

Mesures essentielles

Pour assurer sa sécurité numérique

L'CAPIAL
MAISON D'ANIMATION • SAINT-JUERY





Décembre 2025

.@REDbySFR @SFR (données clients : nom, email, adresse, téléphone)
.@Sports_gouv (Pass’Sport : 3,5 millions de foyers) ParaShop (données d’identité et adresses)
.@SoundCloud (≈ 20 % des utilisateurs)
.@Pornhub (données d’analytics liées à certains comptes Premium : activité/consultation/recherches)
.@Interieur_Gouv (“un certain nombre de fichiers”)
.@FFCyclisme (≈ 1 million d’adhérents)
.@UFOLEP (UFOLEP / Exalto : données d’identité et de contact)
.@Cuisinella (données de contact) Schmidt France (données de contact)
.@FFHandball (GestHand : données d’identité et contact)
.@leroymerlinfr (données de fidélité et de contact)
.@FranceTravail (≈ 1,6 million de jeunes)

Novembre 2025

.@FFF (Footclub : données de licence)
.@AG2RLAMONDIALE (AG2R / Itelis : données de santé + NIR)
.@MalakoffHumanis (Itelis : demandes de devis optique)
.@Michelin (ransomware / données d’entreprise)
.@ColisPrive (données de contact)
.@Alfortville_94 (RDV360 : données de contact) Synbird_com (données de rendez-vous) Resana Interieur_Gouv (données non précisées)
.@Urssaf (Pajemploi : ≈ 1,2 million / IBAN + NIR)

Le rapport annuel sur la cybercriminalité 2025 (CNIL) indique que plus de **348 000 atteintes numériques ont été enregistrées**, soit une **hausse de 74 % en cinq ans**, bien que le chiffre réel dépasse probablement ce nombre car de nombreuses victimes ne portent pas plainte. En 2025, près de **90 % des utilisateurs commettent des erreurs courantes en matière de sécurité numérique**, ce qui aggrave la vulnérabilité des particuliers

Août 2025

.@auchan_france (fidélité + contact)
@GoogleFR (2,25 millions de données)FranceTravail (contact + identifiants)
.@optic2000 (NIR, date de naissance, n° client)
.@airfrance (Flying Blue + contact)
.@bouyguestelecom (≈ 6,4 millions / IBAN)
.@Pandora_FR (noms + emails)

Juillet 2025

.@orange_france (données non précisées)
@LouisVuitton (achats + préférences)
.@Sorbonne_Univ_ (données employés + familles)
@CNFPT (≈ 34 000 / pièces d’identité, IBAN, CV)
@unss (≈ 8 millions d’élèves)

Avril 2025

.@cerballiance (données non précisées)
@CarrefourFrance (Carrefour Mobile : ≈ 64 000 / mots de passe + passeports)
easycashfr (noms + dates de naissance)
ALAIN_AFFLELOU (données de contact + commerciales)
@HertzFR (permis, passeports, CB) Harvest_Groupe (≈ 50 000 personnes + 5 000 entreprises)
UTWIN_Assurances (identité + contact)
Reporterre (données de contact)

Mars 2025

.@MAIF (MAIF & BPCE : patrimoine, revenus, situation familiale)
Autosur (Autosur & Diagnosur : plaques + contact)
Intersport_FR (≈ 3,4 millions : transactions + fidélité)
DirectAssurance (données non précisées)
Laforet_france (dossiers locataires, pièces d’identité, RIB)
LaPosteBusiness (identité + contact)

Février 2025

.@EDFofficiel (EDF DPIH : plans maintenance centrales)
École Nationale de la Sécurité (≈ 30 000 / NIR + diplômes)
Département 59 (Nord Emploi : dossiers RSA, CAF, CV)
FFF (ITAC : justificatifs d’identité + photos)
sdis86 (logins + mots de passe hachés)
SportDecouverte (488 023 comptes)
Mutuelle Motards (données de contact)
Caisse des dépôts (≈ 70 000 personnes)
Chronopost (signatures + coordonnées)
KingJouet_fr (détails de commandes)
Vorwerk FR (Espace-Recettes[.]fr : données Thermomix)

Février 2025

assoAIDES (données de santé, NIR, IBAN)
FFME_officiel (808 881 comptes)
Leclerc (dossiers de primes + montants)
FFF Tir à l’Arc (ITAC : 625 434 comptes)
FFForce_ (ITAC : 64 512 comptes)
FFRollerSkate (ITAC : données de licence)
KiabiFrance (IBAN / credential stuffing)

Source : <https://bonjourlafuite.eu.org/>

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques ? Quelques bonnes pratiques essentielles à adopter pour assurer sa sécurité numérique.



