



**INTERNET, MOBILES,
RÉSEaux SOCIAUX**



....
**PROTECTION DES DONNÉES
RESPECT de la VIE PRIVÉE**
....

PARLONS-EN !

Je n'ai  

rien **à** 

cacher **Mais vous n'avez pas à tout savoir sur moi** 

A chaque instant,
nos données personnelles
sont exploitées par
les géants du web.

Ils nous espionnent,
ils nous traquent,
ils nous contrôlent.

Ils ont fait de nous des dates,
ce n'est pas une fatalité,

Je reprends le contrôle

DÉCOUVREZ
CE QU'ILS SAVENT SUR VOUS
www.lesusosdesdonnees.fr

Conférence
organisée par l'association Verneuil Détente
en partenariat
avec la municipalité de Verneuil-sur-Vienne

Le 12 Mars 2025 À 20h30

**Au foyer rural de
Verneuil-sur-Vienne**

Empreintes pour tous adultes



Présentation et introduction

L'association Verneuil Détente et sa section «Initiation à l'informatique »



Avec les publications de

- Cybermalveillance.fr
- CNIL
- UFC que Choisir



Avez-vous conscience que vos données ont de la valeur ?

Naviguer sur Internet, utiliser les réseaux sociaux, ne sont pas sans risques !

Les pirates informatiques ne manquent pas d'ingéniosité

pour renouveler leurs arnaques.

Leurs objectifs sont de vous extorquer votre argent, votre identité ...

Via vos données, vos informations déposées dans votre ordinateur, votre smartphone ... ou sur le WEB, votre géolocalisation, vos habitudes, vos préférences sont aussi convoitées !

Mieux connaître les risques, s'informer régulièrement sont déjà les premiers moyens de protection.

Avez-vous consulté déjà les Conditions Générales d'Utilisation des réseaux sociaux ?

Avez-vous confiance en cliquant sur les liens des mails de votre banque, des services publics, de vos services d'abonnements (EDF, bibliothèque, ...) ?

Avez-vous adapté vos paramètres de confidentialité sur vos PC, ... ?

oui vous pouvez le faire ! 🤔



Protéger sa vie privée ?

Je n'en vois pas l'intérêt, je n'ai rien à cacher ! 😲

C'est quoi d'ailleurs la vie privée sur le net ?

On pourrait dire que c'est l'ensemble des activités qui relève de notre intimité par opposition à la vie publique.

Ce sont toutes les choses auxquelles on attache des sentiments spéciaux et personnels, nos secrets, nos désirs, nos envies, nos opinions, tout ce qui nous définit un peu plus en tant qu'être unique et que l'on veut garder pour soi, sans que cela ne se sache à l'extérieur, dans la vie publique. 😊

C'est à chacun d'estimer le degré de privation qu'il veut donner à sa vie privée.

Les atteintes à la vie privée sur internet revêtent plusieurs formes :

Le droit à l'image : La diffusion d'images, de vidéos sans accord écrit préalable des personnes reconnaissables peut entraîner de lourdes conséquences.

Le secret de correspondance : partager un écrit sur internet sans l'accord de son auteur est répréhensible.

Le morphing : transformer, détourner une image avant de la publier sur internet est considéré comme une atteinte à la vie privée.

Eh bien... en fait si, nous avons beaucoup de choses à cacher ! 😊

En vous dévoilant publiquement, vous êtes plus vulnérable au monde extérieur :

Vous vous exposez à des rumeurs, de la diffamation et une violation de votre... intimité. 😞

Lorsque des sites ou des 'pirates' collectent vos données personnelles (photos, sites fréquentés, communications...)

Vous ne le voyez pas, ne le sentez pas, ni ne l'entendez. C'est quasiment imperceptible.

Vous pourrez éventuellement vous en apercevoir en bout de course, lorsque le mal sera fait

(usurpation d'identité avec fausses déclarations, refus d'un poste à cause de propos ou de photos douteuses...).

C'est là toute la difficulté :

Avoir conscience que même si vous ne le ressentez pas,

le danger existe.



Où laissez-vous des informations sur vous sur internet ?



Sur les **réseaux sociaux** : quand vous publiez une photo, commentez un message, regardez une vidéo...



Dans un **moteur de recherche** : quand vous tapez des mots clés



Sur un **site internet** : quand vous visitez des pages, lisez un article...



Dans un **formulaire en ligne** pour créer un compte ou faire un achat : quand vous écrivez votre nom, prénom...



