

# Dispositif « Citoyens vigilants et participation citoyenne » Agir ensemble pour notre tranquillité

Fiche conseil :

## Démarchages et escroqueries



# À SAVOIR...

\* Par arrêté municipal 2024-016 en date du 06-02-2024, le démarchage et toute prospection commerciale à domicile sont interdits sur le territoire communal sauf autorisation expresse et exceptionnelle de la commune.

\* La mairie de Soisy-sur-Seine ne recommande jamais aucune entreprise ou service quelconque. Si une personne se présente comme étant recommandée par la Mairie, contactez immédiatement la Police Municipale.

## À votre domicile...

• **Les fournisseurs de services** (eau, gaz, électricité, fibre, téléphone ou autre) **ne se présentent jamais sans un avis de passage préalable**. De même, une mairie, une préfecture ou un bailleur social ne mandate jamais d'entreprise pour effectuer une enquête ou réaliser des travaux sans en aviser les personnes concernées par courrier ou affichage.



« Si je ne suis pas prévenue à l'avance, je n'ouvre pas ! »

• **N'ouvrez pas votre porte avant d'avoir vérifié l'identité de votre visiteur**, même s'il se présente comme un policier. Vérifiez toujours la qualité de votre visiteur en appelant l'organisme invoqué (police, mairie...). Utilisez les numéros de téléphone que vous avez en votre possession (figurant généralement sur les avis d'échéance et les factures) et non pas ceux donnés par la personne qui se présente.

• **Ne vous laissez pas abuser par une carte professionnelle ou un uniforme**. En cas de doute, faites patienter à l'extérieur et contactez immédiatement la Police Municipale (01 69 89 18 18).

- **Ne recevez jamais seul(e) quelqu'un que vous ne connaissez pas.** Si vous souhaitez recevoir une société, prenez rendez-vous et faites-vous accompagner. Ne laissez jamais votre visiteur seul chez vous.
- Même en cas d'urgence, **préférez faire appel à un professionnel ou un artisan connu** plutôt qu'à un démarcheur ou une entreprise référencée sur un prospectus. Faites jouer la concurrence.
- **Prenez le temps de réfléchir** et/ou faites vous conseiller avant de signer une proposition quelconque (devis...), même si elle émane d'une entreprise «connue».
- Lors de la visite d'un commercial, **ne versez jamais aucune somme d'argent et ne remettez jamais de document bancaire** (RIB, chèque postdaté, autorisation de prélèvement ou numéro de carte bancaire). La loi vous donne 14 jours pour vous rétracter ou accepter de payer le produit qui vous a été vendu.
- N'évoquez jamais les endroits où vos objets de valeur sont rangés.

## Sur Internet...

- Sur internet ou par téléphone, une banque ou un autre service (assurance, sécurité sociale...) ne vous demandera **jamais l'identifiant de connexion ou le mot de passe** de l'accès de votre compte en ligne.
  - **Protégez votre ordinateur** en installant un logiciel antivirus, un logiciel anti-espion, un pare-feu. Effectuez régulièrement les mises à jour recommandées.
  - Si vous avez **un doute sur la provenance d'un courriel**, ne l'ouvrez pas et n'ouvrez pas les pièces jointes.
  - Vous recevez un courriel qui vous dirige vers un site qui ressemble à celui de votre banque ou d'une marque que vous connaissez bien : soyez extrêmement prudent, il peut s'agir d'une manœuvre frauduleuse de «phishing». Une banque ou un autre service (assurance, sécurité sociale...) ne vous demandera jamais votre identifiant de connexion ou le mot de passe de votre compte en ligne.
- En cas de doute, appelez immédiatement votre banque.**

- Vous recevez un courriel d'une personne que vous ne connaissez pas et qui vous demande de l'aider. Il s'agit d'une manœuvre frauduleuse. **Ne répondez pas et détruisez le courriel sans ouvrir aucune pièce jointe.**
- **Réalisez vos achats uniquement sur les sites de confiance**, dont l'adresse au moment de la transaction commence par «https». L'apparition d'icônes (cadenas et clés  ) en bas du navigateur est un gage de sécurité.
- Si vous vendez un bien, **attendez d'avoir matériellement reçu l'argent** avant de livrer le bien.

## Par téléphone...

- Vous recevez un appel téléphonique vous informant d'opérations inhabituelles sur votre compte bancaire et vous demandant de rappeler un numéro. Il s'agit d'une manœuvre frauduleuse de « vishing » : **ne rappelez pas ce numéro, appelez plutôt votre établissement bancaire habituel.**
- Si vous devez effectuer un contre-appel, **utilisez les numéros de téléphone que vous avez en votre possession** (figurant généralement sur les avis d'échéance et les factures) et jamais ceux donnés par la personne qui vous appelle.
- **Ne communiquez jamais vos coordonnées bancaires par téléphone**, aucune instance bancaire ne vous demandera de procéder ainsi, même pour une simple vérification.
- En cas de démarchage par téléphone, souvenez-vous que **vous n'êtes pas engagé tant que vous n'avez pas reçu et renvoyé un contrat signé.**

Sources et informations : Enquêtes cadre de vie et sécurité 2013-2018, INSEE-ONDRP, Ministère de l'intérieur, Gendarmerie Nationale, Sirpa, Ville de Carbone... / Sites [www.data.gouv.fr](http://www.data.gouv.fr); [www.interieur.gouv.fr](http://www.interieur.gouv.fr); [www.sitesurete.maire59.fr](http://www.sitesurete.maire59.fr)...

**POLICE  
MUNICIPALE**

**01 69 89 18 18**

Lundi, mardi, jeudi, vendredi

**GENDARMERIE  
NATIONALE**

**17**

Accueil Soisy : mardi et vendredi