DÉPARTEMENT
BOUCHES-DU-RHÔNE

BIEN VIEILLIR EN CONFIANCE

APPRENEZ À REPÉRER LES PIÈGES ET À VOUS PROTÉGER !

Arnaques téléphoniques, démarchage abusif, cyberarnaques, cambriolages…



MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE

BIEN VIEILLIR,

c'est pouvoir vivre librement, sereinement et en toute confiance.

Madame, Monsieur,

Avec les années, nous avons tous à cœur de préserver notre liberté, nos habitudes et les liens qui nous sont chers. Votre bien-être et votre tranquillité sont précieux. C'est pourquoi le Département des Bouches-du-Rhône est à vos côtés pour vous accompagner au quotidien.



Les arnaques et les abus prennent aujourd'hui des formes diverses : faux sites Internet, démarchage abusif, usurpation d'identité ou escroqueries bancaires et sentimentales. Face à ces pièges, chacun peut être vulnérable. En parler, s'informer et demander conseil sont autant de façons de se protéger.

C'est tout le sens de cette journée « Bien vieillir en confiance » : vous apporter des repères simples, répondre à vos questions et vous permettre d'aborder ces situations plus sereinement.

Avec les Maisons du Bel Âge, nous veillons à rester proches de vous et à vous offrir des lieux d'écoute et de soutien. N'hésitez jamais à solliciter de l'aide : personne ne doit se sentir seul face à une difficulté.

Je souhaite que ce forum soit avant tout un moment chaleureux, fait de rencontres, d'échanges et de conseils utiles, où chacun se sente accueilli et écouté.

Parce que vieillir en confiance, c'est aussi savoir que l'on peut compter sur les autres, nous continuerons à agir pour que chacun trouve sa place et puisse avancer en âge dignement, entouré et libre de ses choix.

Je vous souhaite à toutes et à tous un très beau forum, placé sous le signe de la bienveillance et du partage.

Bien sincèrement,

Martine Vassal
Présidente du Conseil départemental des Bouches-du-Rhône



HAMEÇONNAGE PHISHING :

Définition : L'hameçonnage ou phishing est une technique de cyberfraude via un SMS ou mail frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance.

Exemples :

1 - Mme Dubois reçoit un SMS : « *Assurance Maladie : Vous avez droit à un remboursement de* ***47 €****. Cliquez sur le lien ci-dessous pour mettre à jour votre dossier*. »
Après avoir cliqué, on lui demande ses informations personnelles, numéro de Sécurité Sociale, mail, téléphone et informations bancaires.

2 - M. Bernard, 70 ans, reçoit un E-MAIL qui semble provenir des impôts. L'adresse de l'expéditeur est étrange : impots-france-remboursement@mail-service.com / au lieu d'une adresse officielle du gouvernement. Cet e-mail indique un montant de remboursement et lui demande de cliquer sur le lien.

Les bons réflexes :

1 - Ne cliquez jamais sur un lien reçu par mail ou SMS et ne répondez pas aux messages suspects.

2 - Ne communiquez jamais votre numéro de carte bancaire.

3 - Gardez vos identifiants et mots de passe strictement confidentiels.

4 - Connectez-vous directement sur le site officiel ou l'application habituelle.

5 - Supprimez immédiatement les messages frauduleux ou suspects.

6 - Demandez de l'aide à un proche ou à la Maison du Bel Âge.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



FRAUDE À LA CARTE BANCAIRE

Définition : La fraude à la carte bancaire désigne l'utilisation frauduleuse des coordonnées de la carte bancaire d'une personne à son insu alors que celle-ci est pourtant toujours en possession de sa carte.

Exemples :

1 - Mme Bernard, 74 ans, consulte son compte bancaire et découvre un paiement de **89 €** chez un commerçant qu'elle ne connaît pas. Elle est certaine de ne jamais avoir effectué cet achat.

