Entraide Collonges

Cyberattaques en France

Comprendre les fuites de données et savoir réagir

Atelier de 45 minutes· Informations à jour le 2 novembre 2026



Introduction

A ce stade on parle de cyberattaques réussies non pas contre vous mais contre des sites du gouvernement ou privés.

> « Quand vous entendez parler d'une cyberattaque, qu'est-ce qui vous inquiète le plus ? »

Toutes les questions sont bienvenues.

Cinq mots pour s'y retrouver

Cyberattaque
Action malveillante contre un système informatique.

Fuite de données
Informations personnelles divulguées ou volées.

Hameçonnage
Faux message ou appel pour obtenir une information.

Rançongiciel
Logiciel qui bloque des fichiers et réclame une rançon.

Usurpation d'identité : se faire passer pour une autre personne grâce à ses informations.

Sources : CNIL, 18 mars 2024 · Cybermalveillance.gouv.fr, mis à jour le 7 mai 2026 · Rançongiciel, mis à jour le 10 juillet 2026

Trois incidents proches du quotidien

Intermarché Drive · courses
Date de l'accès non autorisé non publiée ; **confirmé publiquement le 3 août 2026**.

DGFiP · impôts
Accès illégitimes de juin à août ; vol connu les 12–13 août ; **communiqué le 14 août 2026**.

Carrefour · achats
Incident chez un prestataire, date d'intrusion inconnue ; **information publiée le 30 septembre 2026**.

Sources : TF1 Info/AFP · DGFiP · Le Monde Informatique

DGFiP : des données fiscales volées

Ce qui est confirmé

Des accès illégitimes ont permis de consulter et d'extraire des données d'identité, de contact et de situation fiscale.

Point essentiel

Selon la DGFiP, les espaces personnels et professionnels sur **impots.gouv.fr** n'ont pas été compromis.

L'annonce de cette fuite ne signifie pas que tous les contribuables sont concernés. En cas de doute, vérifiez auprès de la DGFiP par un canal officiel.

Sources : DGFiP, 14 août 2026 · ANSSI, 29 septembre 2026

Intermarché Drive : les données de clients

Ce qui est confirmé

Accès non autorisé à des données du service de courses en ligne : identité, téléphone, adresse, naissance, carte de fidélité et certaines commandes.

Ce qui est établi au 3 août

287605 clients identifiés et informés par l'enseigne.

Selon elle : ni données bancaires, ni mots de passe, ni adresses électroniques exposés.

L'enquête se poursuit pour savoir si d'autres clients étaient concernés.

Source : Groupement Mousquetaires à l'AFP, repris par TF1 Info, 3 août 2026

Carrefour : un prestataire touché

Ce qui est confirmé

Carrefour a alerté certains clients après un incident de sécurité chez un prestataire.

Nom, prénom, adresse électronique et téléphone ont été exposés.

Ce qui reste inconnu

La date de l'intrusion et le nombre de clients touchés ne sont pas publiés.

Selon Carrefour, ni mots de passe ni données bancaires exposés ; aucun indice d'intrusion dans ses systèmes.

Source : Le Monde Informatique, 30 septembre 2026, d'après l'alerte de Carrefour

Une fuite peut rendre un faux message crédible

1. Des données

Nom, adresse ou organisme connu.

→

2. Un prétexte

« Nous connaissons votre dossier. »

→

3. Une demande urgente

Cliquer, payer ou donner un code.

> Ce n’est pas une conséquence automatiquement constatée dans ces trois incidents mais c'est fort possible à l'avenir que ce soit utilisé.

Source : CNIL, « Fuite ou vol de données », 18 mars 2024

Données personnelles : quel niveau de prudence ?

⚠ **FAIBLE · 1/3**

Nom, prénom, âge, ville
Un faux message peut devenir plus personnel. **Si possible :** pseudonyme.

⚠ ⚠ **MOYEN · 2/3**

Date de naissance, courriel, adresse postale
Leur croisement facilite l'identification. **Si possible :** âge, courriel dédié, point relais.

⚠ ⚠ ⚠ **ÉLEVÉ · 3/3**

Carte d'identité, avis d'imposition, fiche de paie, justificatif de domicile, RIB
Risque d'usurpation d'identité. **Avant l'envoi :** destinataire vérifié et canal officiel, si possible version filigrane ou à usage temporaire.

Carte d'identité : **France Identité** remplace la photocopie par un justificatif à usage unique.
Autres documents : **FiligraneFacile** limite la réutilisation d'une copie. Un scan déjà envoyé n'est pas annulé.

Sources : Cybermalveillance.gouv.fr, 23 septembre 2026 · France Identité · FiligraneFacile

Usurpation d'identité : trois chiffres à situer



4e escroquerie la plus répandue en **2021**, selon France Identité.



Hausse des **fraudes à l'identité** entre **2019 et 2020**.



Des Français ont été victimes d'**usurpation d'identité** ; période non précisée.

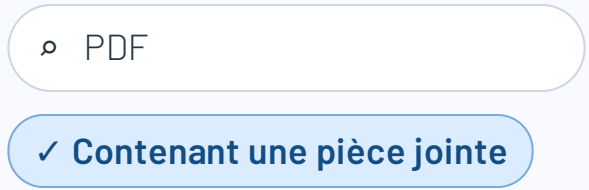
Ces chiffres portent sur des mesures différentes, datent de 5 ans et surtout sont en forte progression chaque année depuis 10 ans.

