ce stade, deux possibilités : soit la transmission du dossier à une société de recouvrement de créances, soit à un avocat.

La société de recouvrement et/ou l'avocat envoient un courrier de mise en demeure par lettre recommandée avec avis de réception en précisant qu'à défaut de paiement immédiat une assignation en justice qui entraînera une condamnation au paiement de la somme principale assortie d'intérêts au taux conventionnel (dont souvent, on entend parler pour la première fois et qui n'apparaissent pas sur le contrat d'origine), ainsi qu'au paiement d'importants dommages et intérêts et des frais de procédure.

Ce courrier peut être suivi d'une autre lettre de même facture ou mieux être délivrée à domicile par le ministère d'un huissier de justice.

Cette seconde partie du processus peut durer de 6 à 12 mois.

Troisième partie du processus

Il s'agit du processus dit « judiciaire ». Plusieurs possibilités sont offertes tant au « créancier - arnaqueur » qu'au « débiteur - victime de l'escroquerie ».

- Pour le « créancier – arnaqueur »

1. La procédure de recouvrement de créance par l'intermédiaire d'un huissier de justice.

2. L'injonction de payer par saisine du juge (tribunal de commerce, d'instance ou de grande instance selon la nature du contrat litigieux et le montant en jeu).

L'injonction de payer est une procédure rapide (3 à 4 semaines) et économique (coût : 100 € maxi). Le juge commis à cette fonction prend une décision au vu des seuls éléments fournis par le créancier (arnaqueur) sans avoir pu entendre les arguments du débiteur (AD, prêtre …) Si le juge estime la requête justifiée, il rend une « *ordonnance portant injonction de payer* » pour la somme qu'il retient. Ce peut être la totalité de la créance ou une partie seulement.

Si, au contraire, le juge rejette la demande, le créancier (l'escroc qui réclame le paiement) ne dispose d'aucun recours, mais il peut engager une procédure judiciaire classique.

Le défendeur n'est pas avisé de cette procédure, il découvre l'action entreprise lors de la délivrance par huissier de l'ordonnance d'injonction de payer à partir de laquelle **il dispose d'un délai d'un mois pour faire opposition. Ce qu'il est conseillé de faire s'il s'agit d'un créancier arnaqueur.**

L'affaire est alors abordée au fond devant le tribunal en présence des parties et/ou de leurs représentants.

3. L'instance au fond.

C'est la procédure classique avec assignation du défendeur devant le tribunal statuant au fond, en premier ou dernier ressort selon l'importance de la créance. La représentation par avocat n'est pas obligatoire devant le tribunal d'instance et le tribunal de commerce. Elle est en revanche obligatoire devant le tribunal de grande instance.

Cette procédure est longue : 12 à 18 mois devant le tribunal d'instance ou le tribunal de grande instance, au minimum 6 mois devant le tribunal de commerce en fonction du plan de charge des tribunaux.

- Pour le « débiteur – victime de l'escroquerie » : le référé devant le juge des référés.

C'est aussi une procédure rapide (4 à 6 semaines). La demande est portée par voie d'assignation du défendeur (AD, prêtre …) devant le juge des référés à une date proche (environ 15 jours). L'assignation est réalisée par un huissier de justice.

Le défendeur a intérêt à se présenter et à contester la demande en produisant un dossier de plaidoirie accompagné des pièces justificatives. En effet, dans le cadre de contestation d'une créance, le juge des référés est le juge de l'évidence. S'il a le moindre doute du bien-fondé de la demande, il renvoie les parties à se pourvoir au fond. Si toutefois le juge en reconnaît le bien fondé en partie ou en totalité, la décision n'a pas au fond l'autorité de la chose jugée et peut faire l'objet d'une opposition ou d'un appel selon le cas, dans un délai de 15 jours de la date de notification de l'ordonnance.

Cependant, si la décision est exécutoire à titre provisoire, un appel ne suspend pas son exécution par la partie adverse qui peut saisir à toutes fins utiles un huissier de justice sauf pour l'appelant à solliciter selon une procédure judiciaire distincte la suspension de l'exécution provisoire. Le coût de l'opposition à injonction de payer et de l'assignation en référé peut être nul pour le défendeur, s'il se présente en personne devant le juge, la représentation par un avocat n'étant pas obligatoire devant le tribunal d'instance et le tribunal de commerce.

Quelle attitude conseiller au défendeur tout au long de ce processus ?

Tout d'abord, il y a lieu de constater que le processus global est de longue durée. (2 à 3 ans). L'intérêt du demandeur (l'escroc) est de poursuivre son débiteur (AD, Prêtre …) aussi longtemps que la procédure ne coûte quasiment rien avec l'espoir de l'amener à payer par lassitude ou crainte des tribunaux ou encore l'amener à composition.

Ce type de fournisseur connaît parfaitement le droit en la matière. Il sait quelle est la limite de son action. Il engagera l'affaire aussi loin que son espoir de gain subsistera tout en tenant compte du montant de la somme en cause.

Peu lui importe que le souscripteur ne le revoie pas une seconde fois sous le même nom, pour le même type de contrat. Sa société peut prendre une autre raison sociale et lui-même user d'un autre nom d'usage.

Il ne sert à rien d'argumenter longuement du bien-fondé du non-paiement sinon à engager ainsi un échange de correspondance avec le demandeur au risque à terme de reconnaître implicitement la dette, par exemple en sollicitant des délais de paiement ou une remise sur le principal.

Il faut éviter l'échange de conversations téléphoniques avec un prétendu avocat ou même magistrat… Il faut systématiquement refuser tout entretien de ce type soit par téléphone, soit à domicile.

Les indices qui doivent vous alerter

Depuis longtemps, le Service juridique de la Conférence est consulté au sujet de difficultés et litiges résultant de contrats, conclus dans des conditions très discutables, portant sur la fourniture de biens ou services.

Exemple éclairant : dans un dossier actuel, trois paroisses et leur curé ont réglé, à fonds perdus, par chèque de banque, 60.000 € au titre d'un contrat particulièrement lésionnaire conclu avec une maison d'édition dénuée de tout scrupule.

Pour prévenir de tels gâchis, lorsque vous êtes amenés à signer un bon de commande ou un contrat il faut absolument vérifier d'une part la présence de clauses obligatoires pour la validité de l'engagement et d'autre part que certaines clauses ne pourraient pas être qualifiées d'abusives.

C'est pour cette raison que nous vous conseillons que la signature d'un contrat soit toujours précédée de l'avis autorisé de l'économat diocésain.