1



Utiliser des mots de passe différents

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.



Utiliser un mot de passe long et complexe

il est admis qu'un bon mot de passe doit comporter au **minimum 12 signes** mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Protéger ses accès avec des mots de passe solides

Combien de temps faut-il à un pirate pour trouver votre mot de passe 2025

12 x RTX 5090 | bcrypt (10)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	57 minutes	2 heures	4 heures
6	Instantané	46 minutes	2 jours	6 jours	2 semaines
7	Instantané	20 heures	4 mois	1 an	2 ans
8	Instantané	3 semaines	15 ans	62 ans	164 ans
9	2 heures	2 ans	791 ans	3k ans	11k ans
10	1 jour	40 ans	41k ans	238k ans	803k ans
11	1 semaine	1k ans	2M ans	14M ans	56M ans
12	3 mois	27k ans	111M ans	917M ans	3Md ans
13	3 ans	705k ans	5Md ans	56Md ans	275Md ans
14	28 ans	18M ans	300Md ans	3Bn ans	19Bn ans
15	284 ans	477M ans	15Bn ans	218Bn ans	1Bd ans
16	2k ans	12Md ans	812Bn ans	13Bd ans	94Bd ans
17	28k ans	322Md ans	42Bd ans	840Bd ans	6Tn ans
18	284k ans	8Bn ans	2Tn ans	52Tn ans	463Tn ans



Hive Systems

> hivesystems.com/password

1

Protéger ses accès avec des mots de passe solides



Utiliser un mot de passe impossible à deviner

- . La méthode des premières lettres : *Un tiens vaut mieux que deux tu l'auras* --> **ltvmQ2tl'A**
- . La méthode phonétique : *J'ai acheté huit CD pour cent euros cet après-midi* --> **ght8CD%E7am**



Ne jamais communiquer son mot de passe à un tiers

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone.



Changer son mot de passe au moindre soupçon

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas.



Activer la "double authentification" si possible

Pour renforcer la sécurité des accès, de plus en plus de services proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, sous forme de code provisoire reçu par SMS ou par courrier électronique via une application ou une clé spécifique que vous contrôlez.

1



Ne pas utiliser ses mots de passe sur un ordi partagé

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « **navigation privée** » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et **n'enregistrez jamais vos mots de passe dans le navigateur**. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

Protéger ses accès avec des mots de passe solides



Utiliser un gestionnaire de mots de passe

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. **Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès.** Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès.

KeePassXC : <https://keepassxc.org/>
Bitwarden : <https://bitwarden.com/fr-fr/>

2



Effectuer des sauvegardes régulières

Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données.



Choisir une solution de sauvegarde adaptée

Il existe des solutions gratuites ou payantes qui répondent à différents besoins. Identifiez-les et déterminez quelles sont les fonctionnalités attendues, l'espace de stockage requis et la facilité d'utilisation de la solution. Sachez qu'il est également possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe, une clé USB, etc.

Sauvegarder ses données régulièrement



Déconnecter le support de sauvegarde après utilisation

Si vous êtes victime d'un virus comme un rançongiciel et que votre sauvegarde est connectée à votre ordinateur ou au réseau de votre entreprise, elle peut également être affectée par le programme malveillant qui pourrait la détruire. Déconnectez votre support de sauvegarde de votre ordinateur ou de votre réseau informatique.



Tester régulièrement les sauvegardes

Parfois, le processus de sauvegarde ne s'effectue pas correctement. Aussi, assurez-vous régulièrement que votre sauvegarde fonctionne, par exemple, en la copiant dans le système original.

3

Appliquer les mises à jour sur tous vos appareils



Mettre à jour sans tarder logiciels et matériels

Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Il est **primordial de réaliser les mises à jour** de vos équipements dès qu'elles sont disponibles.



Activer les mises à jour automatiques

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur.



Mettre à jour uniquement depuis les sites officiels

Seuls les dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées. À l'installation de vos mises à jour, **soyez attentif aux éventuelles conditions d'utilisation** ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

2 exemples de failles (parmi des milliers d'autres)

. Des cybercriminels ont réussi à dérober des données confidentielles d'un casino grâce au thermomètre connecté présent dans un aquarium de l'établissement.