Source et illustrations : France Identité, « Le justificatif d'identité à usage unique » · date de publication non indiquée · consulté le 2 novembre 2026.

Exercice : utilisation de Filigrane Facile

1. Retapez l'adresse : **filigrane.beta.gouv.fr**
2. Dans Gmail, cherchez **PDF**, puis cliquez sur **« Contenant une pièce jointe »**.
3. Choisissez un PDF reçu d'un expéditeur connu. **Téléchargez-le.**
4. Sur Filigrane Facile, sélectionnez le fichier et saisissez : **« A n'utiliser que pour la société XYZ »**.
5. Cliquez sur **« Ajouter le filigrane »**, puis téléchargez le nouveau PDF.

REPÈRE VISUEL · GMAIL (SCHÉMA)



Selon la version de Gmail, un filtre « PDF » peut aussi apparaître.

Sources : Aide Gmail, recherche et filtres · FiligraneFacile, service officiel

Exemple fictif : le faux message Netflix

EXEMPLE FICTIF · SMS INVENTÉ, PAS UN MESSAGE DE NETFLIX

« M. Guillaume Arluison, sur votre télévision, votre compte Netflix nécessite un code tous les 30 jours. Veuillez taper 143254 sur https://lnk.me/xoEf34 »

Le prénom et le nom rendent-ils le message fiable ? Que feriez-vous ?

> Indices : urgence · code demandé en réponse · règle des « 30 jours » non confirmée. Vérifier dans l'application Netflix.

Source : Centre d'aide Netflix, vérification d'une TV hors du foyer

Exemple fictif : « votre colis n'a pas été livré »

EXEMPLE FICTIF · SMS OU COURRIEL INVENTÉ

« Nous sommes passés vous livrer un colis, mais vous étiez absent. Choisissez un nouveau créneau et réglez 1,95 € de frais de relivraison : https://lnk.me/xNGhEj3a »

Et si vous attendez vraiment un colis ?

> Vérifiez le suivi depuis la commande (soit email de quand vous avez commandé SOIT sur le site ou l'application du vendeur), ouvert par vous-même.

Source : Cybermalveillance.gouv.fr, « L'hameçonnage à la livraison de colis », mis à jour le 26 août 2026

Face à un message douteux : trois gestes

1. Faire une pause. Ne pas cliquer ni répondre sous la pression.

2. Garder ses secrets. Ne donner ni mot de passe, ni code reçu par une autre méthode que le fonctionnement habituel, ni validation bancaire.

3. Vérifier soi-même. c'est à dire inverser : je ne clique pas mais je vais manuellement sur le site par le favori ou en tapant l'adresse ou l'application, indépendamment du "raccourci" du message.

Sources : CNIL, 18 mars 2024 · Cybermalveillance.gouv.fr, mis à jour le 7 mai 2026

Si vous avez cliqué ou transmis quelque chose

Vous avez seulement ouvert une page ? Fermez-la sans rien saisir. En cas de doute, demandez conseil.

Vous avez donné un mot de passe ou un code ? Changez le mot de passe concerné ; contactez aussitôt le service ou la banque par son canal officiel.

Vous avez donné des données bancaires ? Contactez immédiatement votre banque pour faire opposition ou sécuriser le compte.

N'hésitez pas à vous entraider : écrivez sur le groupe WhatsApp de Entraide, quelqu'un vous répondra (si possible avec capture d'écran).

Gardez le message et les captures ; Cybermalveillance.gouv.fr peut vous orienter. Si une fraude est constatée, portez plainte.

Six réflexes à retenir

1. **Prendre le temps** face à une demande urgente.
2. **Vérifier par soi-même** y aller manuellement ou par un canal officiel.
3. **Garder secrets** mots de passe et codes de validation.
4. **Utiliser des mots de passe différents** et la double authentification si disponible.
5. **Faire les mises à jour et des sauvegardes** régulièrement.
6. **Demander** un autre avis avant, ou un conseil après.

Sources : ANSSI, « 10 règles d'or » · CNIL, 18 mars 2024

Sources et ressources utiles

TF1 Info/AFP · Intermarché Drive
3 août 2026

DGFiP · Vol de données
14 août 2026, modifié le 14 septembre

ANSSI · Rapport DGFiP
29 septembre 2026

Le Monde Informatique · Carrefour
30 septembre 2026

Netflix · Vérifier une TV hors du foyer
Date de publication non indiquée

France Identité · Justificatif à usage unique
11 mai 2022, modifié le 21 novembre 2023

FiligraneFacile · Ajouter un filigrane
Date de publication non indiquée

Aide Gmail · Effectuer une recherche
Date de publication non indiquée

Cybermalveillance.gouv.fr · Livraison de colis
31 août 2022, mis à jour le 26 août 2026

Cybermalveillance.gouv.fr · Usurpation
4 octobre 2021, mis à jour le 23 septembre 2026

CNIL · Donnée personnelle
Date de publication non indiquée

CNIL · Fuite ou vol de données
18 mars 2024

Cybermalveillance.gouv.fr · Hameçonnage
10 janvier 2020, mis à jour le 7 mai 2026

Cybermalveillance.gouv.fr · Rançongiciel
2 mars 2022, mis à jour le 10 juillet 2026

ANSSI · 10 règles d'or
Date de publication non indiquée

Questions ? Informations vérifiées le 2 novembre 2026.