Sur une **application mobile** : quand vous l'autorisez à vous "géolocaliser" (c'est à dire, savoir où vous êtes).

Je tourne 7 fois ma souris avant de publier !

Où laissez-vous des informations sur vous sur internet ?

UNE JOURNÉE TYPE EN LIGNE

Au lever, vous demandez à votre assistant vocal de vous lire vos derniers courriers électroniques pendant que vous vous habillez pour vous rendre au travail. Dans les transports en commun, vous vous rendez sur une plateforme de *microblogging* avant de consulter un site d'information en ligne renommé. Sur le chemin, vous vous arrêtez prendre une tasse de café et en profitez pour publier une photo de votre petit-déjeuner en « taguant » l'établissement dans lequel vous vous trouvez sur votre réseau social préféré. Durant la pause déjeuner, vous vous rendez sur un site d'e-commerce afin de rechercher une nouvelle paire de lunettes de ski pour votre week-end à la montagne avant de vous rendre sur votre réseau social pour partager vos plans avec vos amis.

Il ne s'agit que d'une poignée de services, mais les données relatives à ces activités et associées à votre profil ont potentiellement été collectées non pas par une dizaine d'acteurs avec lesquels vous avez eu une interaction en ligne mais par plus d'une centaine d'entreprises différentes en l'espace d'une journée.

Si les sites web et les applications avec lesquels vous interagissez sont visibles, d'autres sociétés peuvent suivre vos activités et collecter des données relatives à votre navigation en ligne sans que cela ne soit nécessairement évident pour vous, pour vous afficher de la publicité. Plus tard dans la journée, vous commencez à voir des messages sponsorisés sur votre plateforme de *microblogging* à propos de week-ends à la montagne, des annonces publicitaires sur votre réseau social pour les lunettes de ski que vous avez cherchées et des suggestions de nouveaux cafés à découvrir près de votre lieu de travail.

Il ne s'agit pas de coïncidences, mais bien du résultat de la collecte de vos données de navigation et de géolocalisation.

Pourquoi ces informations sont-elles précieuses ... pour les autres ?

Ces informations sont précieuses car elles permettent à des entreprises (réseaux sociaux, moteurs de recherche, sites, applications...) de savoir qui vous êtes et ce qui vous intéresse pour vous faire acheter.

Comment les entreprises utilisent-elles ces informations ?

- 1 Certaines entreprises, comme Google et Facebook, à qui vous avez donné des centaines d'informations sur vous, vous montrent des publicités qui correspondent à vos goûts sur les sites que vous visitez et sur Facebook. D'autres entreprises les paient pour montrer leurs publicités aux personnes intéressées. On appelle ça des **publicités "ciblées"**.
- 2 D'autres entreprises se servent de ces informations pour **vous montrer et vous faire acheter des objets qui ressemblent à ce que vous aimez** chaque fois que vous retournez sur leurs sites.

Et n'oublions pas le piratage de compte en ligne

La prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime.

Il représente la seconde cybermenace la plus rencontrée tant par les professionnels que les particuliers.

On ne peut protéger que ce que l'on connaît !

Qu'est-ce qu'une donnée personnelle ?

Toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne physique peut être identifiée selon la CNIL (commission Nationale informatique et libertés)

Directement , ex. : nom et prénom

Indirectement, ex. : un numéro d'adhérent, un numéro de téléphone

ou de plaque d'immatriculation, le numéro de sécurité sociale, une adresse postale ou courriel,
mais aussi la voix ou la photo.

*En revanche, des coordonnées d'associations ou d'entreprises par exemple, avec l' adresse postale,
le numéro de téléphone de son standard, un courriel de contact générique ,...
ne sont pas des données personnelles.*

On ne peut protéger que ce que l'on connaît ! Et les données sensibles ?

Elles sont encore plus personnelles, qualifiant la personne :

La prétendue origine raciale ou ethnique,

Les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale.

Elles comprennent également **les données de santé**, génétiques, biométriques, etc.

L'utilisation de ces données est, par principe, interdit

sauf cas limitatifs prévus par l'article 9.2. du RGPD ou Règlement Général de protection des données,

Parmi ces exceptions, on retrouve le consentement explicite de la personne

Le consentement est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le RGPD impose que ce consentement soit libre, spécifique, éclairé et univoque. Les conditions applicables au consentement sont définies aux articles 4 et 7 du RGPD.