. Un utilisateur utilise son navigateur non mis à jour, un site malveillant utilise une faille et installe un malware. Vol des mots de passe, prise en main à distance de l'appareil et compte en banque vidé.

4

Quelques autres préconisations



Utiliser un antivirus

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que **les antivirus de vos équipements sont bien à jour** et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

Antivirus (gratuits)

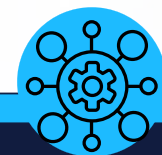
Avira Free Security : <https://www.avira.com/fr/free-security>

Bitdefender Antivirus Free : <https://www.bitdefender.com/fr-fr/consumer/free-antivirus>



Eviter les réseaux wifi publics ou inconnus

En mobilité, privilégiez la connexion de votre abonnement téléphonique (4G ou 5G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et **peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles** (mots de passe, numéro de carte bancaire...). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).



Se protéger contre le hameçonnage

. Si un courriel vous semble douteux, **ne cliquez pas sur les pièces jointes** ou sur les liens qu'il contient !
. Si vous réglez un achat en ligne et que vous devez ainsi fournir des informations relatives à votre carte bancaire, **vérifiez que vous êtes sur un site web sécurisé dont l'adresse commence par « https »** (cadenas).

IA et vie privée

De plus en plus d'entreprises utilisent les données personnelles de leurs utilisateurs pour entraîner des modèles d'IA. La CNIL propose des solutions pour s'y opposer pour les principales plateformes.



IA, vie privée et agents conversationnels



Je vais en voyage en Italie du sud, que voir ?

Colonne de gauche
moteur de recherche, de droite IA

Je vais en voyage en Italie du sud, que voir ?

Tout Images Vidéos Actualités Plus Search Assist Duck.ai

Toploc
https://toploc.com › blog › europe › visiter-italie-du-sud

Les 13 choses à voir et à faire pour visiter l'Italie du Sud

12 nov. 2025 · Quelles sont les choses à voir et à faire pour visiter l'Italie du Sud ? Démarrez votre séjour à Rome puis Tivoli et rendez-vous aux Abruzzes avant de prendre la direction des Pouilles vers Bari, Alberobello et Matera.

LovelyItalyClub.com
https://lovelyitalyclub.com › fr › top-10-des-endroits-a-visiter-dans-le-sud-de-litalie-en-10-jours-fr

Top 10 des endroits à visiter dans le sud de l'Italie en 10 jours

14 oct. 2025 · Ce guide vous emmènera dans une aventure immersive de 10 jours à travers les 10 meilleures destinations touristiques d'Italie, en vous concentrant spécifiquement sur ses joyaux du sud.

Partir.com
https://www.partir.com › Italie › italie-du-sud › lieux-d-interet.html

Le TOP 7 des lieux à voir en Italie du sud. Que voir | Que visiter

31 oct. 2025 · Des atypiques habitations d'Alberobello aux vestiges historiques de Pompéi, en passant par la beauté ensoleillée de Ravello... l'Italie du Sud regorge de lieux à explorer entre nature et culture.

nunkie.fr
https://nunkie.fr › que-faire-et-que-voir-dans-le-sud-de-litalie

Que faire et que voir dans le sud de l'Italie - nunkie.fr

2 juill. 2025 · Ce guide vous propose cinq activités incontournables pour découvrir le Sud italien autrement, à travers des lieux emblématiques et des pratiques locales, chiffres à l'appui.

Comptoir des Voyages
https://www.comptoirdesvoyages.fr › guide › italie-du-sud › que-voir-en-italie-du-sud › 1088

Que voir en Italie du Sud ? | Conseils voyage Italie du Sud

Que voir en Italie du Sud ? Trois mers et un volcan, des îles et des villes, les plus beaux témoignages de la vie antique et l'occasion d'expérimenter la dolce vita ...

re/visiter-italie-du-sud

Je vais en voyage en Italie du sud, que voir ?



Voici quelques incontournables à voir en Italie du Sud :

Pouilles (Puglia)

- **Alberobello** : ses trulli (maisons coniques) classés au patrimoine mondial de l'UNESCO.
- **Lecce** : ville baroque surnommée la "Florence du Sud".
- **Bari** : vieille ville et port historique.
- **Les Grottes de Castellana** : impressionnantes grottes karstiques.

