



**“ATTENTION
ARNAQUE!”**

*Les bons
gestes*



BANCAIRE
RÉSEAUX FAUSSES
RUSE INDÉLICATESSE
DÉMARCHAGE ARNAQUER ORDINATEUR
VOL SOCIALS SITE TROMPERIE DANGER FRAUDE INTERNET
ATTENTION SMS
DOMICILE CARTE ARNAQUES MALHONNÉTÉTÉ TRUANDERIE
COURRIER ESCROQUERIE IDENTITÉ TRAVAUX
BANQUE COURRIEL GOUROU
BLOCTEL USURPATION
RÉNOVATION AMENDES

Qu'est ce qu'une arnaque?

Une arnaque désigne une escroquerie ou un vol , c'est à dire le fait d'obtenir quelque chose par une manoeuvre frauduleuse.

L'abus de faiblesse

L'abus de faiblesse est le fait de vendre un produit ou de faire signer un devis à une personne en profitant de son ignorance, de sa faiblesse physique ou mentale. Le vendeur a connaissance de la vulnérabilité de la personne et peut aller jusqu'à exercer des pressions répétées pour manipuler la victime de manière à obtenir son consentement

L'usurpation d'identité

L'usurpation d'identité désigne l'utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses





A domicile



Méfiez-vous des apparences

Une personne en uniforme (policiers, artisans, dépanneurs à domicile, livreurs, ...) ou un "faux voisin" se présente chez moi sans être attendue ou en prétendant avoir rendez-vous.

Le démarchage à domicile (aussi appelé porte-à-porte ou vente à domicile) est une activité commerciale légale et encadrée par la loi. Mais certains délinquants utilisent ce prétexte pour pénétrer dans votre logement afin de commettre un vol ou effectuer un repérage.

Démarchage: distinguer le "vrai" du "faux"

- Les **"vrais" démarcheurs** sont des travailleurs indépendants ou rattachés à une entreprise, qui doivent pouvoir justifier de leur identité et de leur profession. Le contrat signé doit aussi respecter plusieurs conditions (délai de rétractation, devis, conditions de paiement) pour être considéré comme valide
- Les **"faux" démarcheurs** utilisent le prétexte du porte-à-porte pour s'introduire chez vous afin d'effectuer un repérage en vue d'un cambriolage ou de voler de petits objets de valeur. Ils agissent en général par deux.

Je vérifie toujours via l'oeil de ma porte, si j'en ai un, qui se présente	Je m'équipe d'un entrebâilleur
Je ne laisse pas un inconnu pénétrer dans mon domicile	Si la personne est entrée chez moi, je ne la laisse pas sans surveillance
Face à un démarcheur, je ne signe pas le jour même. Je prends le temps de la réflexion et je fais des devis comparatifs	ATTENTION: la mairie ne recommande jamais de démarcheurs. Je ne les laisse pas entrer dans mon domicile
Je fais attention aux individus qui invoqueraient une profession officielle (policier, employé EDF, ...) . Je leur demande leur carte professionnelle et je les fais patienter en refermant la porte. je vérifie leur intervention en téléphonant à leur service ou administration	
Si je reçois une convocation ou un courrier m'annonçant un rendez-vous à mon domicile, je vérifie auprès de l'administration ou de la société concernée si cette information est vraie	En cas de doute, je ne sors pas ma carte bancaire ni mon chéquier pour régler une facture de livraison



Quand vous signez un document, vous vous engagez. Mais pas de crainte, un délai de rétractation existe alors parlez en à vos proches .



Au téléphone



Trop beau pour être vrai

Un appel téléphonique m'annonce que j'ai remporté un cadeau. Pour le récupérer, je dois délivrer à mon correspondant des informations bancaires et/ou personnelles

Le **vishing** est une forme d'arnaque qui consiste à utiliser un appel téléphonique pour tromper les gens en leur faisant croire qu'ils parlent à un conseiller bancaire ou à un autre professionnel de confiance.

Les escrocs utilisent ce moyen pour obtenir des informations personnelles comme des numéros de compte bancaire ou des mots de passe, dont ils se servent ensuite pour accéder à des comptes en ligne et voler de l'argent.

Les escrocs utilisent des techniques de manipulation pour tromper les gens, comme l'utilisation de sentiments d'urgence ou de pression pour contourner les dispositifs de sécurité.