L'article 9 alinéa premier du code civil stipule que « chacun a droit au respect de sa vie privée ». Votre vie privée englobe votre image, votre voix, votre situation de famille, vos opinions politiques ou vos croyances religieuses. Elle peut concerner aussi la diffusion d'images d'un de vos biens (mobiliers ou immobiliers).

Chacun doit respecter votre liberté de mener votre vie comme vous l'entendez. Vous avez aussi le droit de vous opposer à la révélation d'éléments relevant de votre sphère privée.

Car toute publication de données personnelles doit être faite avec le consentement des personnes concernées.

On ne peut protéger que ce que l'on connaît !

ATTENTION

L'identification d'une personne physique peut être réalisée par un croisement d'un ensemble de données.

Exemples :

- une enquête par questionnaire auprès des adhérents d'une association sportive peut, même lorsque les noms et prénoms ne sont pas indiqués, contenir des réponses qui peuvent permettre de retrouver l'identité des personnes lorsqu'elles sont combinées les unes avec les autres.
- la collecte des informations relative à l'âge, au sexe, à la pratique d'un sport à tel niveau au sein de telle ville est susceptible de révéler l'identité de la personne.



On ne peut protéger que ce que l'on connaît ! Vous devez garder le contrôle

L'utilisation de vos données est encadré par la loi informatique et libertés(1978) et le Règlement Général de Protection des Données (2018)

Le consentement est une des bases légales sur laquelle peut se fonder un traitement de données personnelles.

Le RGPD impose que ce consentement soit libre, spécifique, éclairé et univoque. Les conditions applicables au consentement sont définies aux articles 4 et 7 du RGPD.

Politique de confidentialité

Ce site utilise des cookies strictement nécessaires pour améliorer votre visite et pour recueillir des statistiques de navigation

[Plus d'infos](#)

Vos données, votre choix.

[Continuer sans accepter](#)

Sur nos sites et nos applications, nous recueillons à chacune de vos visites des données vous concernant. Ces données nous permettent de vous proposer les offres et services les plus pertinents pour vous, et de vous adresser, en direct ou via des partenaires, des communications et publicités personnalisées et de mesurer leur efficacité. Elles nous permettent également d'adapter le contenu de nos sites à vos préférences, de vous faciliter le partage de contenu sur les réseaux sociaux et de réaliser des statistiques. Pour en savoir plus sur l'utilisation des cookies [Cliquez ici](#)

Merci d'avance pour votre confiance.

Boulangers #Sibienensemble

J'ai compris

Le respect de votre vie privée est notre priorité

Pour améliorer votre expérience, La Poste et [ses partenaires](#) utilisent des cookies (ou technologies similaires). Les finalités des cookies sont les suivantes :

- **Mesure d'audience** : établir des statistiques complémentaires sur l'utilisation de nos sites et suivre la navigation.
- **Analyse et personnalisation** : analyser les parcours clients et personnaliser en temps réel nos sites et communications en fonction de votre navigation.
- **Publicité** : permettre de vous adresser des publicités en lien avec vos centres d'intérêts sur notre site et en dehors.

En cliquant sur "J'accepte" vous acceptez tous les cookies. Le bouton "Continuer sans accepter" vous permet d'indiquer votre refus et seuls les cookies nécessaires au fonctionnement du site seront déposés. Vous pouvez modifier vos choix à tout moment ou obtenir plus d'informations via [notre politique de cookies](#).

[Continuer sans accepter](#)

Gérer mes choix

J'accepte

Personnaliser mes choix

Accepter et fermer

Comment limiter nos traces sur le WEB ... ?

Lorsque vous allez sur un site web, votre navigateur (Firefox,Quant...) enregistre un fichier (.Txt), sur votre appareil et note :

vos traces de navigation (tracking) , votre 'profil' (profiling), et même votre mode d'utilisation du site ou votre comportemental = COOKIES

Prenez le temps de personnaliser votre consentement (...)

Le blocage de l'accès à un site internet est interdit en cas de refus des cookies

Les cookies permettent de suivre vos activités en ligne, enregistrer vos préférences. Ils sont utiles pour offrir une meilleure expérience utilisateur, mais parfois, vous pouvez vouloir supprimer les cookies.