Campanie

- **Naples** : centre culturel et historique, avec son musée archéologique et son port.
- **Pompéi et Herculaneum** : villes antiques fossilisées par l'éruption du Vésuve.
- **Capri** : île paradisiaque avec ses falaises et la Grotta Azzurra.
- **Amalfi et Positano** : côtes spectaculaires, villages colorés accrochés aux falaises.

Calabre

- **Tropea** : vue imprenable sur la mer Tyrrhénienne.
- **La Sila** : massif montagneux avec lacs et forêts.
- **Reggio de Calabre** : musée national avec les Bronzes de Riace.

Basilicate

- **Matera** : Sassi, cité troglodytique classée à l'UNESCO, capitale européenne de la culture en 2019.
- **Policoro** : plage et vestiges arcs.

Laissez Euria rechercher sur le web

+ Automatique



Euria peut faire des erreurs. Infomaniak n'entraîne pas Euria avec vos données.

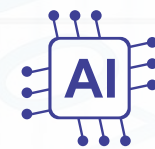
IA, vie privée et agents conversationnels



Google – Gemini

Dans les paramètres de compte

1. Une fois connecté sur le site internet de Gemini, rendez-vous dans l'onglet « Activité ».
2. Parmi les configurations possibles de l'« Activité dans les applications Gemini », sélectionnez « Désactiver et supprimer l'activité ».
3. Dans l'application mobile, le réglage de ces paramètres est accessible en cliquant sur l'icône du profil utilisateur, puis sur « Activité dans les applications Gemini ».



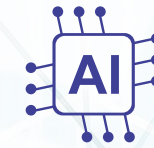
Meta – Instagram / Facebook

Instagram. Se rendre dans "Réglages" puis dans "Centre de confidentialité". Une page s'ouvre avec le message ci-dessus. L'utilisateur doit ensuite cliquer sur le mot "opposer", puis en bas de la page, renseigner son adresse mail associée à ses comptes et un message (facultatif).

Pour ce dernier, vous pouvez copier coller celui-ci :

"Je m'oppose strictement à l'utilisation de mes données personnelles ou publiques présentes sur mes comptes Instagram et Facebook, dans le cadre du développement ou de l'entraînement de l'intelligence artificielle de Meta ou de ses partenaires. Conformément à la législation européenne sur la protection des données (RGPD), je vous demande de respecter mon droit d'opposition. Merci de confirmer la prise en compte de cette demande."

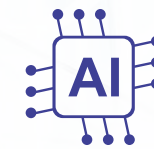
Facebook. Il suffit de se rendre dans "Paramètres et confidentialité", puis "Politique de confidentialité". La même page apparaît, et nécessite la même démarche.



Meta – Cas de WhatsApp

Pour s'opposer à l'utilisation de vos données pour améliorer les modèles de Meta AI lors des interactions avec l'agent conversationnel depuis WhatsApp, il faut remplir un formulaire dédié.

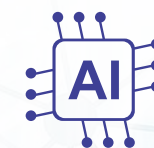
1. Commencez par vous rendre sur lien vers le formulaire de contact.
2. Cochez l'option « Comment formuler une opposition au traitement de mes informations ? ».
3. Puis indiquez que la demande concerne « l'IA par Meta ». Il reste ensuite à compléter le formulaire.



Open AI – Chat GPT

Dans les paramètres de compte

Une fois connecté sur le site internet de ChatGPT ou sur l'application mobile, rendez-vous dans les paramètres de compte, onglet « Gestion des données » puis « Améliorer le modèle pour tous ». Il est ensuite possible de décocher les cases relatives à la collecte de données utilisateur à des fins d'amélioration de modèles d'IA.



