MONTASTRUC
La Conseillère

Cybersécurité

Guide de prévention contre les arnaques

Arnaques en ligne : comment s'en protéger ?

L'essor de l'intelligence artificielle expose les particuliers à des fraudes toujours plus nombreuses et toujours plus sophistiquées. Aucun profil n'est épargné : les arnaques en ligne frappent les Français de tous âges et de tous milieux. Pour les déjouer, une vigilance de chaque instant s'impose.

Hameçonnage (phishing)

De quoi s'agit-il ?

- L'hameçonnage est la menace numérique la plus répandue en France. L'escroc vous contacte par SMS, courriel ou appel téléphonique en se faisant passer pour un organisme de confiance (banque, assurance maladie, administration fiscale, opérateur téléphonique etc.) afin de récupérer vos identifiants, vos mots de passe ou vos données bancaires.

Comment l'éviter ?

- Sachez qu'aucun organisme légitime ne vous demandera vos identifiants et mots de passe personnels.
- Examinez attentivement l'adresse mail de l'expéditeur avant de cliquer sur un lien reçu par message (une seule anomalie suffit à déceler l'arnaque).
- Contrôlez l'URL du site caractère par caractère : le nom de domaine doit être rigoureusement identique à celui du site officiel.
- Au moindre doute, tapez vous-même l'adresse du site officiel dans votre navigateur plutôt que de suivre le lien reçu.

Que faire si vous êtes victime ?

- Modifiez sans attendre les mots de passe compromis.
- Prévenez votre banque si vous avez communiqué vos données bancaires à l'escroc.
- Signalez le message frauduleux sur signal-spam.fr ou par SMS au 33700.
- Rendez-vous sur cybermalveillance.gouv.fr pour obtenir un accompagnement sur mesure.
- Portez plainte auprès d'un commissariat ou d'une gendarmerie.

Usurpation d'identité

De quoi s'agit-il ?

- Munis de vos données personnelles (pièce d'identité, coordonnées, RIB), des fraudeurs ouvrent des comptes bancaires, contractent des crédits ou commettent des délits en votre nom. Ces informations proviennent le plus souvent d'un document dérobé, d'une fuite de données ou d'une campagne d'hameçonnage.

Comment l'éviter ?

- N'envoyez jamais la copie d'une pièce d'identité sans y inscrire au préalable la date et l'usage auquel elle est destinée.
- Choisissez des mots de passe solides et distincts pour chaque service en ligne.
- Passez en revue régulièrement vos relevés de compte bancaire.
- Déchirez ou broyez systématiquement vos documents personnels avant de les mettre à la poubelle.

Que faire si vous êtes victime ?

- Alertez sans délai votre banque ainsi que l'ensemble des 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.

Boutiques en ligne frauduleuses

De quoi s'agit-il ?

- 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 l'éviter ?

- Contrôlez systématiquement l'identité du vendeur : adresse postale, numéro de téléphone, mentions légales.
- Choisissez un moyen de paiement qui vous laisse un recours en cas de litige : la carte bancaire, plutôt que le virement notamment.
- Consultez les avis d'autres acheteurs sur des plateformes indépendantes.
- Méfiez-vous des offres soumises à un compte à rebours ou des prix anormalement bas.

Que faire si vous êtes victime ?

- Appelez sans attendre votre banque pour contester l'opération et en réclamer le remboursement.

- Rassemblez et conservez l'ensemble des 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.

Escroquerie au placement financier

De quoi s'agit-il ?

- L'objectif de l'escroc est ici de voler l'épargne d'un particulier en lui faisant miroiter des gains élevés sur des placements présentés comme sans risque (actions, cryptomonnaies, devises, etc.). Le premier contact avec la victime se noue souvent sur un réseau social, une messagerie instantanée, un forum ou même un site de rencontre. Un site vitrine d'allure très professionnelle rassure généralement la victime. Le jour où l'épargnant souhaite le retour de ses fonds, l'escroc devient injoignable (l'escroc réclame parfois le paiement préalable de prétendues taxes pour soutirer davantage d'argent à sa victime).

Comment l'éviter ?

- Fuyez toutes les offres qui proposent des rendements élevés avec peu ou pas de prise de risque.
- Assurez-vous que l'intermédiaire financier est bien agréé en interrogeant les registres officiels de Regafi ou de l'Orias.
- Consultez les listes noires de l'AMF et de l'ACPR sur abe-infoservice.fr.
- Documentez-vous sur des sites fiables tels que Finance Héros. Finance Héros propose notamment un comparatif des banques en ligne, un comparatif des PEA, un comparatif des PER et un comparatif des meilleurs livrets du marché. Finance Héros vous propose également une sélection des meilleures assurances-vie du moment ainsi qu'un guide pour investir dans la crypto monnaie en toute sécurité.
- Ne souscrivez ni sous la pression ni dans la précipitation.

Que faire si vous êtes victime ?

- Rompez tout contact avec l'escroc et restez méfiant face aux offres d'aide pour récupérer votre argent : il s'agit souvent d'une seconde escroquerie.
- Contactez votre banque pour tenter de récupérer vos fonds et conservez toutes les preuves à votre disposition.
- Faites un signalement auprès de l'AMF ou à l'ACPR.
- Déposez une plainte auprès d'un commissariat ou d'une gendarmerie.

Faux support technique

De quoi s'agit-il ?

- Une alerte alarmante s'affiche et paraît bloquer votre ordinateur. Le message vous presse alors d'appeler sans délai un prétendu service d'assistance (Microsoft, Apple,

etc.). À distance, un faux technicien prend la main sur votre machine et vous facture, souvent au prix fort, une réparation entièrement fictive.

Comment l'éviter ?

- Sachez qu'un véritable service d'assistance ne vous réclamera jamais d'argent de cette manière.
- N'appelez en aucun cas le numéro indiqué sur ce type de message.
- Si votre navigateur semble bloqué, redémarrez votre ordinateur.
- Ne permettez jamais à un inconnu de prendre le contrôle de votre appareil à distance.

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.
- Rapportez les faits sur internet-signalement.gouv.fr.
- Déposez plainte auprès du commissariat ou de la gendarmerie de votre secteur.

Faux sites administratifs

De quoi s'agit-il ?

- 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 l'éviter ?

- Rappelez-vous que toutes les démarches administratives officielles sont accessibles gratuitement depuis le site service-public.gouv.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.

Faux appels aux dons et cagnottes frauduleuses

De quoi s'agit-il ?

- 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 l'éviter ?

- 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.
- Avant tout versement, vérifiez que l'organisme est légitime (adresse et numéro d'immatriculation notamment).
- Vérifiez que la plateforme de collecte est enregistrée auprès de l'ACPR.

Que faire si vous êtes victime ?

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