On peut visualiser son historique de navigation, et le supprimer

avec Chrome, utiliser le raccourci clavier « Ctrl »+ «H »

On peut supprimer les Cookies :

consulter les paramètres de votre navigateur, : confidentialité, sécurité

Je sors le balai et je fais le ménage régulièrement dans mes mails, mes historiques (recherche, navigation, lecture de videos, géolocalisation...).

Confidentialité et sécurité

| | |
|----|---|
| 🗑️ | Supprimer les données de navigation Supprimer l'historique et les cookies, vider le cache, etc. |
| 📖 | Guide sur la confidentialité Examinez les paramètres clés de confidentialité et de sécurité |
| 🕒 | Cookies tiers Les cookies tiers sont bloqués lorsque vous utilisez le mode navigation privée |
| 🔍 | Confidentialité des annonces Personnalisez les informations utilisées par les sites pour vous montrer des annonces |
| 🔒 | Sécurité Navigation sécurisée (protection contre les sites dangereux) et autres paramètres de sécurité |
| 📷 | Paramètres des sites Permet de contrôler les informations que les sites peuvent utiliser et afficher (position, appareil photo, fenêtres pop-up et plus) |

Comment limiter nos traces sur le WEB ... ?

L'avis de la CNIL : la navigation privée ?

Cette option est activable depuis n'importe quel navigateur, et vous permet de ne pas enregistrer certaines informations au cours de votre session de navigation :

l'historique des sites visités, vos mots de passe, les champs d'un formulaire que vous remplissez, les cookies traceurs déposés par les sites que vous avez visités.

Sont néanmoins enregistrés : Les sites que vous avez enregistrés dans vos favoris, Les téléchargements effectués depuis votre navigateur qui sont enregistrés par défaut dans le fichier « téléchargements » de votre ordinateur.

Même avec un navigateur en mode privée, votre navigation n'a pas de secrets :

... pour le site que vous visitez : en mode navigation privée et tant que votre navigateur n'est pas fermé, les cookies continuent d'être déposés et donc potentiellement de transmettre en temps réel des informations au site que vous visitez. Il en est de même pour votre historique de navigation ou encore les mots de passe enregistrés **qui ne s'effacent qu'une fois que votre navigateur a été fermé**. Enfin, l'activation de la navigation privée n'empêchera pas un site - ou même un réseau publicitaire - de reconnaître votre terminal en utilisant d'autres technologies que les cookies (adresse IP ou Fingerprinting).

... **pour des personnes malveillantes : la navigation privée ne peut rien contre des logiciels espions qui auraient pu être installés sur votre terminal par des personnes malveillantes.**

Les pirates peuvent lire vos cookies et mieux vous connaître et utiliser vos vulnérabilités...

Comment limiter nos traces sur le WEB... ?

Limiter vous à l'obligatoire !

4 Ne pas tout dire... ou mentir !

Pour créer un compte sur un site ou une application, remplissez un formulaire. Ne vous inscrivez pas avec votre compte Facebook. Dans le formulaire, ne remplissez que les cases obligatoires, avec une étoile. Si vous créez un compte pour jouer à un jeu, vous pouvez écrire un faux nom, prénom, adresse...

The image shows a registration form with two main sections. The first section is 'Date de naissance' with a red circle around an asterisk indicating it is mandatory. Below it are three dropdown menus for day (10), month (07), and year (1957). The second section is 'Téléphone mobile' with a dropdown menu showing the French flag.

5 Lire les conditions avant de s'engager

A la fin du formulaire pour créer un compte, lisez les conditions générales d'utilisation comment l'entreprise utilise des informations sur vous.

Interdire le suivi

L'activation de la demande "Interdire le suivi" implique l'inclusion de cette dernière avec votre trafic de navigation. Le résultat dépend de la réponse d'un site Web à cette demande et de la façon dont cette dernière est interprétée. Par exemple, des annonces qui ne sont pas basées sur d'autres sites que vous avez consultés peuvent s'afficher sur certains sites Web en réponse à cette demande. Vos données de navigation continuent d'être collectées et utilisées sur de nombreux sites Web, notamment pour améliorer le niveau de sécurité, ou pour fournir du contenu, des services, des annonces et des recommandations sur le site, ainsi que pour générer des statistiques destinées à la création de rapports. [En savoir plus](#)

Paramètres de votre navigateur : Confidentialité et sécurité/cookies tiers/ activer l'option 'DO NOT TRACK' (DNT)

Soit interdire le suivi

Annuler

Confirmer

Quelques solutions sur les réseaux sociaux

Et ... ce n'est pas une option !

