



DÉMARCHAGE ET ARNAQUES

**En partenariat avec
la ville de VENELLES**





Aix-en-Provence

LE DÉMARCHAGE

LE DÉMARCHAGE

Le démarchage consiste en le fait pour une personne de contacter directement des personnes afin de leur faire souscrire un contrat à visée commerciale.

→ Par téléphone

→ Au domicile



Attention le démarchage à domicile peut également avoir un but de repérage en vue d'un délit ou d'une arnaque (vérification charpente, isolation sous toiture, ...)

LE DÉMARCHAGE

Légal mais juridiquement encadré



Contrat valable



Support durable

Articles L221-5, L221-7 et L221-13 du Code de la consommation



Rétractation - délai 14 jours

Art. L221-18 du Code de la consommation

LE DÉMARCHAGE

Lutter contre les appels intempestifs



Loi du 24 juillet 2020 interdit le démarchage pour les travaux de rénovation énergétique



Loi du 19 décembre 2022 interdit le démarchage pour le CPF



Amende 75 000 € pour les personnes physiques à 375 000 € pour les personnes morales

LE DÉMARCHAGE

Lutter contre les appels intempestifs



- ✓ Bloctel / Signal Conso / DGCCRF
- ✓ Applications mobiles
- ✓ Téléphone fixe Panasonic KX-TGH720FR recommandé par l'UFC-Que Choisir
- ✓ Appels malveillants réitérés
Article 222-16 du Code pénal punit d'un an d'emprisonnement et 15 000 € d'amende

LE DÉMARCHAGE

Lutter contre les appels intempestifs



Décret du 14 octobre 2022 applicable au 1er mars 2023

- ✓ Bloctel ou non
- ✓ Limite le démarchage du lundi au vendredi - 10h-13h/14h-20h
- ✓ Pas plus de 4 appels par mois par le même professionnel
- ✓ Si refus, le professionnel doit attendre 60 jours avant d'établir un nouveau contact
- ✓ Fin des 06, 07 et 04 (uniquement 09 37 / 09 38 / 09 39 / 04 24 / 04 25)



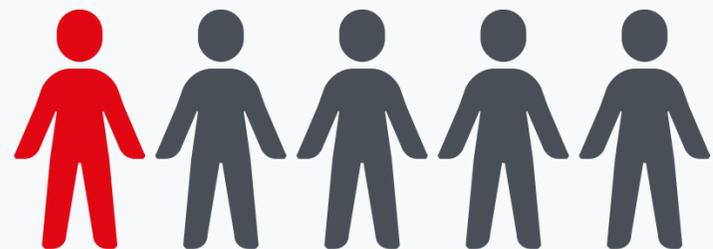
Amende 75 000 € pour les personnes physiques à 375 000 €
pour les personnes morales



Aix-en-Provence

LES ARNAQUES

LES ARNAQUES



En 2020, près d'un Français sur cinq a été victime d'une arnaque

+17%

d'escroqueries en 2022

67%

des victimes n'ont pas déposé plainte

LES ARNAQUES

LES RECOURS CIVILS

LES BANQUES

BANK

Paiements frauduleux = paiements réalisés à l'insu du consommateur : la banque a une obligation de remboursement (art. L.133-18 du code monétaire et financier)

À moins qu'elle ne prouve une faute du consommateur

Cependant, les banques ont tendance à rechigner quant au remboursement en refusant environ 38% des demandes de remboursement.

LES ARNAQUES

LES RECOURS CIVILS



LES BANQUES

- ✓ Invoquer le défaut de conseil par la banque
- ✓ Jurisprudence obligation de **vigilance** vs. obligation de **non ingérence**
- ✓ Manquement au RGPD
- ✓ Signaler les messages frauduleux à l'adresse :
 - ✉ fraude-bretic@interieur.gouv.fr

LES ARNAQUES

LES BANQUES - **Conseils et infos utiles**



➔ **L'authentification forte**

Dispositif permettant de vérifier votre identité pour plus de sécurité lors des paiements. Il faut les 2 éléments suivants :

- un **élément de connaissance** (mot de passe, code secret ou question secrète)
- un **élément de possession** (téléphone mobile)

➔ **Refus de remboursement des fraudes bancaires**

L'UFC-Que Choisir a déposé plainte le 28 juin 2022 contre 12 banques pour **pratique commerciale trompeuse** car refus de remboursement sans démontrer la **négligence grave** du consommateur.