Pour vous aider[1]

Doivent figurer obligatoirement dans un contrat des **informations, dont certaines revêtent parfois un caractère d'ordre public, leur non-respect pouvant entraîner la nullité du contrat[2]** :

- L'identité des parties et leur signature,
- **La possibilité de se rétracter dans un délai de 14 jours**. Il s'agit là d'un délai de réflexion accordé au consommateur pour lui permettre de conclure en connaissance de cause et surtout pas dans la précipitation,
- **Le prix et les modalités de paiement.**

Ces informations doivent figurer de manière claire et compréhensible. Leur caractère commercial doit apparaître sans équivoque.

En outre, qu'il s'agisse du démarchage à domicile des personnes physiques ou de la vente de biens et de la fourniture de prestations de service à distance, **le non-respect de certaines informations obligatoires est assorti de sanctions pénales sous forme de peines d'amende**, voire d'emprisonnement.

Doivent aussi vous alerter la présence de clauses qui ont pour effet de créer à votre détriment un déséquilibre significatif en ce qui concerne les droits et obligations du contrat, **ces clauses sont dites abusives[3].**

LES BONS REFLEXES

Prendre le temps de choisir

Une règle d'or doit vous guider : **ne rien signer, ne pas verser d'argent**. Ne donnez pas non plus vos coordonnées de carte ou de compte bancaire. En restant ferme sur ce point, vous éloignerez de nombreux aigrefins et éviterez tout problème de remboursement.

Exiger et lire la documentation obligatoire

Lire attentivement tous les documents qui vous parviennent pour éviter de remplir, signer et renvoyer un document sans savoir quel est son objet précis.

Se méfier notamment des adresses d'entreprises situées à l'étranger, des boites postales et des enveloppes pré imprimées pour la réponse.

En cas de renvoi de ce document par erreur ou faute d'attention, ne pas se laisser intimider et réagir.

Une attitude défensive est vivement conseillée. Il faut laisser le fournisseur dérouler son processus, y compris dans le démarrage éventuel de la phase judiciaire. Dans la plupart des cas, le fournisseur abandonnera l'action assez rapidement avant la phase judiciaire proprement dite. Si cette étape est franchie, il peut encore stopper le processus avant qu'il lui en coûte.

Saisir la direction départementale de la protection des populations ou la direction départementale de la cohésion sociale et de la protection des populations (DDCSPP) de votre département de résidence,

---

[1] Pour de plus amples informations, se référer au vademecum sur les contrats.

[2] Voir Code de la Consommation, articles L121-17 et suivants.

[3] Voir Code de la Consommation, article L212-1

d'une plainte, soit sur la base de la publicité mensongère (si l'entreprise est située en France), soit dans le cadre de la coopération administrative internationale (si l'entreprise est domiciliée à l'étranger).

Alerter le diocèse ou/et la CEF de ces escroqueries pour l'inviter ou les inviter à adresser des messages d'alerte aux autres diocèses.

Plusieurs actions sont à entreprendre :

Action amiable

- Dans un premier temps, vous pouvez tenter de trouver un arrangement à l'amiable avec le professionnel de manière à ce que celui-ci cesse ses poursuites au titre d'une prétendue créance.
- En cas d'échec, il est nécessaire de rédiger une lettre circonstanciée, expliquant clairement pourquoi on ne reconnaît pas la dette, quelle est la clause abusive, les manquements au contrat ou la non-conformité de la prestation. Envoyer ce courrier en recommandé avec avis de réception, pour prendre date.
- La copie de cette lettre pourra être envoyée aux différents interlocuteurs qui apparaîtront au cours du processus sans autre explication que le mot d'envoi.
- Si à la suite de cette lettre, vous n'obtenez pas satisfaction, vous pouvez, dans un second temps, faire intervenir le Service juridique de la Conférence des évêques de France qui tentera d'obtenir gain de cause en se fondant sur des arguments juridiques.
- Parallèlement, vous pouvez envoyer votre témoignage à la Direction Départementale de la Protection des Populations (DDPP), de préférence par lettre recommandée. Après un certain nombre de témoignages concernant ce prestataire, une enquête sera ouverte et si les éléments sont probants, la DDPP saisira le Procureur de la République afin que le prestataire soit condamné au versement d'une amende.

L'action judiciaire

C'est seulement au moment où l'on rentrera dans la phase judiciaire proprement dite qu'un dossier de plaidoirie bien argumenté deviendra nécessaire. Le dossier sera alors confié à un avocat qui prendra en charge la suite du dossier et sera à même de vous demander tous les éléments que vous pourrez lui communiquer pour lui permettre de préparer au mieux son dossier de plaidoirie.

A ce stade, préalablement à toute action au fond, devront être examinées les règles de compétence concernant la personne du prêtre, le tribunal, le lieu.

Au pire, le juge peut reconnaître la validité du contrat mais aussi modérer la clause pénale encourue, si elle est manifestement excessive par rapport à l'engagement souscrit.

Dans la plupart des cas, il prononce la nullité de la clause ce qui peut selon le cas entraîner celle du contrat tout entier.

Ann-Sophie de Jotemps ann-sophie.dejotemps@cef.fr

Anne-Violaine Hardel anne-violaine.hardel@cef.fr

Marie-Laure Bénech marie-laure.benech@cef.fr

*_*_*
_

SOMMAIRE

I – LISTE NON EXHAUSTIVE DES ARNAQUES

FICHE N° 1 : ARNAQUE SMS – ARNAQUE SUR SMARTPHONE

Cadre de l'arnaque

La direction générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF) appelle les consommateurs à la vigilance vis à vis des arnaques par internet et par SMS. Messages aux termes desquels il sera demandé invariablement l'envoi de fonds par virement bancaire ou par prélèvement direct sur votre compte via la facture de votre fournisseur en téléphonie mobile.

- Un SMS frauduleux peut inviter son destinataire à rappeler un numéro de téléphone fortement surtaxé commençant par 0899 en lui promettant des bénéfices mensongers, ou en lui demandant la confirmation d'un débit bancaire ….

- Plus grave il peut s'agir d'aider un ami, un des contacts de la boite mail, l'adresse mail ayant été piratée. Ici le statut social de la personne qui demande de l'aide accroit la prétendue crédibilité des aigrefins.

Exemples

Exemple de SMS

« C'est Bernard, rappelle moi au 0899 ; ...» ; « Vous avez gagné xxx euros, rappelez le 0899...» ; «Vous avez reçu un colis. Contactez le 0899...» ; « J'ai vu votre annonce sur ABC et je suis très intéressée par votre table. Merci de me rappeler au 0899...» ; ou même, pire encore : *«votre colis est arrivé au point relais, merci d'appeler le numéro 06...»* (Numéro sur lequel une messagerie vous demande d'appeler un numéro surtaxé du type 0899...).