1. Consulter leur politique de confidentialité dont le partage de vos données
2. Utiliser les paramètres de confidentialité en fonction de vos besoins !

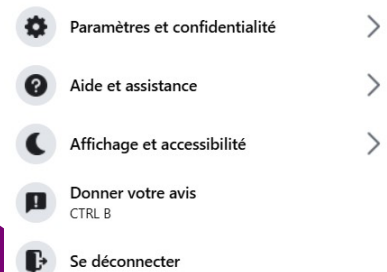


Nicole Giry Alamome

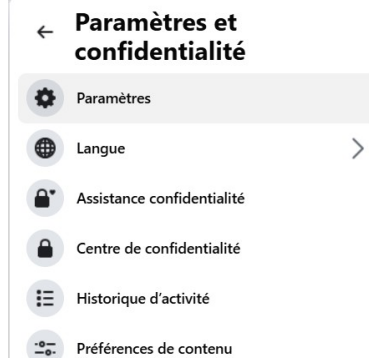
Test2

Test3

Voir tous les profils

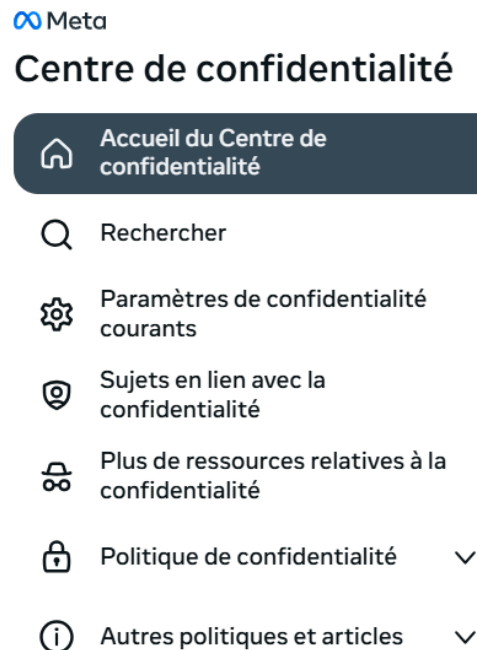


- Paramètres et confidentialité >
- Aide et assistance >
- Affichage et accessibilité >
- Donner votre avis
CTRL B
- Se déconnecter



← Paramètres et confidentialité

- Paramètres
- Langue >
- Assistance confidentialité
- Centre de confidentialité
- Historique d'activité
- Préférences de contenu



Meta

Centre de confidentialité

Accueil du Centre de confidentialité

Rechercher

Paramètres de confidentialité courants

Sujets en lien avec la confidentialité

Plus de ressources relatives à la confidentialité

Politique de confidentialité ▾

Autres politiques et articles ▾

Que DIT la CNIL ?

5 CONSEILS POUR PROTÉGER ma vie privée sur les réseaux sociaux

2

JE PROTÈGE

ma vie privée en utilisant des pseudonymes et des avatars selon les services que j'utilise et en fonction de mes usages. Je veille à bien distinguer mes amis de mes simples connaissances... en m'assurant de leur identité.



3

JE VERRAILLE

mon compte ! D'abord en le sécurisant avec un mot de passe fort et en activant les options complémentaires comme la « double authentification ». Ensuite en réglant mes paramètres de confidentialité pour limiter l'accès à mon profil ou à mes publications à des utilisateurs que j'ai choisis.



1

J'AI CONSCIENCE

que mes données personnelles ont de la valeur ! Toutes les informations que je poste sur Youtube et Instagram sont réutilisées. Pour savoir comment sont exploitées mes données de géolocalisation, mes photos, mes habitudes, mes like, je consulte les Conditions Générales d'Utilisation.



4

J'ANTICIPE

les conséquences de mes publications ! Internet est un lieu public où je peux laisser des traces, même sur Snapchat ! Avant de publier, je m'assure que mes publications ne nuisent ni à ma réputation, ni aux autres, ni à la loi.



5

JE VÉRIFIE

les informations auxquelles j'ai accès avant de les partager ou de cliquer dessus. Derrière certaines publications virales se cachent une « fake news », une arnaque, un contenu qui peuvent nuire à une personne... et parfois un programme malveillant.



Et ... les fausses informations

On parle aussi de fake news ou infox.

Il s'agit d'informations créées ou détournées pour manipuler le public, pour faire peur, pour partager des idées reçues, pour diffuser des propos racistes, sexistes, sectaires, idéologiques, etc.