2 - M. Durand, 68 ans, remarque sur son relevé bancaire un prélèvement de **420 €** vers un compte inconnu. Il comprend rapidement qu'il n'est pas à l'origine de cette opération.

Les bons réflexes :

1- Faites opposition à votre carte bancaire sans attendre :

> Heures ouvrables : via votre conseiller bancaire ou via l'application de votre banque.

> Heures non ouvrables : via l'application ou le numéro serveur interbancaire national (cf. numéro utile).

2 - Conservez toutes les preuves de la fraude.

3 - N'utilisez plus la carte bancaire concernée.

4 - Réagissez immédiatement, n'attendez pas plusieurs jours pour voir si le problème se règle tout seul.

5 - Vérifiez tous les prélèvements inhabituels, même les plus petits.

6 - Demandez de l'aide à un proche ou à la Maison du Bel Âge.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



FRAUDE AU FAUX CONSEILLER BANCAIRE

Définition : La fraude au faux conseiller bancaire désigne un type d'escroquerie qui consiste à tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes.

Exemples :

1- Mme Martin, 72 ans, reçoit un appel d'une personne qui se présente comme conseiller bancaire : « *Madame, nous avons détecté un virement frauduleux de **1 500 €** sur votre compte. Il faut agir immédiatement sinon vous allez perdre cet argent !* » La personne paraît très convaincante et insiste pour obtenir des informations rapidement.

2 - M. Dupont reçoit le SMS suivant :
*" "ALERTE FRAUDE". Une opération de **950 €** est en cours sur votre compte. Pour l'annuler, cliquez sur ce lien et saisissez le code reçu par SMS"*. Peu après, il reçoit un appel d'une personne affirmant être du service fraude de sa banque.

Les bons réflexes :

1 - Raccrochez immédiatement ou ne répondez pas au message.

2 - Contactez directement votre banque avec vos coordonnées habituelles :

> Heures ouvrables : via votre conseiller bancaire ou via l'application de votre banque.

> Heures non ouvrables : via l'application de votre banque ou le numéro serveur interbancaire national (cf. numéro utile)

3 - Ne communiquez jamais vos informations bancaires par téléphone.

4 - Ne rappelez jamais un numéro communiqué par un interlocuteur inconnu.

5 - Demandez de l'aide à un proche ou à la Maison du Bel Âge.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



SPAM TÉLÉPHONIQUE

Définition : Le spam téléphonique désigne un appel téléphonique ou SMS non voulu à des fins publicitaires, commerciales ou malveillantes.

Exemple :

Mme Martin, 81 ans, reçoit un appel d'un commercial. Celui-ci insiste sur le fait que ses enfants devront payer des frais importants à son décès si elle ne souscrit pas immédiatement un contrat de prévoyance. Sous la pression et sans prendre le temps de la réflexion, elle donne son accord par téléphone et souscrit à un contrat dont les cotisations sont élevées et peu adaptées à sa situation.

Les bons réflexes :

1 - Raccrochez ou mettez fin à l'échange si vous n'êtes pas intéressé.

2 - Prenez le temps de réfléchir.

3 - Ne communiquez jamais votre RIB à un inconnu.

4 - Protégez vos informations personnelles.

5 - Ne signez jamais un contrat dans l'urgence. Un professionnel sérieux vous laisse toujours le temps de la réflexion avant de prendre une décision.

6 - Demandez de l'aide à un proche ou à la Maison du Bel Âge.

MAISON DU **BEL ÂGE**
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



FAUX SITES INTERNET

Définition : Un faux site Internet est un site web frauduleux qui imite l'apparence d'un site officiel, d'une entreprise connue ou d'un commerce en ligne afin de tromper les internautes.

Exemple :

Mme Dupont, 67 ans, voit une publicité sur Internet : « *Vélo électrique **79 €** au lieu de **1 200 €** - Déstockage exceptionnel !* » Le site affiche un compte à rebours et indique : *« Plus que 3 exemplaires disponibles !* ». Pressée de profiter de l'offre, elle commande immédiatement.