Intrigués et tentés, en rappelant, votre facture de téléphone grimpe considérablement. Il est trop tard et vous comprenez alors que vous avez composé, à votre insu, un numéro surtaxé ou bien, lorsque vous avez composé un numéro banal 06.., que l'on vous a dirigé vers un numéro surtaxé.

Exemple de mail

Voici un exemple de message d'arnaque qui peut vous parvenir avec une adresse piratée (un des contacts de votre boîte mail par exemple)

"*Bonsoir,*

J'espère que tu vas bien, où es-tu présentement ? J'espère aussi que je ne te dérange pas ? Mais j'ai sérieusement besoin de ton aide. Contacte-moi par mail en toute discrétion, je suis en déplacement en Afrique pour des raisons personnelles et je suis dans une situation indicible.

C'est vraiment délicat. J'ai besoin de ton assistance financière, juste un prêt que je te rembourserais dès mon retour de voyage.

Je reste dans l'attente urgente de te lire. Cordialement "

Comment éviter de se laisser prendre ? Que faire ?

Il faut rester vigilent, s'interroger surtout lorsque l'on ne reconnait pas le numéro de téléphone ou l'adresse mail sur l'opportunité d'ouvrir le message. Vous pouvez également vérifier sur internet en tapant le numéro tout simplement avant de la rappeler pour savoir s'il apparait comme malveillant. Dans la majorité des cas, les numéros sont déjà dénoncés sur internet.

En tout état de cause, ne jamais répondre à ces mails ou ces SMS car c'est en répondant que votre messagerie est piratée. Si vous recevez ce type de message, supprimez-le tout de suite !

Si vous avez déjà rappelé l'escroc, vous pouvez vous tourner vers le service "Info escroquerie" au 0811 02 02 17**. Surtout ne versez pas d'argent.**

Quels moyens ?

Connaître le tarif d'une communication avec un numéro à tarification surtaxée en consultant le site gratuit : http://www.infosva.org/

Utiliser le numéro 33700, dispositif de signalement des SMS ou appels aux autorités nationales que les consommateurs jugent suspects mis en place par la Fédération française des télécoms Pour cela il suffit d'envoyer un SMS au 33 700 avec le texte "Spam vocal" suivi du numéro de l'arnaque.

Vous trouverez toutes les réponses adaptées

- lorsque vous avez reçu un message SMS indésirable (SPAM SMS)
- lorsque vous avez reçu un appel indésirable (SPAM vocal)

Chercher des informations sur le site de l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes) à destination des consommateurs de Télécoms en consultant la fiche «SMS indésirables et appels frauduleux» à l'adresse : http://www.telecom-infoconso.fr/sms-indesirables-et-appels-frauduleux/

S'inscrire gratuitement sur la liste d'opposition au démarchage téléphonique récemment mise en place le 1er juin 2016 «Bloctel» à l'adresse suivante :
«https://conso.bloctel.fr/».

Ainsi, vous ne recevrez plus de sollicitations par un professionnel avec lequel vous n'avez pas de relation contractuelle en cours, conformément à la loi n° 2014-344 du 17 mars 2014 relative à la consommation.

Cette loi précise qu'il est interdit à tout professionnel, directement ou par l'intermédiaire d'un tiers agissant pour son compte, de démarcher téléphoniquement un consommateur inscrit sur cette liste, sauf pour quelques cas très particuliers. De plus, si un numéro persiste à vous contacter, il vous sera possible par l'intermédiaire du site «Bloctel» de le signaler à la DGCCRF afin que cette dernière enquête.

Les sommes en jeu sont souvent trop faibles pour se lancer dans une procédure pénale. Le meilleur conseil reste encore la prudence et la vigilance.

FICHE N° 2 : ARNAQUE AU PHISHING

Cadre de l'arnaque

Le *phishing* (ou hameçonnage en bon français) consiste pour un escroc à obtenir des informations confidentielles (numéro de comptes bancaires, de cartes bleues, etc.) simplement en vous les demandant.

Depuis plusieurs années on peut noter une augmentation des escroqueries par divulgation des coordonnées bancaires pour rejet d'une facture.

Les techniques utilisées sont les suivantes :

- La boite mail a été piratée et les escrocs ont pu remarquer un nouvel abonnement, une commande d'un produit … .Ils adressent alors un mail dont l'intitulé reprend, fictivement les références du nouveau fournisseur, qui annonce que le paiement a été rejeté et qu'il faut redonner, par un lien internet, ses coordonnées bancaires.
- il peut, par exemple faire croire à la victime, grâce à la contrefaçon d'un site officiel, qu'elle s'adresse à un tiers de confiance — banque, administration, etc. ... — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.
- ces escroqueries peuvent également se produire par téléphone. En effet, les escrocs n'hésitent pas à utiliser d'autres moyens pour récupérer des données bancaires.-Particulièrement visée par les tentatives de *phising*, EDF, les centres des finances publiques, mais également Carrefour Banque et bien d'autres sociétés tentent d'alerter leurs clients sur ce type d'arnaque.

Exemple dans le cadre d'une paroisse :

Voici un exemple de mail reçu par des économes diocésains et des paroisses. Le courriel pourrait provenir de votre banque, d'EDF, du Centre des Impôts …

« Chers Membres PayPal,
Par mesure de sécurité, nous contrôlons régulièrement les activités PayPal.
Nous avons récemment remarqué un problème sur votre compte.
Nous avons déterminé que quelqu'un a peut-être tenté d'accéder à votre compte PayPal sans votre autorisation.
Pour votre protection, nous avons restreint l'accès à votre compte.
Nous avons temporairement restreint l'accès à votre compte.
Nous réétudierons cette restriction lorsque vous aurez fourni les informations demandées.
Cliquez Ici Pour activer votre compte
Nous vous remercions de votre coopération dans le cadre de ce dossier.

Cordialement, PayPal »

Comment éviter de se laisser prendre ?

Très souvent ces messages ont l'apparence de messages provenant de l'organisme en références, on s'y laisse prendre tant les couleurs, la copie des logos correspondent visuellement au code de la société. Reprise des logos et des lettres qui peuvent être adressées par les banques, l'EDF….

Mais en y regardant d'un peu plus près on peut souvent déceler des fautes d'orthographes plus ou moins grossières, des tournures de phrases incorrectes… cependant les arnaqueurs progressent également dans ces domaines rendant plus difficile la mise à jour de ces escroqueries.

Le bon sens doit simplement prévaloir puisque aucun organisme officiels sérieux n'a besoin que vous leur donniez vos coordonnées bancaires pour prélever une facture… puisqu'ils ont DEJA vos coordonnées.

Que faire ?