Elle peut être transmise par n'importe qui, A une vitesse très rapide sur Internet.

Comment les repérer pour s'en protéger ? Se poser les bonnes questions :

- Qui est l'auteur ? (la source)
- Où l'information est publiée ? (le média)
- Y'a-t-il d'autres médias qui en parlent ? (la diversité de l'information)
- Quand a été publiée l'information ? (le contexte)
- Y'a-t-il des éléments bizarres ? (la fiabilité)

POUR ALLER PLUS LOIN

COMMENT PARLER DE CYBERSÉCURITÉ AVEC SES ENFANTS ?

Quotidiennement exposés aux outils numériques, mais souvent peu conscients des risques encourus dans leurs pratiques, les jeunes représentent des cibles faciles (cyberharcèlement, vol de données personnelles, piratage de comptes en ligne...). D'où l'importance de les sensibiliser et de les aider à acquérir des « réflexes » avec les bonnes pratiques, et ce, dès le plus jeune âge.

QUE FAIRE FACE AUX CONTENUS ILLICITES SUR INTERNET ?

DES MINEURS VICTIMES...

Au même titre que les adultes, les enfants peuvent être confrontés à des contenus choquants, parfois illicites : incitation à la haine, propagande terroriste, pédopornographie, etc. L'encadrement des mineurs dans leur navigation sur Internet reste donc un enjeu majeur. Cyberharcèlement, injure, diffamation, corruption de mineur, incitation à commettre un crime ou un délit... Pour signaler un contenu illicite sur Internet, rendez-vous sur le site du ministère de l'Intérieur www.internet-signalement.gouv.fr. Le 3018 propose également des informations sur ces dangers.



...OU AUTEURS DE CONTENUS

ET DE COMPORTEMENTS ILLICITES

Il arrive également que les jeunes soient tentés de se rendre visibles sur les réseaux sociaux ou Internet, avec un fort sentiment d'impunité. Or, Internet n'est pas un espace de non-droit et contrairement à certaines légendes, l'anonymat absolu n'y existe pas. Sur le web, tout comme le monde « réel », des lois existent dont les mineurs et les familles ne sont pas toujours conscients. Selon la nature des infractions, les auteurs de propos illicites tenus sur Internet encourent des peines qui peuvent aller jusqu'à plusieurs milliers d'euros d'amende et même dans certains cas des peines d'emprisonnement.

Et ... les fausses informations

6 MÉFIEZ-VOUS DES MESSAGES SUSPECTS

Qui n'a jamais reçu un message (mail ou SMS) ou un appel de la part d'individus se faisant passer pour une banque, une administration (impôts, assurance maladie...), une entreprise de livraison ou encore un site marchand ? Ces escrocs cherchent à nous tromper et vont nous inciter à communiquer des informations personnelles, à ouvrir une pièce jointe susceptible de contenir un virus ou à cliquer sur un lien malveillant pour nous rediriger vers un site frauduleux.

POUR NOUS PIÉGER, LES CYBERCRIMINELS UTILISENT DIFFÉRENTS RESSORTS TELS QUE LA PEUR, L'APPÂT DU GAIN, LA CRÉDULITÉ, L'URGENCE OU LA COÏNCIDENCE AVEC UNE SITUATION DE LA VIE QUOTIDIENNE.

Ex. : arnaque à la livraison de colis, à la mise à jour de notre carte Vitale, remboursement d'impôts...



LES RISQUES

Les **informations dérobées** (mots de passe, informations d'identité ou bancaires) seront ensuite **directement utilisées par les escrocs ou bien revendues** à d'autres cybercriminels pour mener diverses actions frauduleuses : piratage de compte en ligne, fraude à la carte bancaire, usurpation d'identité, hameçonnage ciblé sur la victime ou ses proches...

LES CONSEILS

Premier réflexe : **ne pas cliquer sur le lien qui vous est proposé. Au moindre doute, nous vous recommandons de contacter directement l'organisme concerné par un autre moyen** (exemple : par téléphone ou en se connectant par soi-même à son compte en ligne). Il peut en effet s'agir d'un message d'hameçonnage (phishing) visant à vous piéger.