LES ARNAQUES

LES BANQUES - **Conseils et infos utiles**



➔ **Des pénalités de retard prévues**

Depuis le 19 août 2022, des pénalités sont désormais prévues en cas de retard de remboursement par les banques des opérations non autorisées

- la banque doit rembourser **immédiatement**
- Exception si **soupçon de fraude** par l'utilisateur du service de paiement avec dénonciation à la BF

➔ **Et si votre banque vous demande de déposer plainte ?**

Pratique illégale : les banques ne doivent pas exiger un dépôt de plainte pour traiter la demande de remboursement

LES ARNAQUES

LE RECOURS PÉNAL

Si dépôt de plainte rapide, possibilité de bloquer les fonds

- **VOL** art. 311-1 du Code pénal
- **EXTORSION** art. 312-1 du Code pénal
- **ESCROQUERIE** art. 313-1 du Code pénal
- **ABUS DE CONFIANCE** art. 314-1 du Code pénal



Aix-en-Provence

Liste des arnaques Comment les repérer

Le faux conseiller bancaire

Une escroquerie consistant à vous faire confirmer des opérations de paiement à votre insu est en pleine recrudescence. Si votre soi-disant conseiller bancaire vous appelle et vous demande d'annuler – ou de valider – des opérations frauduleuses sur votre compte, raccrochez !

Une personne vous appelle et se présente comme votre conseiller bancaire. Le numéro affiché sur votre téléphone correspond à celui de votre établissement. Votre interlocuteur vous indique avoir repéré des mouvements frauduleux sur votre compte bancaire. Afin d'empêcher ces opérations, le pseudo-conseiller vous demande de procéder à une validation de paiement.



Le faux conseiller bancaire

Conseils et astuces



Vérifiez l'information : **raccrochez puis appelez** votre conseiller afin qu'il confirme l'information. Ce dernier ne vous demandera jamais vos codes par téléphone.



Si vous avez été escroqué, **faites opposition** sur votre carte bancaire et contactez votre banquier. Même s'il refuse de vous rembourser, il surveillera votre compte.



Signalez la fraude en ligne avec le téléservice **Perceval** (via *service-public.fr*). Le signalement n'est pas un dépôt de plainte, mais il permet de centraliser les déclarations de fraude bancaire pour aider les services de police.

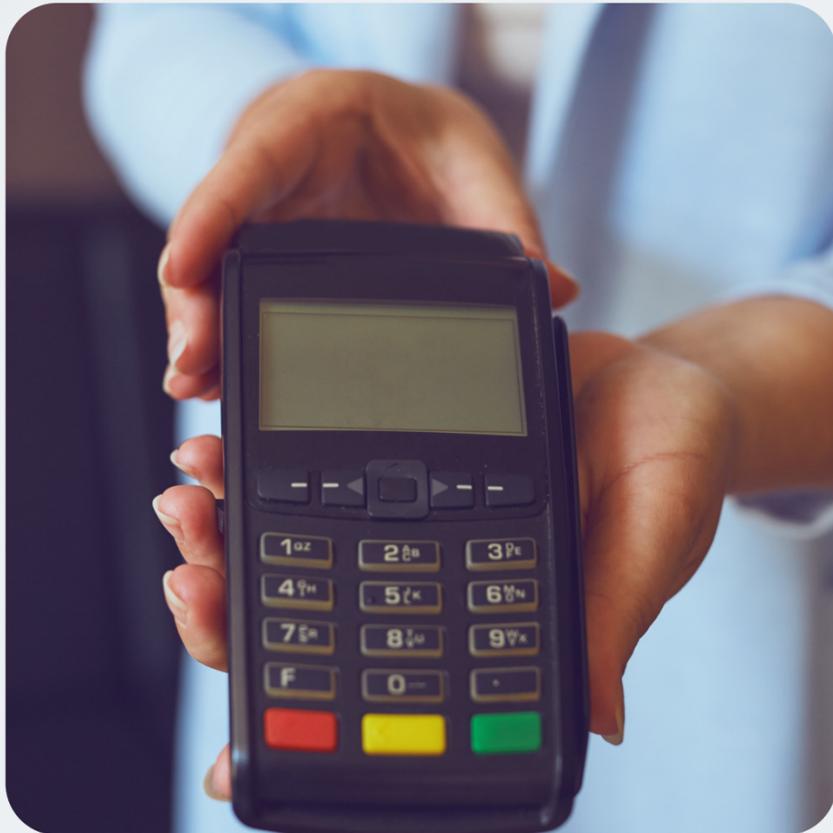


Depuis le 15 mars 2022, il existe la **plateforme Thésée**. Par ce biais, il est possible de déposer plainte en ligne pour les escroqueries.