Quel que soit le contenu du courriel, il ne faut jamais communiquer de coordonnées bancaires avant d'avoir vérifié l'identité de l'interlocuteur et le bien-fondé de sa demande.

Il faut surtout ne jamais répondre à ces mails ou ces SMS car c'est également en répondant que votre messagerie est piratée.

Si vous recevez ce type de message, supprimez-le tout de suite !

Lors d'un appel téléphonique, il vaut mieux mettre fin à la conversation et appeler soi-même le service client concerné

Autre astuce : sauf exception, il n'est pas possible de créditer un compte avec une carte bancaire. Si on vous demande de transmettre ses références (numéro, date d'expiration, cryptogramme) pour « créditer de l'argent sur votre compte », cela doit vous mettre la puce à l'oreille. En cas de doute appeler le service client de l'organisme concerné, non pas en utilisant le numéro donné dans le message, mais en consultant votre propre répertoire.

Si vous le pouvez signalez ces messages aux autorités nationales Il suffit d'envoyer un SMS au 33 700 avec le texte "Spam vocal" suivi du numéro de l'arnaque. Si vous avez déjà rappelé l'escroc, vous pouvez vous tourner vers le service "Info escroquerie" au 0811 02 02 17. Surtout ne versez pas d'argent.

Si vous êtes victime d'un phishing, vous pouvez effectuer une alerte sur :

www.internet-signalement.gouv.fr

www.phishing-initiative.com (alimente les principaux navigateurs afin que l'accès à ces sites soit bloqué) et porter plainte pour tentative d'escroquerie (art 313.3 du code pénal et/ou usurpation d'identité (art 226-4-1 du code pénal).

FICHE N° 3 : ARNAQUE SUR LE SITE BANCAIRE

Bien choisir ses mots de passe et les garder pour soi

Pour choisir un mot de passe efficace, évitez les chiffres évidents comme votre date de naissance par exemple ou les codes secrets utilisés sur d'autres services. Il ne doit pas être définitif et être changé régulièrement (pensez à le faire plusieurs fois par an).

IMPORTANT : Sachez que les établissements bancaires ne vous demanderont **JAMAIS vos codes d'accès que ce soit par email, par courrier ou par téléphone,** ils sont personnels gardez-les pour vous !

Protéger son ordinateur

Afin de prévenir votre ordinateur de tous les risques liés à Internet, nous vous conseillons de prendre quelques précautions :

- Installez les mises à jour récentes de votre système d'exploitation et de votre navigateur internet pour disposer des derniers correctifs de sécurité.
- Equipez-vous d'un logiciel antivirus mis à jour régulièrement et automatiquement pour pouvoir être protégé des virus, vers ou autres chevaux de Troie, très répandus sur Internet.
- Veillez à disposer d'un Pare-feu aussi appelé " Firewall " pour empêcher les accès non autorisés de tiers à votre ordinateur et aux données qu'il contient.

Vérifier que le site est sécurisé

Il existe une technique simple pour vérifier que le site internet sur lequel vous êtes est sécurisé, c'est-à-dire si vos données sont protégées par chiffrement.

Cette sécurité est visible via le sigle " https " dans la barre de navigation. Le " S " ajouté au http habituel nous indique que nous sommes bien sur une page sécurisée, comme c'est le cas sur le site du Crédit Mutuel par exemple :

Vérifiez soigneusement l'adresse affichée par votre navigateur Internet. Seul le début d'adresse "https://www.creditmutuel.fr " vous garantit que vous vous adressez bien au site sécurisé. Avant de saisir votre identifiant et votre mot de passe, assurez-vous impérativement de la présence stricte de chacun des caractères de ce début d'adresse.

Une adresse de site frauduleux présentera une légère différence : par exemple, un caractère en moins comme dans "https://www.credimutuel.fr/ " (caractère "t" manquant).

FICHE N°4 : ARNAQUE AU MESSAGE PERSONNALISE SUR INTERNET

La direction générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF) appelle les consommateurs à la vigilance vis à vis des arnaques par internet et par SMS. Messages aux termes desquels il sera demandé invariablement l'envoi de fonds par virement bancaire ou par prélèvement direct sur votre compte via la facture de votre fournisseur en téléphonie mobile.

Le message joue 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 fait miroiter une promesse d'argent ou un remboursement.

Plus grave il peut s'agir d'aider un ami, un des contacts de la boite mail, l'adresse mail ayant été piratée. Ici le statut social de la personne qui demande de l'aide accroit la prétendue crédibilité des aigrefins.

Deux exemples

« Bonsoir,

J'espère que tu vas bien, où es-tu présentement ? J'espère aussi que je ne te dérange pas ? Mais j'ai sérieusement besoin de ton aide. Contacte-moi par mail en toute discrétion, je suis en déplacement en Afrique pour des raisons personnelles et je suis dans une situation indicible.

C'est vraiment délicat, j'ai besoin de ton assistance financière, juste un prêt que je te rembourserais dès mon retour de voyage.

Je reste dans l'attente urgente de te lire

Cordialement »

Ou

Abbé Alexandre de Bucy
BP. 178 San - Mali
E-mail : alexandredebucy@yahoo.fr
Cher Olivier ,
J'espère que tu vas bien,
ici tout va pour le mieux, malgré mes diverses charges pastorales, toujours entre deux villages pour des célebrations ou des formations IL y avait ici une réligieuse médecin,
non loin de notre maison qui a été affectée il ya 9 mois au Cameroun qui m'a laissé avec un dépot de 3100 euros que j'ai reversé sur mon compte en France ,
lle me demande à présent de lui transferer ce dépot destiné à la couverture médicale des pensionnaires de son orphelinat là-
bas ,et signale l'urgence de ce transfert à cette fin .Je suis prèt maintenant si j'ai tes réfere nces de compte de te faire un virement de cette somme à partir de mon compte sur ton c ompte , et de te faire tenir les justificatfs de ce virement ,
à charge pour toi ,dès lors de lui avancer cette somme ,moins les frais d'envoi par un guic het de Western Union que tu trouveras là-bas dans ton bureau de Poste ,
par son adresse que je te communiquerai , par ce canal , l'avantage est que
l'opération prend moins de 10mn au guichet ,et la soeur recevra le meme jour ses fonds .Fra ternnellement
Alexandre

Comment éviter de se laisser prendre ? Que faire ?

Il faut rester vigilent, s'interroger surtout lorsque l'on ne reconnait pas le numéro de téléphone ou l'adresse mail sur l'opportunité d'ouvrir le message. Vous pouvez également vérifier sur internet en tapant le numéro tout simplement avant de la rappeler pour savoir s'il apparait comme malveillant. Dans la majorité des cas, les numéros sont déjà dénoncés sur internet.