POUR ALLER PLUS LOIN

Comment se prémunir et faire face au phishing ?
www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Retrouvez toutes nos ressources dédiées au phishing :
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/boxer-phishing

Apprendre : Se protéger, se défendre, être aidé



Assistance et prévention
en sécurité numérique

est la plateforme du dispositif national de prévention et d'assistance aux victimes d'actes de cyber malveillance. Elle s'adresse aux particuliers comme aux professionnels au travers de nombreux contenus et services gratuits en ligne. Elle propose également des prestataires spécialisés, répartis sur tout le territoire, en capacité de venir en aide aux victimes.

Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les sensibiliser au risque cyber, de les informer sur les menaces numériques et les moyens de s'en protéger.

Apprendre : Se protéger, se défendre, être aidé



Assistance et prévention
en sécurité numérique



Bienvenue sur 17Cyber

Un service public d'assistance en ligne destiné aux particuliers, entreprises, associations et collectivités victimes de cybermalveillance

Vous pensez être victime de cybermalveillance ?

Évaluez la situation grâce au diagnostic 17Cyber.

Complétez de manière anonyme le questionnaire suivant pour déterminer le problème que vous rencontrez et les solutions pour y remédier.

[J'établis mon diagnostic](#)

Accueil → Les bonnes pratiques

[PARTICULIERS](#) [PROFESSIONNELS](#) [COLLECTIVITÉS](#)

Je suis un particulier, je voudrais me documenter sur les bonnes pratiques relatives à toutes les menaces

- à toutes les menaces
- à mes données
- aux emails
- aux ordinateurs
- aux sites webs
- aux tablettes
- aux téléphones

Protégé

Les smartphones
voire plus, d'i



Assistance et prévention
en sécurité numérique

Exemple de fiche d'aide



LE PIRATAGE DE COMPTE



Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne. En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières: le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (phishing en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

BUT RECHERCHÉ

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (vente de données, usurpation d'identité, transactions frauduleuses, spam, etc.).

COMPRENDRE LES RISQUES

SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS.** Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez-en un solide ([voir notre fiche sur la gestion des mots de passe](#)). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION.**

CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTÉ** au [commissariat de police](#) ou [à la gendarmerie](#) ou écrivez au [procureur de la République](#) dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Utilisez des **mots de passes** différents et complexes pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

Lorsque le site ou le service le permettent, activez la **double authentification** pour augmenter le niveau de sécurité.

Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

Appliquez de manière régulière et systématique les **mise à jour de sécurité** du système et des logiciels installés sur votre machine.

Maintenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide.

Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

Si le site le permet, vérifiez les date et heure de la dernière connexion à votre compte afin de repérer d'éventuelles connexions anormales.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate.

Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.





ADOPTÉZ LES CYBER RÉFLEXES VOUS PROTÉGER DES RISQUES SUR INTERNET

Protégez vos comptes avec des mots de passe robustes

Ils sont les clés qui protègent l'accès à toute votre vie numérique.

RISQUES

- Fraude bancaire,
- Piratage de vos comptes,
- Usurpation d'identité.

CONSEILS

- Utilisez des **mots de passe longs, complexes et différents** pour chaque compte,
- **Changez-les** au moindre doute,
- Activez si possible la **double authentification**.



Sauvegardez vos données

En cas de vol ou de piratage de votre appareil, les données contenues dans vos appareils numériques peuvent être perdues, ou tomber entre de mauvaises mains.

RISQUES

- Perte de vos données,
- Vol de vos données.

CONSEILS

- **Identifiez** vos données importantes,
- Faites des **sauvegardes** régulières de vos appareils,
- **Conservez une copie** sur un support externe : clé USB, disque externe ou sur des services en ligne (Cloud).



Méfiez-vous des messages inattendus et alarmistes

Technique frauduleuse qui consiste à vous envoyer un faux message (e-mail, SMS, appel...) usurpant l'identité d'un tiers pour vous tromper.

RISQUES

- Fraude bancaire,
- Vol de vos données,
- Piratage de vos comptes.

CONSEILS

- **Ne cliquez pas** sur les liens et n'ouvrez pas les pièces jointes des messages suspects,
- Contactez **directement** l'organisme par un autre moyen,
- **Ne donnez jamais d'informations personnelles** sur des sites dont vous n'êtes pas certains de l'identité.



Sécurisez vos appareils et logiciels

Vos matériels et logiciels peuvent contenir des failles de sécurité permettant de vous attaquer.

RISQUES

- Piratage de vos appareils,
- Fraude bancaire,
- Vol de vos données.