Attention, arrêt du 28 mars 2023 de la Cour d'appel de Versailles - BNP Paribas

Le faux terminal de paiement



Une recrudescence d'arnaques au terminal de paiement électronique (TPE) à la sortie des magasins. Les escrocs abordent les clients après leur passage en caisse en se faisant passer pour des employés de l'enseigne et prétextent une erreur en leur faveur lors du paiement à la caisse. Les escrocs sont équipés d'un terminal de paiement et demandent alors au client d'insérer sa carte bancaire et de recomposer son code afin d'être recredité.

- ✓ Adressez-vous à l'accueil ou à votre caisse

Les faux RIB

Vous êtes en relation avec une entreprise ou une personne à qui vous devez de l'argent. Celle-ci vous adresse un RIB par courriel et une facture en pièce jointe afin de procéder au règlement. Ce courriel est intercepté par un escroc, en piratant soit votre boîte e-mail, soit celle de la société, pour remplacer le RIB de votre créancier par le sien.



- ✓ Essayer d'obtenir le RIB par remise physique
- ✓ Vérifiez l'adresse courriel de l'expéditeur
- ✓ Vérifiez que le RIB est français (IBAN commence par FR)
- ✓ Essayer de contacter le professionnel

Attention pas de remboursement par votre banque

La vignette Crit'Air

Vous recevez un mail ou sms vous rappelant que votre véhicule ne possède pas de vignette Crit'Air et que vous risquez une amende. Le message est suivi d'un lien frauduleux dont le but est de vous soutirer des informations personnelles ou bancaires, voire de vous faire payer la vignette à un tarif exorbitant.

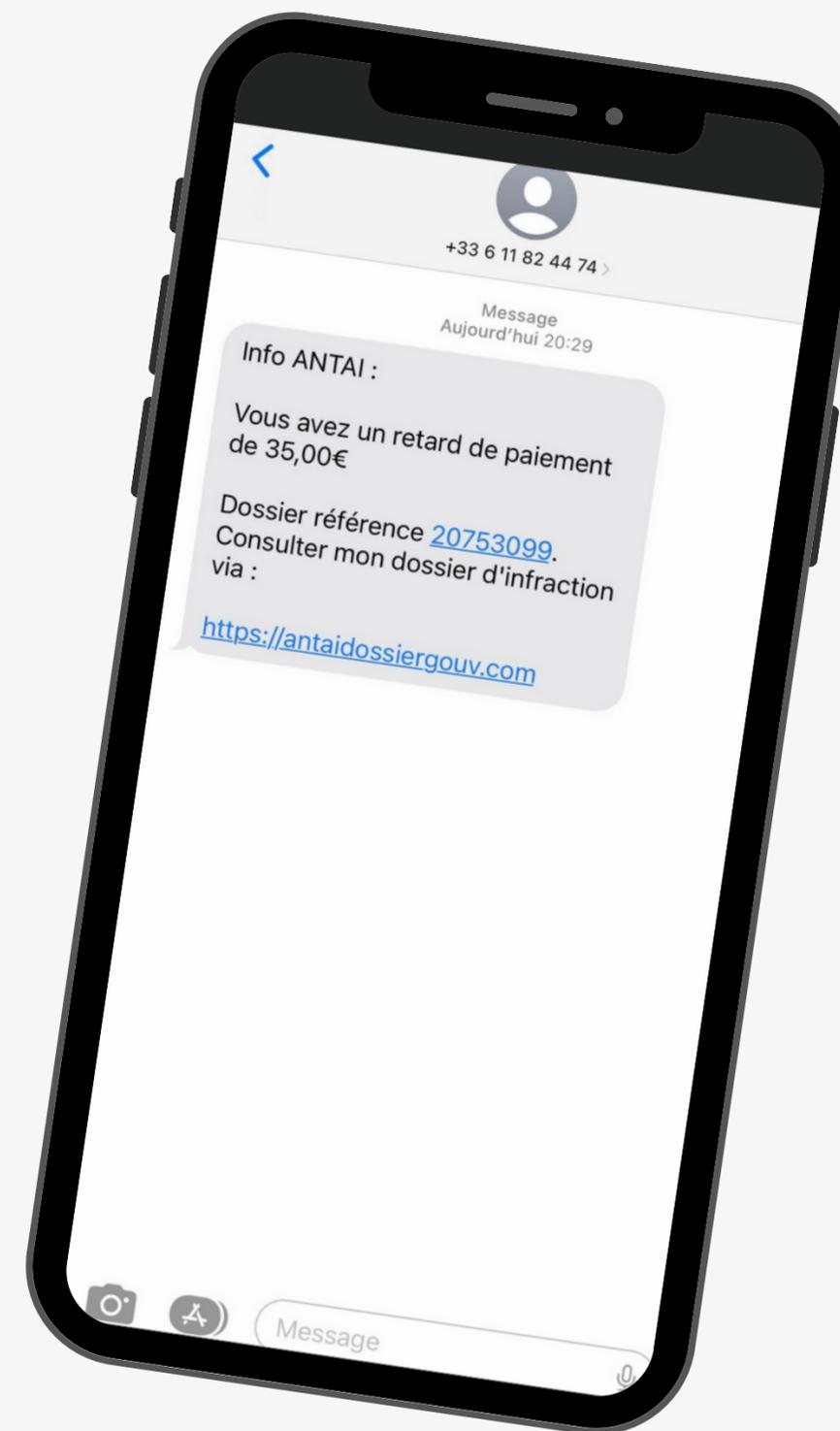
- ✓ Site officiel : www.certificat-air.gouv.fr
- ✓ Coût de la vignette : 3,72€
- ✓ Renseignements au 0 800 97 00 33