En tout état de cause, ne jamais répondre à ces mails ou ces SMS car c'est en répondant que votre messagerie est piratée. Si vous recevez ce type de message, supprimez-le tout de suite !

Si vous avez déjà rappelé l'escroc, vous pouvez vous tourner vers le service "Info escroquerie" au 0811 02 02 17**. Surtout ne versez pas d'argent.**

Quels moyens ?

Connaître le tarif d'une communication avec un numéro à tarification surtaxée en consultant le site gratuit : http://www.infosva.org/

Utiliser le numéro 33700, dispositif de signalement des SMS ou appels aux autorités nationales que les consommateurs jugent suspects mis en place par la Fédération française des télécoms Pour cela il suffit d'envoyer un SMS au 33 700 avec le texte "Spam vocal" suivi du numéro de l'arnaque.

Vous trouverez toutes les réponses adaptées

- lorsque vous avez reçu un message SMS indésirable (SPAM SMS)
- lorsque vous avez reçu un appel indésirable (SPAM vocal)

Chercher des informations sur le site de l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes) à destination des consommateurs de Télécoms en consultant la fiche «SMS indésirables et appels frauduleux» à l'adresse : http://www.telecom-infoconso.fr/sms-indesirables-et-appels-frauduleux/

S'inscrire gratuitement sur la liste d'opposition au démarchage téléphonique récemment mise en place le 1er juin 2016 «Bloctel» à l'adresse suivante :
-«https://conso.bloctel.fr/».

Ainsi, vous ne recevrez plus de sollicitations par un professionnel avec lequel vous n'avez pas de relation contractuelle en cours, conformément à la loi n° 2014-344 du 17 mars 2014 relative à la consommation.

Cette loi précise qu'il est interdit à tout professionnel, directement ou par l'intermédiaire d'un tiers agissant pour son compte, de démarcher téléphoniquement un consommateur inscrit sur cette liste, sauf pour quelques cas très particuliers. De plus, si un numéro persiste à vous contacter, il vous sera possible par l'intermédiaire du site «Bloctel» de le signaler à la DGCCRF afin que cette dernière enquête

Les sommes en jeu sont souvent trop faibles pour se lancer dans une procédure pénale. Le meilleur conseil reste encore la prudence et la vigilance.

FICHE N° 5 : ARNAQUE A L'HERITAGE OU A LA PROMESSE DE LEGS

Cadre de l'arnaque

Au sein de l'Eglise, l'arnaque à l'héritage est une tentative d'escroquerie à la fois très ancienne et très commune encore aujourd'hui. Les escrocs vous adressent un mail vous informant que vous avez été choisi pour toucher un fabuleux héritage providentiel.

En analysant dans le détail une arnaque à l'héritage, on découvre que le mode opératoire est le suivant :

Vous recevez un mail ou une lettre généralement très longue et très polie d'un ou d'une inconnu(e) indiquant notamment posséder une forte somme d'argent. Mais cette personne se trouve malheureusement dans une situation critique qui l'empêche d'en profiter. Et bien sûr, elle n'a aucune famille à qui faire en faire profiter. Voilà pourquoi elle s'adresse à vous.

Cette personne vous invite alors à l'aider à débloquer cet argent contre une commission représentant un pourcentage de la somme (de 10 à 25%!)

Si vous répondez que vous êtes d'accord, elle vous indique qu'il y a soit des frais préalables à verser (frais de dossier, de notaire, d'avocats etc.), soit qu'il faut donner votre autorisation pour un prélèvement depuis votre compte juste pour vérifier la faisabilité de la transaction de la commission en question. On pourrait penser qu'il s'agit d'une petite somme au regard des millions qui vont arriver ensuite, mais le problème est que c'est vous qui faites le premier mouvement d'argent.

Exemples

« Bien Le Bonjour, je suis désolée de vous contacter ci-brusquement je tiens à vous informer que c'est la grâce de Dieu qui m'a dirigé vers vous et je le remercie. J'aimerais vous faire une Proposition qui pourra vous intéressez; Il s'agit d'un Don d'une forte somme .Pour avoir plus de renseignement concernant mon don je vous prie de lire ma lettre en fiche joint
Ceci n'étant pas un spam ni un pub mensongère. Aujourd'hui, je suis sous-observation médicale pour le mal dont je souffre depuis plus de deux ans.
J'ai actuellement un chiffre d'affaire de 3240000E, que je voudrai vous remettre pour les œuvres caritative de bon cœur pour la suite.
Je vous prie de me contacter sur mon mail privé suivant pour la suite :
CONTACT Mail!:philippe. ----------@GMAIL.COM / Pour avoir plus de renseignement concernant mon don je vous prie de la lettre en fiche joint.
Recevez mes salutations les plus sincères pour cette année, bonheur, réussite, pour vous, et toute votre famille. »

Ou il y a quelques années « DONATION DU FEU CARDINAL GANTIN » Arnaque qui pourrait parfaitement être réactualisée.

« Je suis Mr PATRICK.DORLEAN en collaboration avec le pape BENOIT XVI et suite aux consignes laissées par le FEU Cardinal GANTIN, dans son testament je cite :<>. Si vous recevez ce courriel c'est que vous êtes le bénéficiaire de ce don que vous soyez chrétien ou non n'a pas d'importance nous sommes tous les même devant Dieu. Avec l'accord du pape BENOIT XVI les vœux de mon feu frère seront respectés. Pour rentrer dans vos droits de bénéficiaire nous vous prions de remplir les informations si dessous.

1. *NOM ET PRÉNOM……..*
2. *PAYS……*
3. *ADRESSE*
   OCCUPATION……

4. CONTACT TÉLÉPHONIQUE……

Nous vous prions de bien vouloir envoyer ces informations à l'avocat chargé de la remise de la donation après les avoir remplir. Voici les contacts de l'avocat. Cabinet Maître Da Silva

LOT 107 JOINKET COTONOU BENIN RÉPUBLIQUE

Émail notariale.cabinet@yahoo.com

Je vous prie de le contacter au plus vite car je vais en Italie et je ne pourrai vous répondre sitôt. Faites bon usage de votre bien.

Bien à Vous »

Que faire ?

Si vous versez ces frais préalables, votre contact ne donnera plus jamais de nouvelles.

Si vous donnez vos informations bancaires, une transaction d'argent se fera de votre compte vers celui des escrocs (et non l'inverse) et votre contact ne donnera plus jamais de nouvelles.