Les bons réflexes :

1 - Prenez le temps de vous renseigner sur les sites que vous ne connaissez pas.

2 - Méfiez-vous des prix anormalement bas.

3 - Comparez les offres avant de passer commande.

4 - Assurez-vous que le paiement s'effectue sur une page sécurisée. Avant de renseigner vos coordonnées bancaires, vérifiez que l'adresse du site commence par https:// et qu'un cadenas apparaît dans la barre d'adresse de votre navigateur.

5 - Demandez de l'aide à un proche ou à la Maison du Bel Âge.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



FAUX SITES ADMINISTRATIFS

Définition : Un faux site administratif est un site internet frauduleux qui imite un service public ou une administration officielle.

Exemples :

1 - Le faux site ANTS pour refaire sa carte d'identité

Sur internet : Mme Dupont souhaite renouveler sa carte d'identité. Elle tape « *Renouvellement carte d'identité ANTS* ». Le premier site proposé indique : « *Démarches ANTS simplifiées - Service rapide : **49 €*** ». Elle pense être sur le site officiel, paie les frais et transmet ses documents personnels.
En réalité, il s'agit d'un site privé qui facture un service inutile ou récupère des données personnelles.

2 - M. Bernard a besoin de consulter ses points de permis. Il trouve un site qui indique :
« *Consultez instantanément votre solde de points **- 29 €*** ».

Le site demande :

> sa carte d'identité ;

> son permis ;

> ses coordonnées bancaires.

Les escrocs utilisent souvent l'apparence des sites officiels pour récupérer des informations personnelles.

Les bons réflexes :

1 - Vérifiez toujours que l'adresse du site se termine par « .gouv.fr ».

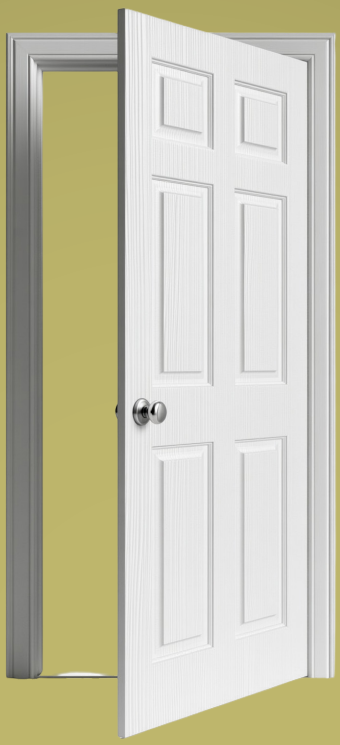
2 - Privilégiez les sites officiels de l'État.

3 - Ne cliquez pas systématiquement sur le premier résultat d'une recherche internet.

4 - Ne transmettez jamais vos documents d'identité sans vérifier le destinataire.

5 - Demandez de l'aide à un proche ou à la Maison du Bel Âge.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



DÉMARCHAGE ABUSIF À DOMICILE ET FAUX PROFESSIONNELS

Définition : 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.

Exemples :

1 - Mme Durand, 82 ans, laisse entrer un prétendu agent chargé de vérifier son installation électrique. Pendant qu'elle cherche une facture à sa demande, il repère ses objets de valeur. Quelques jours plus tard, son domicile est cambriolé.

2 - M. Bernard, 78 ans, laisse entrer un prétendu plombier venu vérifier une fuite dans l'immeuble. Pendant qu'il lui demande de faire couler l'eau dans la salle de bain, le faux professionnel fouille le logement et vole des objets de valeur.

Les bons réflexes :

1 - Si vous le pouvez, vérifiez le nombre de personnes présentes avant d'ouvrir la porte (par le visiophone ou le judas).

2 - Demandez systématiquement une carte professionnelle.

3 - Ne signez jamais un document sans avoir reçu et consulté un devis. Ne versez pas d'argent, ne signez pas de chèque, surtout antidaté.