Le retard de paiement d'une amende

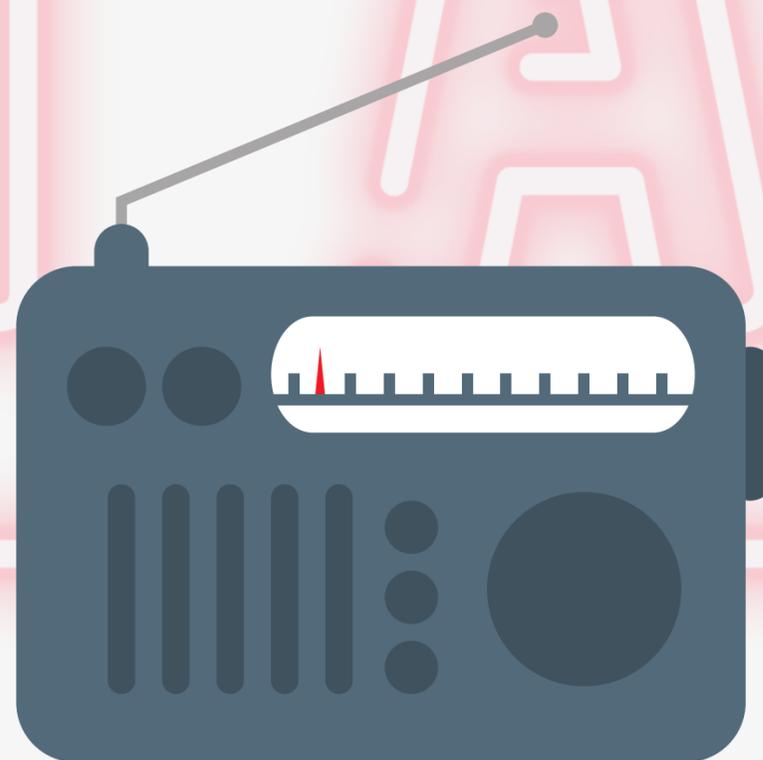
Les escrocs se font passer pour l'Agence nationale de traitement automatisé des infractions (Antai). Des sms frauduleux mentionnent un retard de paiement pour une amende et essaient de récupérer vos informations personnelles ou vos données bancaires. Le principe est simple, le sms prétend que le destinataire a un "*retard de paiement d'une amende*", le message est suivi d'un lien amenant vers un site frauduleux comme *amendes-gouv.org*, *dossier-antai-gouv.info*, etc.