Des précautions simples permettent d'éviter ce genre de litiges. Le premier conseil lorsque vous recevez ces mails étranges est déjà de :

- Ne pas répondre et de procéder à leur destruction immédiate.
- Ne **JAMAIS** envoyer d'argent à un inconnu via un service de transfert d'argent ou par virement bancaire. Vous aurez, sinon, la surprise d'être sollicité pour d'autres affaires « intéressantes ».
- Ne pas ouvrir la (ou les) pièce jointe pouvant contenir des logiciels espions.
- Détruire immédiatement ces e-mails.
- Signaler l'arnaque sur le site officiel mis à la disposition des internautes par le gouvernement français : www.internet-signalement.gouv.

FICHE N° 6 : ARNAQUE A LA NIGERIANE OU FRAUDE 419

Cadre de l'arnaque

« Arnaque nigériane » est un synonyme de « Fraude 419 ». Le nom formel pour ces fraudes est « Fraude 419 » (419 étant la référence de la section du code pénal du gouvernement nigérian traitant de ce type d'arnaques).

Les « Arnaques nigérianes » sont matérialisées par des « spams » ou des échanges sur les réseaux sociaux et les sites de rencontres, ou tout autre moyen d'entrer en contact avec une future victime. Tout cela relève de techniques de manipulations psychologiques mettant en œuvre de l'Ingénierie sociale (l'art du tirer les vers du nez afin de nuire, arnaquer, convaincre, etc. ...).

Les « Arnaques nigérianes » sont massivement utilisées par l'Afrique noire (Nigeria et autres pays, avec extension vers les « diasporas noires » dans le monde) visant à faire croire à une victime qu'elle va recevoir une grosse part d'une énorme cagnotte, si cette personne aide à transférer (à sortir de son pays d'origine) cette cagnotte (compte bancaire, argent liquide, coffre plein de lingots d'or ou de sacs de diamants, titres de sociétés, etc. ...).

Le point de départ de la cagnotte est toujours un pays connaissant des troubles, ce qui permet d'ajouter un aspect romanesque, et généralement tragique, à l'histoire qui va être racontée à la victime pour l'appâter.

Pays d'origine de l'arnaque

Ces « **Arnaques nigérianes** » arrivent de partout :

- Les pays d'origine sont tous les pays d'Afrique de l'Ouest (zone CEDEAO à savoir Bénin, Burkina Faso, Cape Vert, Côte d'Ivoire, Gambie, Ghana, Guinée, Guinée Bissau, Libéria, Mali, Niger, Nigeria, Sénégal, Sierra Leone et Togo) auxquels il faut ajouter Irak, Iran, Afrique du Sud, République Centrafricaine, Éthiopie, Congo, etc. ...).
- D'autres pays, non africains, sont lourdement impliqués. Avec les « **diasporas noires** », ces **arnaqueurs**, **criminels** et **cybercriminels**, appelés « brouteurs », se retrouvent dans tous les pays du monde et c'est hors d'Afrique qu'ils sont les plus virulents.
- L'Asie et les pays de l'Est, dans leurs populations non noires, sont également des pépinières d'**arnaqueurs** aux « **Arnaques nigérianes** ».
- Dans une faible proportion, des ressortissants occidentaux de pays démocratiques pratiquent également cette forme d'**escroqueries**.

Comment fonctionne l'escroquerie ? Cette fraude prend des formes multiples. Le plus souvent, l'arnaque démarre sur Internet par un mail avec la mention "urgent", "confidentiel" ou "sérieux". Il peut par exemple émaner d'un médecin, d'un avocat, d'un grand patron ou bien encore d'un officiel de gouvernement étranger. Des personnes censées mettre en confiance l'internaute. L'expéditeur du courriel va vous demander de l'aide pour sortir une importante somme d'argent de son pays (un héritage, des pots-de-vin, ou tout simplement de l'argent qui dort sur un compte) en échange d'une commission sur cette somme (en moyenne 10% selon le ministère de l'Intérieur). Si le destinataire accepte, il s'engage à donner son numéro de compte afin que l'argent y soit versé. L'escroc demande en parallèle au destinataire de faire l'avance d'un montant destiné à couvrir des frais.

Bien entendu, la somme ne parviendra jamais sur le compte du destinataire, qui ne sera jamais remboursé de l'avance pour frais fictifs.

Cibles de l’arnaqueur

Cette escroquerie, qui existait déjà sous la forme de livraison postale avant le développement sur Internet, utilisent plusieurs sources pour choisir ses cibles : les sites de rencontres, de petites annonces, de loteries ou bien encore d'offres d'emplois. En raison de la démocratisation d'Internet à travers le monde, presqu’aucun pays n’échappe à ce phénomène.

Que faire ?

Des précautions simples peuvent être prises. Le premier conseil lorsque vous recevez ces mails étranges est déjà de ne pas répondre et de procéder à sa destruction immédiate. De façon générale, mieux vaut se fier à des sites Internet de confiance, signalés par un logo identifiable et dont l'adresse commence par "https". De bons logiciels anti-virus, pare-feu et anti-espion permettent également de limiter la propagation de courriers frauduleux.

En cas d'arnaque avérée, il faut déposer plainte au commissariat ou à la gendarmerie la plus proche. Comme le rappelle le Ministère de l'Intérieur, munissez-vous de références des transferts d'argent effectués, de détails sur les contacts (messagerie, pseudos utilisés) ainsi que tout autre renseignement pouvant aider à l'identification de l'escroc.

FICHE N° 7 : INSERTIONS DANS DES ANNUAIRES

Cadre de l'arnaque

Depuis plusieurs années, ces sociétés, souvent situées à l'étranger, proposent aux professionnels, associations ou collectivités l'insertion de leurs coordonnées dans des annuaires. La présentation ambiguë de certaines sollicitations peut laisser croire qu'il s'agit d'une simple d'adresse alors qu'il s'agit, en fait, vérification d'une commande ferme pour figurer dans un annuaire. L'engagement est généralement peu visible sur le document et le prix demandé d'autant plus élevé que le « contrat » est renouvelable automatiquement.

Des sociétés de recouvrement se chargent ensuite de harceler les professionnels pour qu'ils effectuent les versements demandés. Certains démarcheurs sollicitent aussi les professionnels sur leur lieu de travail et, après avoir obtenu leur signature, ne remettent ni double, ni leurs coordonnées.