5 - En cas de doute, proposez d'appeler l'organisme professionnel auquel est rattaché le démarcheur.

6 - Si possible, faites-vous accompagner.

La présence d'un voisin, d'un proche ou d'une personne de confiance peut vous aider à prendre du recul et à éviter toute décision précipitée.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



ARNAQUE AUX DISTRIBUTEURS DE BILLETS

Définition : Les arnaques aux distributeurs de billets regroupent les techniques utilisées par des personnes malveillantes pour voler de l'argent ou récupérer les données bancaires d'un usager lorsqu'il retire de l'argent à un distributeur automatique.

Exemples :

Les billets de banque bloqués dans le distributeur

Des escrocs installent un dispositif artisanal (souvent en plastique ou fixé avec du ruban adhésif) dans la fente de sortie des billets afin de bloquer la sortie des billets. La victime pense alors à une panne et quitte les lieux, laissant les billets de banque coincés que les malfaiteurs récupèrent ensuite.

La carte bancaire piégée ou « collet marseillais »

Des individus installent un dispositif pour retenir la carte bancaire. L'automate refuse de rendre la carte de paiement. Un complice intervient alors en proposant son aide et incite la victime à saisir de nouveau son code confidentiel. Une fois la victime partie, l'escroc, ayant mémorisé le code, récupère la carte et l'utilise pour effectuer des achats ou retraits.

Les bons réflexes :

1 - Contactez votre banque dès que possible pour faire opposition à votre carte bancaire.

> Heures ouvrables : via son conseiller bancaire ou via l'application de votre banque.

> Heures non ouvrables : via l'application de votre banque ou le numéro serveur interbancaire national (cf. numéro utile)

2 - Restez vigilant : si aucun billet ne sort alors que la transaction a été validée, prenez le temps de vérifier la fente de distribution pour repérer toute anomalie.

3 - Ne quittez pas immédiatement le distributeur : en cas de problème, contactez rapidement la banque via le numéro indiqué sur le distributeur.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE



ARNAQUES AUX SENTIMENTS

Définition : L'arnaque aux sentiments, également appelée escroquerie amoureuse, est une fraude dans laquelle une personne mal intentionnée crée une relation affective ou amoureuse fictive avec sa victime, le plus souvent via Internet (réseaux sociaux, sites de rencontre, messageries).

Exemples :

1 - Monsieur Jean, 72 ans, veuf depuis plusieurs années, fait la connaissance d'une femme sur un réseau social. Très attentionnée, elle échange avec lui chaque jour et lui déclare rapidement ses sentiments. Quelques semaines plus tard, elle lui demande **1 500 €** pour résoudre un prétendu problème de voyage.

2 - Madame Marie, 68 ans, rencontre un homme sur un site de rencontre. Après plusieurs semaines d'échanges, celui-ci affirme être en difficulté financière à l'étranger et lui demande de lui envoyer **800 €** en urgence.

Les bons réflexes :

1 - Ne donnez jamais vos coordonnées bancaires à qui que ce soit.

2 - Ne transférez jamais d'argent, même si la personne vous prend par les sentiments.

3 - Demandez l'avis d'un proche avant toute démarche financière et vérifiez l'identité de votre interlocuteur.

MAISON DU BEL ÂGE
DÉPARTEMENT DES BOUCHES-DU-RHÔNE

NOTES

NUMÉROS UTILES

cybermailveillance.gouv.fr

Info escroquerie : 0805 805 817

Signalement sms et appels frauduleux : 33700

Serveur interbancaire d'opposition : 0 892 705 705*

*Numéro surtaxé (+ 0,35 € / minute)

Contre le démarchage téléphonique : Appli Saracroche

En cas de doute ou d'incident suspect : appelez le 17

DÉPARTEMENT BOUCHES-DU-RHÔNE

departement13.fr

Direction de la communication - Département des Bouches-du-Rhône