- ✓ Ne jamais cliquer sur les liens
- ✓ Signaler le SMS au **33 700**
- ✓ Site officiel : **www.amendes.gouv.fr**



SUPER FM : la fausse radio

Une personne se présente comme chargée de marketing d'une nouvelle radio nommée "Super FM" fréquence 98,5. Pour promouvoir cette nouvelle radio, ils offrent des cadeaux aux nouveaux auditeurs (300 à 600 euros). Pour recevoir les cadeaux, il faut joindre le 09 73 42 11 56 (numéro surtaxé).



Vous avez gagné à l'EuroMillions

Des Français ont reçu dans leur boîte mail un message leur indiquant un gain lors d'un tirage. *"Bonjour Madame / Monsieur, nous vous contactons pour vous informer que vous venez de gagner la somme de 450 000 € du tirage au sort organisé par la Française des Jeux. Loterie EuroMillions. Pour la réclamation du gain veuillez entrer en contact direct avec maître XXX."*

Attention donc à ces escrocs qui vous demanderont de renseigner vos informations personnelles et exigeront des paiements de frais administratifs pour pouvoir toucher vos gains.

- ✓ Rendez-vous chez votre buraliste ou sur www.fdj.fr
- ✓ Ne cliquez pas sur le lien



La carte vitale

Vous recevez un message vous demandant de cliquer sur un lien afin de **renouveler votre carte vitale**. Ce lien vous conduit vers une page internet similaire à celle de l'Assurance maladie. Il vous est demandé ensuite de renseigner votre nom, votre adresse et enfin **vos coordonnées bancaires**. Cette arnaque vous demande ainsi de payer afin d'obtenir votre nouvelle carte vitale.

- ✓ Mise à jour gratuite dans les pharmacies ou chez les médecins



Menace de poursuites judiciaires

Le principe de ces mails, contenant parfois une pièce jointe, est de faire croire à leur destinataire qu'il est convoqué par les forces de l'ordre pour des faits graves (pédopornographie, pédophilie).

Ces courriers usurpent l'appellation de la gendarmerie, de la police, de la préfecture ou bien d'Europol. Les victimes sont alors invitées à poursuivre l'échange en répondant par mail. Puis, il leur est demandé de faire un virement bancaire, présenté comme une amende, afin de "classer l'affaire".


RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

**DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS**

CONVOCAZIONE EN JUSTICE
Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

À votre attention,
À la demande de Madame, Catherine DE BOLLE commissaire générale de la police fédérale, élue au poste de directrice d'Europol " Brigade de protection des mineurs (BPM) " nous vous adressons cette convocation.

La COPJ ou convocation par officier de police judiciaire est prévue par l'article 390-1 du Code de Procédure Pénale. Elle vaut citation devant le Tribunal et est décidée par le Procureur de la République.

En application des dispositions de l'article 372 du code pénal énonce : " Tout attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de seize ans accomplis, sera puni de la réclusion.

L'article 227-23 du Code pénal dispose : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.

Nous engageons à votre rencontre, des poursuites judiciaires peu après une saisie informatique de la Cyber-infiltration pour :

- Pédopornographie
- Pédophilie
- Exhibitionnisme
- Cyber pornographie
- Trafic sexuel

Pour votre information, la loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges mails.
Les photos/vidéos dénudées de vous que vous envoyez aux mineurs ont été enregistrées par notre cyber gendarme et constituent les preuves de vos infractions.

Cette convocation présente un caractère obligatoire. Conformément à l'article 78 du code pénal, l'officier de police judiciaire peut contraindre à comparaître par la force publique, avec l'autorisation préalable du procureur de la République, les personnes qui n'ont pas répondu à une convocation à comparaître ou dont on peut craindre qu'elles ne répondent pas à une telle convocation.

Dans un souci de confidentialité nous vous adressons cet e-mail, vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à Mme Myriam Quémener, procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre rencontre, nous vous adresserons dans ce cas une lettre recommandée avec accusé de réception (arrestation immédiate) par la gendarmerie la plus proche de votre «Lieu de résidence » et vous serez fiché au registre national des délinquants sexuels. Dans ce cas, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux medias pour publication de personne fiché au RNDS.