Exemples

« Une de nos sœurs s'est fait arnaquer par une société dénommée "
Annuaire.Fr" ; elle a signé un contrat pensant qu'il s'agissait des Pages Jaunes. Depuis nous recevons continuellement des courriers de relance avec des menaces de poursuites judiciaires, car nous n'avons jamais voulu payer. Il semble que des centaines de personnes se soient fait arnaquer de la même façon »

«La société PBS établie 360 avenue de la Libération à 84250 LE THOR et qui a pour gérant un certain Robert vous propose de lui retourner un fax à un numéro surtaxé commençant par 0826, sous le nom commercial de "PAGES TELECOM".
Ce nom commercial est choisi de façon à faire croire que la démarche émane de "France TELECOM" dont les "PAGES JAUNES" ou "PAGES BLANCHES" sont bien connues du grand public.
En outre le fax de cette société fonctionne mal et il faut éventuellement vous y reprendre à plusieurs fois pour réussir à le passer...
En retournant ce fax, outre ce que vous perdez définitivement en utilisant le numéro surtaxé, vous vous engagez à payer 970 € H.T. par mois à cette société soit 11 640 € l'année moins 970 € offerts (!!!) la première année. »

Que faire ?

La Direction générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF) indique que la signature d'un tel document constitue un acte contractuel de droit privé dont la validité peut être contestée devant les tribunaux civils, sur la base, par exemple, d'un consentement donné par erreur. La présentation de certains imprimés pourrait également s'analyser comme une publicité de nature à induire en erreur, mais les suites judiciaires pénales contre des entreprises domiciliées à l'étranger sont longues et délicates à mettre en œuvre.

Vous pouvez trouver ces indications sur site de la DGCCRF aux adresses suivantes : http://www.economie.gouv.fr/dgccrf/annuaires-professionnels-attention-aux-arnaques et http://www.economie.gouv.fr/dgccrf/annuaires-professionnels.

Ainsi,

Il est recommandé :

- de faire un signalement auprès de la DGCCRF,
- de refuser tout entretien téléphonique et de ne pas répondre à leur relance,
- éventuellement de rédiger un courrier circonstancié expliquant clairement pourquoi on ne reconnaît pas la dette, quelle est la clause abusive, les manquements au contrat ou la non-conformité de la prestation. (cf. préambule) Envoyer ce courrier en recommandé avec avis de réception, pour prendre date,
- de garder une trace de toutes les pièces du dossier.

Toutefois, à réception d'un courrier recommandé avec accusé de réception de leur part contenant une mise en demeure, nous vous conseillons de contacter le service juridique de la CEF pour nous permettre d'étudier la question et envisager la possibilité de porter plainte.

FICHE N° 8 : ARNAQUE DANS L'ENREGISTREMENT DE MARQUES

Cadre de l'arnaque

Ces pratiques font appel à des techniques bien rodées : une société opérant depuis l'étranger adresse à des entreprises françaises des contrats de publication de leurs marques[4] ou de leurs logos[5] qui se présentent sous forme de factures ou d'ordres de virement.

Le document qui tient sur une page comprend l'adresse de l'entreprise et la reproduction de la marque sur une première moitié de la page et un ordre de virement sur la seconde moitié. Or le service qui est proposé est tout à fait inutile puisque sont démarchées des entreprises qui ont déjà fait le dépôt de leur marque auprès de l'Institut national de la Propriété Industrielle (INPI)

Peuvent aussi être démarchées des paroisses ou des diocèses pour leur logo.

C'est pourquoi, nous conseillons de faire enregistrer les logos, marques auprès de l'INPI. Cet enregistrement a un cout mais permet d'interdire ou de faire cesser plus facilement les utilisations frauduleuses éventuelles de votre marque.

Exemples

Les titulaires de logos, marques, de brevets et de dessins reçoivent des courriers de sociétés privées étrangères (voir liste ci-après) qui leur proposent de publier, d'enregistrer ou d'inscrire leurs titres au niveau européen ou international, moyennant des sommes importantes.

Ces courriers reproduisent la publication du titre au bulletin officiel de la propriété industrielle (photocopie) ou reprennent les informations qui y sont publiées (numéro et date de dépôt et ou d'enregistrement, références aux classifications internationales…)

Voici quelques noms de sociétés concernées par ces envois frauduleux :

Trademark Publisher GMBH: BP 73 A-1190 Wien (Autriche)

Globus Edition S.L: Production and shipping Department Rauchgasse 41 top 1 vienna

Edition The Marks KFT: 9737 BUK ipcar utca 10 – HU (Hongrie)

ZDR-Datenregister GMBH : PO BOX 102422 60024 Frankfurt/M Allemagne

[4] La **marque** est un signe distinctif qui permet au consommateur de distinguer le produit ou service d'une entreprise de ceux proposés par les entreprises concurrentes. La **marque** peut être matérialisée par un nom propre, un mot, une expression ou un symbole visuel.

[5] Un **logo** ou logotype est une représentation graphique d'une marque ou d'une entreprise qui est utilisé sur les différents supports de communication. Le **logo** renforce l'image de l'entreprise. Il peut également favoriser la reconnaissance de la marque comme dans le cas par exemple des articles de sport.

Que faire ?

Attention l'INPI n'a aucun lien avec ces sociétés

La direction générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF) indique que la signature d'un tel document constitue un acte contractuel de droit privé dont la validité peut être contestée devant les tribunaux civils, sur la base, par exemple, d'un consentement donné par erreur. La présentation de certains imprimés pourrait également s'analyser comme une publicité de nature à induire en erreur, mais les suites judiciaires pénales contre des entreprises domiciliées à l'étranger sont longues et délicates à mettre en œuvre.

Ces informations sont disponibles sur le site de la DGCCRF, à l'adresse suivante : http://www.economie.gouv.fr/dgccrf/litiges-avec-professionnel-a-letranger

IPTS Marques

54879654522/IPTS/16515

IPTS Service sp.z.o.o., ul.Dluga 23/25 lok. 21, 00-238 Warszawa
Serge-Henri Saint-Michel
[redacted]
FR-[redacted]
Francja / France

ENREGISTREMENT NUMER: 3839317
DATE ENREGISTREMENT: 16.06.2011
CLASSE(S) : 16 , 35 , 41

ENREGISTREMENT MARQUES

REPRODUCTION DE LA MARQUE:

INI *Xyz*

Pos.	Description	monnaie	montant
01	frais d'inscription	EUR	870,00
02	TVA	EUR	0,00
	La somme totale	**EUR**	**870,00**

modes de paiement :

PAR VIREMENT BANCAIRE:
MONTANT: 870,00
BÉNÉFICIAIRES : IPTS Service
NOM DE LA BANQUE: WBK Bank
IBAN : PL58109017110000000119337358
CODE BIC/SWIFT : WBKPPLPP
ADRESSE DE LA BANQUE : Rynek 9/11, PL 50-950 Wroclaw

BY CHEQUE :
BÉNÉFICIAIRES : IPTS Service BPM 373766
ADRESSE : RN 18 Les Maragolles
54720, Lexy

S'il vous plaît payer le montant, dans les 7 jours par virement bancaire ou par chèque !