Mistral – Le Chat

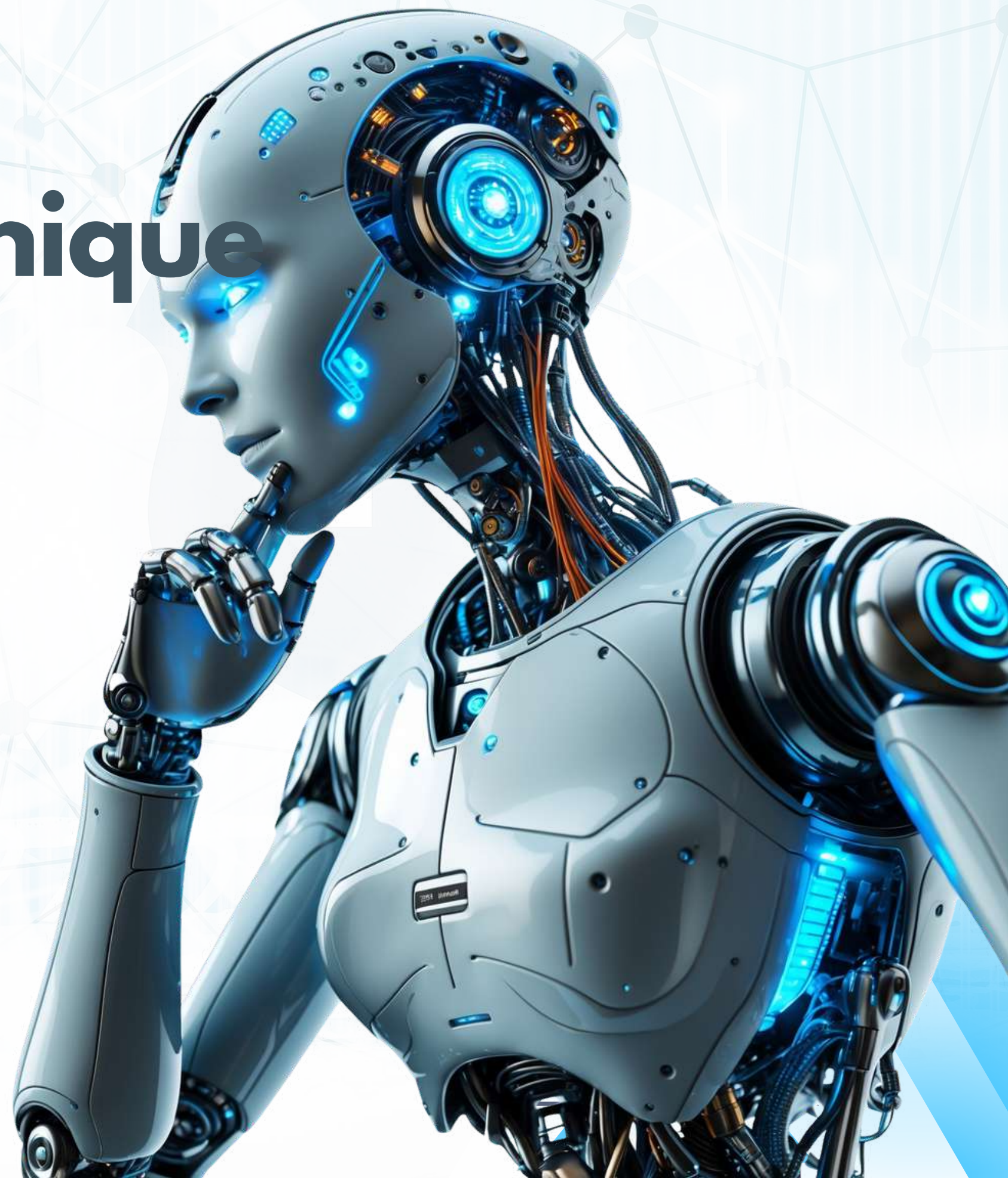
Dans les paramètres de compte

Une fois connecté sur le site internet Le Chat, rendez-vous dans les « Paramètres » du compte, onglet « Préférences » de la section « Le Chat », puis décochez la case « Autoriser l'utilisation de vos interactions pour entraîner nos modèles ».

Euria, l'assistant IA éthique

Cette IA, créée et gérée par une entreprise Suisse, **accessible gratuitement** sans création de compte, **utilise des modèles open source** comme Qwen 3 et promet un **respect strict de la vie privée, sans stockage des données utilisateur ni utilisation de celles-ci pour entraîner des modèles**. Les échanges sensibles, où les données sont **supprimées immédiatement après la conversation**. Elle est également alimentée par de l'énergie renouvelable et valorise la chaleur produite par ses serveurs pour chauffer jusqu'à 6 000 logements à Genève.

<https://www.infomaniak.com/fr/euria>





Le **dispositif 17 Cyber** est un service public d'assistance en ligne gratuit, lancé le 17 décembre 2024, destiné aux victimes de cybermalveillance, qu'elles soient particuliers, entreprises, associations ou collectivités.

Accès au site : **<https://17cyber.gouv.fr/>**

En cas d'urgence, appelez le **17** ou le **112** ou envoyez un SMS au **114** en cas de difficulté à parler ou entendre



Votre adresse de courriel (mail) est-elle compromise ?

Faites le test : **<https://haveibeenpwned.com/>**