*En cas de non-respect de la procédure et du délai, la lettre de convocation vous sera envoyée par courrier postal.
Cordialement,

Mme Catherine De Bolle, commissaire générale de la police fédérale, élue au poste de directrice d'Europol" la brigade de protection des mineurs (BPM)"

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS

Les faux sites web

- ✓ Vérifier le cadenas de sécurité à côté de l'URL 
- ✓ Vérifier les mentions légales du site (bas de page)
- ✓ Chercher les fautes d'orthographe

La banque ne rembourse pas car négligence du client sauf s'il n'avait pas connaissance de l'arnaque.



Les numéros surtaxés

Cette arnaque consiste en le fait de laisser un message vocal ou un sms à un destinataire, en prétendant qu'il faut qu'il rappelle un certain numéro... sauf que ce-dernier est surtaxé : ce qui fera enfler la facture téléphonique.



- ✓ **Surtout ne pas rappeler des numéros commençant par 08... ce ne sont que des numéros surtaxés.**
- ✓ **Dénoncer sur la nouvelle plateforme officielle dédiée aux attaques virtuelles : cybermalveillance.gouv.fr**

Bon à savoir : article L121-16 du Code de la consommation exige que le consommateur dispose d'un numéro de téléphone gratuit pour joindre le professionnel avec lequel il détient un contrat.

Les sites de petites annonces

- ✓ **Paiement par le site et non directement auprès du vendeur**
- ✓ **Vérifier la fiabilité de l'annonce : difficile car les sites ne sont pas contraints par la loi de vérifier la fiabilité des annonces, simplement de les supprimer une fois signalées comme frauduleuses**

leboncoin

Abritel®



Facebook Marketplace

Escroquerie au paiement sans contact

Grâce à un terminal dans leur sac, des arnaqueurs peuvent débitier 50 euros à de nombreuses cartes de paiement sans contact. Attention, les banques réfléchissent à augmenter le plafond de paiement sans contact.



Il existe un moyen de s'en prémunir :
des étuis anti-ondes NFC



Prélèvements frauduleux

Nouvelle arnaque aux prélèvements non autorisés à la suite du vol d'un fichier contenant les IBAN de clients français.

Des prélèvements de prestataires inconnus ont été effectués, notamment avec le libellé d'une entreprise nommée "ENS".

- ✓ **Vérifiez régulièrement vos comptes (prélèvements de petites sommes)**

Si vous n'avez pas autorisé de prélèvement, la banque doit vous rembourser.

Arnaque Agirc-Arrco



The screenshot shows the top navigation bar of the Agirc-Arrco website with links for 'PARTICULIERS', 'ENTREPRISES', and 'NOUS CONNAÎTRE'. A search bar is present on the right. Below the navigation, there are links for 'RETRAITE COMPLÉMENTAIRE', 'Ma retraite', 'Mes services', 'Les actualités', 'Mes contacts', 'Nos offres d'emploi', and 'Médiathèque'. A 'Mon agirc-arrco' button with 'JE ME CONNECTE' is also visible. A breadcrumb trail reads: 'Espace presse > Les dernières actualités > Attention aux SMS, appels ou emails frauduleux'. The main heading of the article is 'Attention aux SMS, appels ou emails frauduleux'. Below the heading is an image of hands typing on a laptop with a large purple padlock icon overlaid, symbolizing security. A small chatbot icon is in the bottom right corner of the image area.

Ces communications usurpent le nom et le logo de l'Agirc-Arrco afin de récupérer des données personnelles. L'Agirc-Arrco rappelle qu'il ne faut en aucun cas répondre aux demandes faites par ces messages.

Les caisses de retraite ne réclament jamais vos coordonnées bancaires par mail ou sms pour effectuer un remboursement.