Cher client,
s'il vous plaît noter que ce formulaire n'est pas une facture. Ceci est une offre pour l'inscription annuelle de votre marque dans notre base de données sur Internet. S'il vous plaît également noter que cette offre deviendra un contrat obligatoire avec le paiement de la somme. l'inscription sur notre base de données n'a pas de lien avec une organisation officielle du gouvernement. Il n'ya aucune obligation pour vous de payer le montant, et nous n'avons pas de relation d'affaires encore. Nous rappelons à nos conditions générales sur notre site www.ipts-register.com S'il ya des erreurs ou des modifications concernant les dates s'il vous plaît nous informer de corriger ou de mettre à jour.

IPTS international Patent and Trademark Service sp.z.o.o., ul. Dluga 23/25 lok.21, 00-238 Warszawa Poland VAT: PL5252534873

Il est recommandé :

- de faire un signalement auprès de la DGCCRF
- de refuser tout entretien téléphonique et de ne pas répondre à leur relance
- éventuellement de rédiger un courrier circonstancié expliquant clairement pourquoi on ne reconnaît pas la dette, quelle est la clause abusive, les manquements au contrat ou la non-conformité de la prestation. (cf. préambule) Envoyer ce courrier en recommandé avec avis de réception, pour prendre date.
- de garder une trace de toutes les pièces du dossier

Toutefois, à réception d'un courrier recommandé avec accusé de réception de leur part contenant une mise en demeure, nous vous conseillons de contacter le service juridique de la CEF pour nous permettre d'étudier la question et envisager la possibilité de porter plainte.

FICHE N° 9 : ARNAQUE AU SCAREWARE

Cadre de l'arnaque

Un *scareware* est un logiciel malveillant qui trompe les utilisateurs pour les amener à visiter des sites Web infestés de programmes malveillants. Également connus sous les noms de rogues ou logiciels de sécurité non autorisés, les *scarewares* peuvent prendre la forme de fenêtres contextuelles.

Ces fenêtres qui ressemblent à des avertissements légitimes d'éditeurs de logiciels antivirus prétendent que les fichiers de votre ordinateur ont été infectés ou bien vous avertissent que des fichiers dangereux ou des contenus pornographiques ont été détectés sur votre ordinateur. Leur présentation est si convaincante que les utilisateurs inquiets se laissent persuader d'acheter un logiciel payant pour résoudre un problème fictif. En réalité, ils téléchargent un faux logiciel antivirus qui n'est autre qu'un programme malveillant destiné à voler les données personnelles de la victime.

Pour distribuer leurs *scarewares*, les *cyber-criminels* recourent également à d'autres techniques telles que l'envoi de courriels indésirables. Une fois le message ouvert, la victime est incitée à acheter des services totalement inutiles.

Les *scarewares* utilisent des méthodes de vente basées sur la crainte. Ils tentent de vous faire peur pour vous inciter à acheter immédiatement le produit, sans vous laisser le temps de réfléchir.

Les fournisseurs d'antivirus réputés ne recourent pas à la peur pour récupérer ce type de données. Mais les *cyber-criminels* sont bien conscients qu'un grand nombre d'utilisateurs l'ignore.

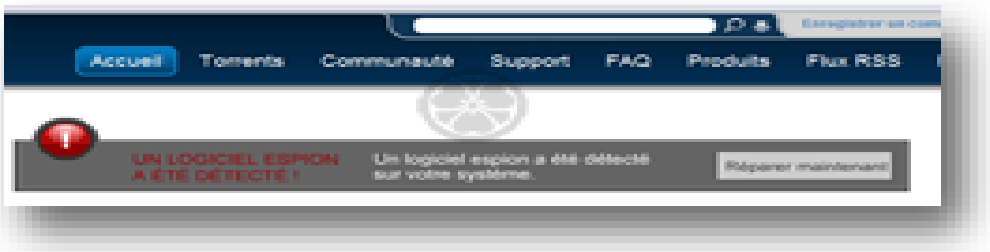
Exemples

Le principe général des *scarewares* repose sur l'instillation, dans votre esprit, d'une crainte :

- Soit par la fourniture d'informations trompeuses et affolantes. C'est le cas de tous les sites d'informations sur les processus, qui prétendent qu'un processus sur lequel vous cherchez de l'information sur le Web est un processus à risque et qu'il faut télécharger immédiatement leur logiciel pour vous en prémunir. Une fois le *scareware* installé, il va trouver des centaines de risques majeurs et dramatiques, imaginaires, etc. ... dans votre ordinateur. Lorsqu'il sera question de cliquer sur le bouton " Supprimer les risques " ou " Corriger les erreurs ", il faudra passer à la caisse.

- Soit par l'exécution gratuite d'une géniale analyse de votre ordinateur, en téléchargeant immédiatement leur scanner gratuit, primé, déjà utilisé par des millions d'internautes, depuis un site avec un logo " Microsoft Partner " qui ne veut rien dire, avec des témoignages, généralement forgés de toutes pièces (de clients satisfaits, bien sûr), etc. ... Cette version d'essai gratuite du *scareware* fera ressortir des centaines d'erreurs, de virus, de contaminations, de trucs mortels et dramatiques qu'il faut éradiquer immédiatement. Lorsqu'il sera question de cliquer sur le bouton " Supprimer les risques " ou " Corriger les erreurs ", il faudra passer à la caisse.

Des publicités comme celles-ci, sur un site, sont des faux ! C'est un mensonge et une tentative de faire peur à l'utilisateur. Le logiciel proposé au bout est un "*scareware*"



Que faire ?

- Mesures préventives

En amont, avant d'être victime de ces escroqueries, il n'y a normalement besoin d'aucun outil. Seul votre bon sens pourra vous aider à déjouer ces arnaques.

  - On ne clique pas n'importe où.
  - On décoche les cases des programmes qui tentent de s'installer en même temps que vous installez un logiciel.
  - On se méfie de tout ce qui prétend améliorer, accélérer, réorganiser, optimiser, compresser, défragmenter, nettoyer et tout autre programme au mieux inutiles, au pire dangereux, voire destructeurs.

- Mesures curatives

Lorsqu'un programme malveillant de type *scareware* est téléchargé, il est généralement impossible de le désinstaller par les voies normales. L'escroquerie s'accroche, gène le fonctionnement de votre ordinateur jusqu'à vous pousser à bout de nerfs et vous faire acheter la pseudo " version complète " du logiciel malveillant qui va enfin cesser de vous importuner. C'est assez proche d'une demande de rançon !

Il vous faudra alors utiliser la procédure de décontamination anti-malwares (programme spécifique) comme celle de *Malwarebytes Anti-Malware* (MBAM) (la version gratuite suffit).

*_*_*