

# Comment détecter les arnaques en ligne et par téléphone ?

Toute personne possédant un ordinateur ou un téléphone peut être victime de démarchage intempestif, d'extorsion d'argent ou de piratage ; en particulier les mineurs et les seniors. Voici quelques conseils pour s'en prémunir. <sup>m</sup>



Messages électroniques et SMS

Appels téléphoniques

Informations personnelles

Être contacté par la Mairie

## Messages électroniques et SMS

Si c'est spontané, c'est suspect !

Un message :

- proposant une offre exceptionnelle ou un remboursement ;
- indiquant un problème avec un colis ;
- menaçant ou urgent : "votre compte a été piraté", "amende ou facture à payer" "vous avez été débité"...
- avec une demande inhabituelle d'un de vos contacts ;
- d'un numéro inconnu ou avec une adresse mail étrange et/ou incompréhensible ;
- avec un lien vers un site ;

doit être considéré avec la **plus grande vigilance**. Il y a de fortes chances que la tentative de contact soit du **démarchage commercial, ou une arnaque**.

Par exemple, la réception ou le paiement d'une amende ne se fait jamais par SMS. Par mail : seulement si vous avez donné vous-même votre adresse électronique lors d'une verbalisation.

**La bonne pratique : on n'utilise pas le lien reçu, et on vérifie l'information par soi-même**

**Plutôt qu'aller directement sur le lien proposé**, regardez directement sur le site où vous avez fait votre achat, ou sur celui du transporteur, avec votre numéro de commande. Ce principe s'applique également pour une facture qui serait impayée, ou un débit sur un compte bancaire.

Si le message vient de l'un de vos contacts, méfiance : il ou elle est peut-être victime d'un piratage. **Au moindre doute, appelez-le ou contactez un de ses proches.**

## Le cas particulier des conseillers bancaires

Même s'il s'agit du bon numéro, et que le conseiller semble avoir des informations correctes (numéro de compte, nom, adresse...) si il ou elle :

vous propose de souscrire directement à quelque chose par téléphone ;

vous alerte sur une tentative de fraude, d'un retrait important, etc. avec action immédiate à approuver de votre part ;

vous demande vos codes personnels ou vos identifiants bancaires ;

ne vous demande pas explicitement d'aller par vous même sur le site de votre banque et vous envoie un lien

Ne poursuivez pas la conversation. **Contactez votre agence** pour vérifier qu'il ne s'agit pas d'une tentative de fraude

## Appels téléphoniques et SMS

Il est fréquent de recevoir des appels d'opérateurs, de fournisseurs d'énergie, ou de spécialistes de l'isolation, de la sécurité, etc.

L'objectif est de vous faire contracter une offre à chaud, **sans avoir le temps d'y réfléchir posément.**

Le bon réflexe **couper court à la conversation**, ou de **ne pas répondre** aux numéros que vous ne connaissez pas : si c'est important, vous recevrez un message sur votre répondeur ou votre boîte mail.

**Attention au "spam vocal"**

Il s'agit d'un appel via un numéro inconnu qui raccroche immédiatement ou au bout de quelques secondes.

**Ne rappelez pas le numéro : il est surtaxé.**

## Informations personnelles et mot de passe

Un mail de Google ou de Microsoft vous demande de mettre à jour vos identifiants ? Un conseiller téléphonique vous propose de faire la démarche à votre place si vous lui communiquez votre mot de passe ? **C'est une tentative de piratage.**

Aucune administration, structure ou entreprise n'a le droit de vous demander vos informations personnelles de connexion, quelque soit la raison évoquée. **Ce principe n'a aucune exception**

## Etre contacté par la Mairie

### Ce qu'il faut retenir

Sans **démarche préalable de votre part** (inscription, recensement, abonnement...) la Mairie ne vous contactera pas par téléphone, SMS ou mail.

Le paiement des prestations se fait toujours depuis **votre espace personnel en ligne, ou par chèque** : auquel cas, l'ordre à indiquer n'est jamais le nom de quelqu'un.

Les agents ne vous contacteront **jamais pour obtenir des informations personnelles bancaires ou informatiques, ou de l'argent** d'une quelconque manière