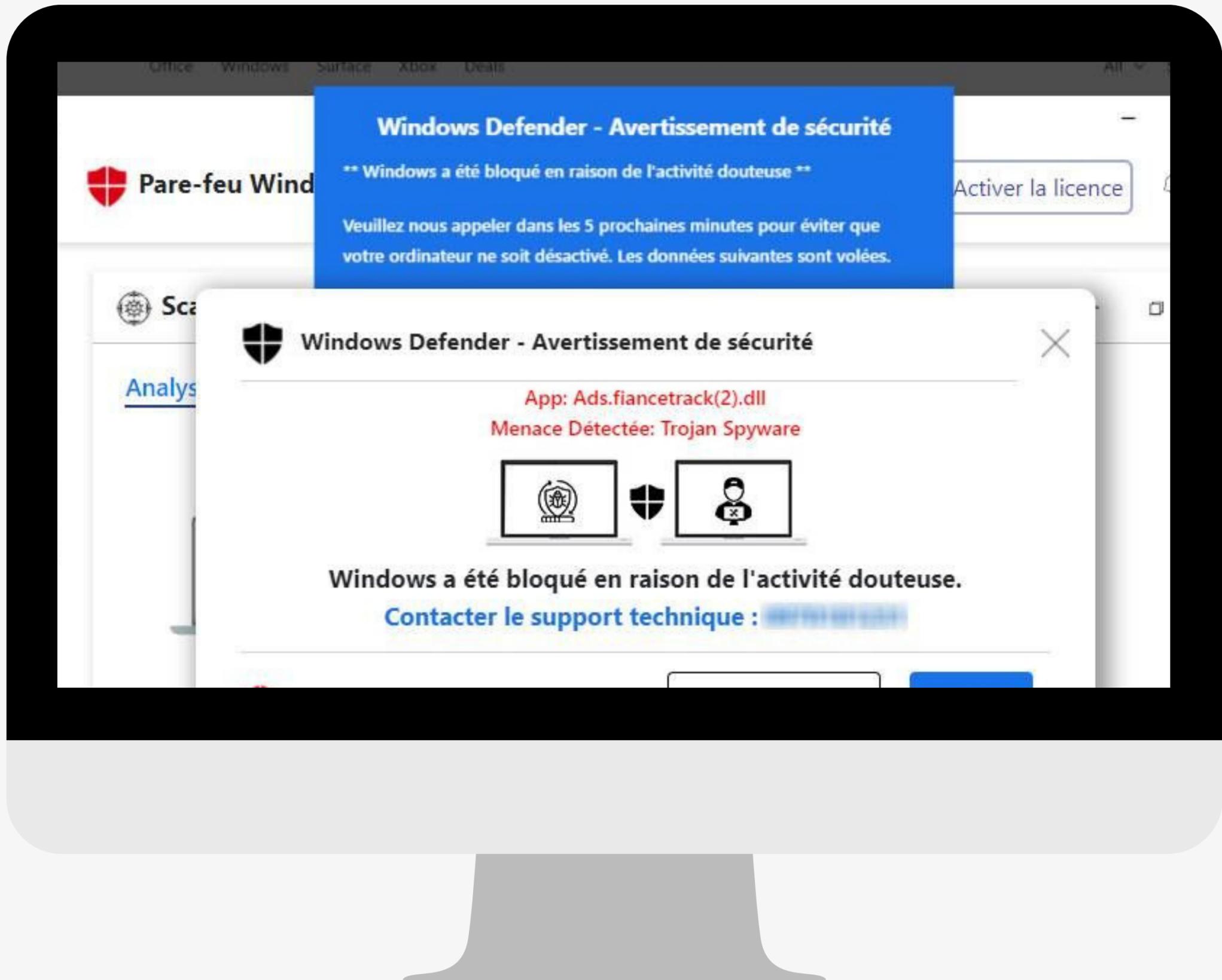


Phishing classique

L'arnaque Microsoft

"Votre ordinateur a un problème"

- ✓ Ne pas appeler le numéro
- ✓ Débrancher et rallumer son ordinateur
- ✓ Supprimer les cookies



Le faux tueur à gages

High-Tech > Internet > Arnaques



ACTUALITÉ

Arnaque

Et maintenant le faux tueur à gages



Vous avez été destinataire d'un message provenant d'un homme menaçant de vous faire la peau si vous ne lui remettez pas une somme d'argent ? Pas de panique. Vous pouvez supprimer le message et dormir tranquille.



Phishing classique



Merci pour votre écoute



**Merci à la ville de VENELLES pour
l'organisation
de cette rencontre**



NOUS CONTACTER



04.42.93.74.57



contact@aixenprovence.ufcquechoisir.fr



aixenprovence.ufcquechoisir.fr



UFCAixProvence



4 place Coïmbra
Le Félibrige, Bât. B
13090 Aix-en-Provence