Je m'inscris sur Bloctel pour ne pas recevoir les appels indésirables

Je contacte mon opérateur pour être sur liste rouge et éviter ainsi des appels indésirables

Je ne transmets jamais d'informations personnelles (mot de passe, numéro de compte ou de carte bancaire, numéro de sécurité sociale, adresse postale), même si vous pensez parler à un professionnel de confiance.

En cas d'appel téléphonique suspect d'une personne se faisant passer pour un proche, prétexter la rappeler ultérieurement puis vérifier la situation auprès de vos proches

Je ne réponds pas aux numéros inconnus et je ne rappelle pas des numéros qui semblent suspects.

J'appelle uniquement les numéros officiels que je connais ou en qui j'ai confiance





Ce site est-il de confiance?

Sur internet



Avoir toujours la puce à l'oreille

Je reçois un mail ou un SMS qui présente un caractère officiel ou institutionnel (gendarmerie, banque, ministère) et dans lequel on m'incite à donner mes coordonnées personnelles

Les outils numériques occupent une place croissante dans notre vie de tous les jours, que ce soit pour communiquer, s'informer, se divertir, gérer ses comptes ou encore faire ses courses.

Compte-tenu de leur utilisation massive et quotidienne, les réseaux sociaux et internet représentent désormais un des principaux vecteurs de promotion et de publicité pour des produits et services parfois frauduleux qui font de nombreuses victimes.

Les pratiques frauduleuses sont très variées et touchent les consommateurs de tous âges: arnaques au compte personnel de formation, faux ordres de virements, usurpation d'identité de professionnels, faux sites administratifs,...

<p>Je suis attentif aux expéditeurs des emails</p>	<p>Je ne clique pas sur les liens douteux d'un email, je supprime tout email suspect et je ne clique pas sur leurs pièces jointes</p>
<p>Je n'enregistre pas mon numéro de carte bancaire sur un site marchand ou sur mon ordinateur</p>	<p>Je surveille les fautes d'orthographe et de grammaire (attention, des emails frauduleux sont de plus en plus rédigés dans un parfait français)</p>
<p>Je ne transmets jamais d'informations personnelles (mot de passe, numéro de compte ou de carte bancaire, numéro de sécurité sociale, adresse postale). Aucun organisme ne sollicite ce genre d'information par mail</p>	
<p>Je me méfie du marketing trop agressif et des offres trop alléchantes</p>	<p>Je ne me précipite pas. Je prends le temps de vérifier la fiabilité du site internet et de regarder les avis des consommateurs</p>
<p>Je vérifie que le site internet est sécurisé: cadenas dans la barre URL, site "https"</p>	<p>Je choisis des mots de passe suffisamment longs, complexes, différents d'un site ou service à l'autre, et je les change souvent</p>



Je suis victime d'une arnaque, que dois-je faire?



- Si vous constatez des débits frauduleux, **déposez plainte** à la brigade de gendarmerie dont vous dépendez.
Une pré-plainte peut être déposée en ligne. La Maison France Service située à la Poste peut vous accompagner dans votre démarche
- Si vous avez cliqué sur le lien frauduleux, connectez vous le plus rapidement possible sur votre compte et changez votre mot de passe pour le site en question.
- Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement: **contactez votre banque et faites opposition immédiatement**
- La loi impose aux banques de rembourser leurs clients en cas de fraude bancaire, sauf si elles sont en mesure de prouver qu'il y a eu une négligence grave de votre part

Les numéros de téléphone utiles

Police nationale

17/ 112

Gendarmerie Pontivy

02 97 25 00 75



Centre d'accès au droit Nord Morbihan

02 97 27 39 63

Mairie de Cléguérec

02 97 38 00 15

Centre Communal d'Action Sociale

02 97 38 11 64

Maison France Service - Cléguérec

02 97 07 11 35



UFC Que Choisir

02 97 79 16 95
02 97 84 74 24



Confédération syndicale des familles

06 88 61 14 97

Opposition carte bancaire

0892 705 705

Opposition chéquier

0892 683 683

France Victimes

116 006



INFO ESCROQUERIES

Informations, conseils, assistance

Pour signaler un courriel ou un site internet d'escroqueries: www.internet-signalement.gouv.fr

0 805 805 817

Service & appel gratuits

du lundi au vendredi / 9h-18h30



Guide réalisé en partenariat avec:

