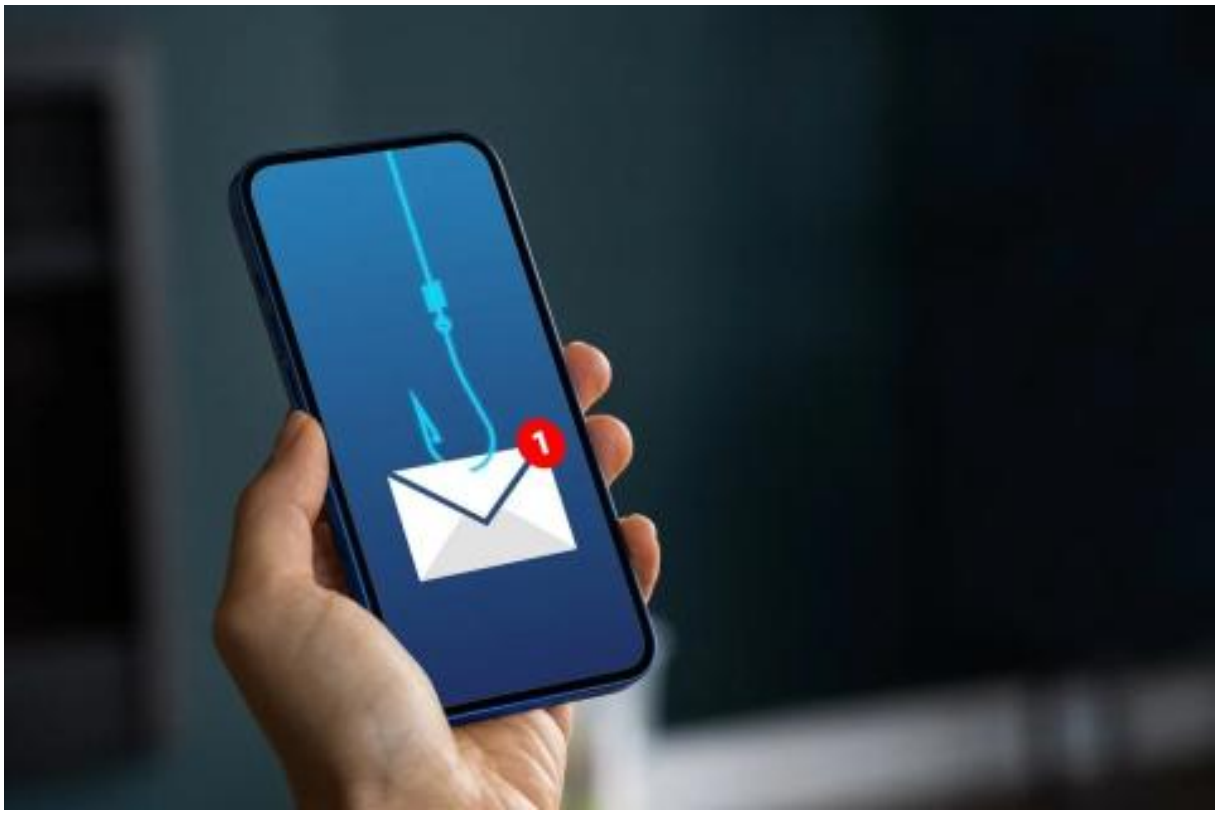
COMMENT DETECTER LES ARNAQUES EN LIGNE ET PAR TÉLÉPHONE ?



Comment se protéger face aux arnaques ?

Avec le déploiement de l'intelligence artificielle, les particuliers sont plus que jamais vulnérables face aux manœuvres frauduleuses de plus en plus nombreuses et sophistiquées. Les arnaques en ligne touchent aujourd'hui tous les Français, sans distinction d'âge ni de catégorie sociale.

Pour les déjouer, votre vigilance doit être permanente et vous devez adopter les bons réflexes.



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.

Hameçonnage

En quoi consiste l'arnaque ?

- L'hameçonnage représente la première menace numérique en France. Des messages frauduleux (e-mail, SMS, appel) imitent des organismes de confiance (banque, assurance maladie, impôts, La Poste, opérateurs téléphoniques) pour soutirer des identifiants, mots de passe ou coordonnées bancaires.

Comment se protéger ?

- Sachez qu'aucun service légitime ne vous demandera vos identifiants et mots de passe personnels.
- Ne cliquez jamais sur un lien reçu par message sans vérifier soigneusement l'adresse de l'expéditeur.
- Vérifiez l'URL avec attention : le nom de domaine doit correspondre exactement au site officiel (une seule lettre différente peut trahir une arnaque).
- En cas de doute, accédez au site officiel directement via votre navigateur, sans utiliser le lien reçu.

Que faire si vous êtes victime ?

- Changez immédiatement les mots de passe compromis.
- Contactez votre banque si des données bancaires ont été transmises.
- Signalez le message frauduleux sur **signal-spam.fr** ou par SMS au 33700.
- Consultez **cybermalveillance.gouv.fr** pour une assistance personnalisée.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Usurpation d'identité

En quoi consiste l'arnaque ?

- Des fraudeurs s'emparent de données personnelles (pièce d'identité, coordonnées, RIB) pour ouvrir des comptes bancaires, souscrire des crédits ou commettre des fraudes au nom de la victime. L'usurpation peut résulter d'un vol physique de document, d'une fuite de données ou d'un hameçonnage.

Comment se protéger ?

- Ne transmettez jamais de photocopie de pièce d'identité sans y apposer la mention de l'usage prévu et la date.
- Utilisez des mots de passe robustes et différents pour chaque service en ligne.
- Surveillez régulièrement vos relevés de compte bancaire.
- Détruisez soigneusement tout document contenant des données personnelles avant de le jeter.

Que faire si vous êtes victime ?

- Prévenez immédiatement votre banque et tous les organismes concernés.
- Consultez le fichier Ficoba sur **impots.gouv.fr** pour vérifier si des comptes ont été ouverts frauduleusement en votre nom (depuis "votre espace particulier" dans la rubrique "autres services").
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Achats en ligne

En quoi consiste l'arnaque ?

- Des sites frauduleux attirent les internautes avec des offres alléchantes : promotions exceptionnelles, disponibilité de produits normalement en rupture de stock, usurpation d'identité d'une marque reconnue etc. La victime règle sa commande mais ne reçoit jamais son produit en contrepartie.

Comment se protéger ?

- Vérifiez toujours les coordonnées d'un vendeur en ligne (adresse postale, numéro de téléphone, mentions légales).
- Privilégiez les modes de paiement sécurisés qui offrent un recours en cas de litige (la carte bancaire plutôt que le virement par exemple).
- Consultez les avis d'autres acheteurs sur des plateformes indépendantes.
- Méfiez-vous des offres avec décompte d'urgence ou prix anormalement bas.

Que faire si vous êtes victime ?

- Contactez immédiatement votre banque pour contester le paiement et demandez un remboursement.
- Conservez toutes les preuves (captures d'écran, e-mails, confirmations de commande).
- Signalez le site frauduleux sur **signal.conso.gouv.fr** et sur **internet-signalement.gouv.fr**.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Placements financiers

En quoi consiste l'arnaque ?

- L'escroquerie au placement financier vise à voler l'épargne d'un particulier en lui promettant des rendements importants sur des placements sans risques (actions, cryptomonnaies, devises etc.). L'escroc peut entrer en contact avec sa victime par l'intermédiaire des réseaux sociaux, messageries instantanées, forums ou encore sites de rencontre. Pour mettre en confiance sa victime, l'escroc dispose souvent d'un site d'allure professionnelle. Le jour où la victime souhaite récupérer ses fonds, l'escroc demande parfois le prépaiement de taxes (pour soutirer davantage d'argent) ou devient distant voire injoignable.

Comment se protéger ?

- Fuyez toutes les offres qui proposent des rendements élevés avec peu ou pas de prise de risque.
- Vérifiez systématiquement l'agrément de tout intermédiaire financier sur les registres officiels de **Regafi** ou de l'**Orias**.
- Consultez les listes noires de l'AMF et de l'ACPR sur **abe-infoservice.fr**.
- Renseignez-vous sur des sites fiables tels que **Finance Héros** qui répertorie notamment **les plateformes cryptos fiables**, **les meilleures banques en ligne**, **les meilleurs PEA**, **les meilleures assurances vie** ou encore **les meilleurs PER** du marché.
- Ne souscrivez ni sous la pression ni dans la précipitation.

Que faire si vous êtes victime ?

- Cessez tout échange avec l'escroc et méfiez-vous des propositions qui vous seront faites pour récupérer vos fonds (il peut s'agir d'une autre escroquerie).
- Contactez votre banque pour tenter de récupérer vos fonds et conservez toutes les preuves à votre disposition.

- Signalez l'arnaque à l'**AMF** ou à l'**ACPR**.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Support technique

En quoi consiste l'arnaque ?

- Un message d'alerte anxiogène semble bloquer l'ordinateur de la victime, l'invitant à contacter d'urgence un soi-disant service d'assistance (Microsoft, Apple, etc.). Un faux technicien prend ensuite le contrôle à distance de la machine et réclame une somme souvent importante pour une réparation totalement fictive.

Comment se protéger ?

- Sachez que les supports techniques légitimes ne réclament jamais d'argent directement.
- Ne composez jamais le numéro affiché dans une telle alerte.
- Si votre navigateur semble bloqué, fermez-le et redémarrez simplement votre ordinateur.
- N'autorisez jamais un inconnu à prendre le contrôle à distance de votre appareil.

Que faire si vous êtes victime ?

- Si un paiement a déjà été effectué, faites opposition immédiatement auprès de votre banque.
- Si un accès à distance a été accordé, changez tous vos mots de passe.
- Signalez les faits sur **internet-signalement.gouv.fr**.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Sites administratifs

En quoi consiste l'arnaque ?

- Des sites imitant l'apparence des services publics officiels (couleurs bleu-blanc-rouge, logo Marianne etc.) proposent des démarches administratives payantes pour des services normalement gratuits : permis de conduire, carte grise, extrait de casier judiciaire, acte de naissance, etc. Certains sites volent également les données personnelles ou bancaires transmises.

Comment se protéger ?

- Sachez que toutes les démarches administratives officielles sont accessibles gratuitement via **service-public.fr**.
- Méfiez-vous des sites qui apparaissent en tête de moteur de recherche sous forme d'annonces payantes.
- Ne communiquez vos coordonnées bancaires que si vous êtes certain de l'identité du site.

Que faire si vous êtes victime ?

- Contactez votre banque pour contester le paiement.
- Signalez le site frauduleux sur **signal.conso.gouv.fr**.

- Si des données personnelles ont été captées, signalez-le à la **CNIL**.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Appel aux dons et fausses cagnottes

En quoi consiste l'arnaque ?

- Des escrocs créent de fausses associations ou de fausses cagnottes en ligne, souvent liées à une actualité dramatique ou une cause populaire, pour détourner la générosité du public. Les victimes donnent de bonne foi mais les fonds ne bénéficient jamais à la cause annoncée.

Comment se protéger ?

- Privilégiez les associations reconnues d'utilité publique et vérifiez leur statut dans le Journal Officiel.
- Méfiez-vous des cagnottes anonymes ou lancées précipitamment après un événement médiatique.
- Vérifiez les informations sur l'organisme avant tout don (adresse, numéro d'immatriculation).
- Assurez-vous que la plateforme de collecte est enregistrée auprès de l'**ACPR**.

Que faire si vous êtes victime ?

- Signalez la cagnotte suspecte à la DGCCRF sur **signal.conso.gouv.fr** et à l'ACPR sur **abe-infoservice.fr**.
- Contactez votre banque pour tenter de récupérer les sommes versées.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.