CONSEILS

- **Faites régulièrement** les mises à jour de vos appareils et logiciels,
- **Effectuez ces mises à jour** uniquement depuis les sites officiels,
- **Installez** un antivirus.



**9 Français
sur 10**
ont déjà été victimes

Étude Opinion Way menée pour
Cyberveilleur - Juin 2023



**Repérer
un message
frauduleux**



Vos données personnelles sont précieuses

Vos nom et prénom, identifiants de connexion, numéro de téléphone, renseignements bancaires sont des données personnelles.

Avant de fournir vos informations personnelles en ligne, demandez-vous toujours si communiquer ces informations est bien nécessaire et justifié.



Se prémunir des arnaques sentimentales

Elles consistent à simuler des sentiments amoureux envers la victime en utilisant un faux profil dans le but d'établir des liens émotionnels et de gagner sa confiance pour lui soutirer de l'argent.

LES BONNES PRATIQUES

- **Réfléchissez bien** avant de partager vos informations personnelles sur des sites de rencontre,
- **Soyez prudent** si la personne trouve toujours une excuse pour ne pas vous rencontrer réellement,
- **N'envoyez pas d'argent** à quelqu'un que vous n'avez jamais rencontré dans la vie réelle.



Vous souhaitez signaler ?

- Un e-mail malveillant : www.signal-spam.fr
- Un SMS malveillant : www.33700.fr
- Un contenu illicite : www.internet-signalement.gouv.fr



BESOIN D'AIDE ?

Besoin d'assistance si vous êtes victime ?
www.cybermalveillance.gouv.fr

Une question sur vos données personnelles ?
www.cnil.fr/fr/cnil-direct

Vous souhaitez de plus amples renseignements ou faire appel à un spécialiste :



L'Union nationale des associations familiales est l'institution chargée de promouvoir, défendre et représenter les intérêts de l'ensemble des familles. Les familles et les aidants familiaux ont un rôle important pour accompagner les personnes âgées ou vulnérables dans la société numérique. C'est dans cet objectif que l'Unaf informe et accompagne les aidants familiaux et les seniors pour une pratique responsable du numérique.
→ www.unaf.fr
→ www.pourlesfamilles.fr



Cybermalveillance.gouv.fr est la plateforme du dispositif national de prévention et d'assistance aux victimes d'actes de cybermalveillance. Elle s'adresse aux particuliers comme aux professionnels au travers de nombreux contenus et services gratuits en ligne. Elle propose également des prestataires spécialisés, répartis sur tout le territoire, en capacité de venir en aide aux victimes.
→ www.cybermalveillance.gouv.fr



La Commission nationale de l'informatique et des libertés (CNIL) a pour mission de protéger vos données personnelles et de faire respecter votre vie privée. Elle vous aide à connaître et comprendre vos droits pour mieux maîtriser vos données personnelles. La CNIL agit également pour faire appliquer la loi en conseillant les organismes et, si besoin, en les sanctionnant.
→ www.cnil.fr



CYBERSÉCURITÉ

Ayez les bons réflexes !

© Océane Neume - communication - Juin 2024 | Ne pas être sur la voie publique

Apprendre : Se protéger, se défendre, être aidé



CNIL | PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

MON QUOTIDIEN | EXERCER MES DROITS | À TÉLÉCHARGER | LA CNIL | 🔍



JE M'INFORME

Comment accéder à vos données personnelles, les rectifier, les supprimer ?

> Découvrir vos droits



J'AGIS

Comment faire valoir vos droits sur vos données ou agir en cas de problème ?

> Découvrir vos moyens d'actions



J'AI BESOIN D'AIDE

Vous recherchez une information ? Retrouvez les questions les plus fréquemment posées.

> Découvrir nos questions/réponses

Depuis 1978 avec la loi Informatique et Libertés : a pour mission de **protéger vos données personnelles et de faire respecter votre vie privée**. Elle vous aide à connaître et comprendre vos droits pour mieux maîtriser vos données personnelles. La CNIL agit également pour faire appliquer la loi en conseillant les organisations .

Le règlement général sur la protection des données, ou RGPD, encadre le traitement des données personnelles, sur le territoire de l'Union européenne. Entré en application en 2018, il renforce le contrôle des citoyens sur l'utilisation qui peut être faite de leurs données.

Consentement, protection des données collectées , contrôles et droits des usagers

Comment limiter nos traces sur le WEB :

La CNIL vous aide

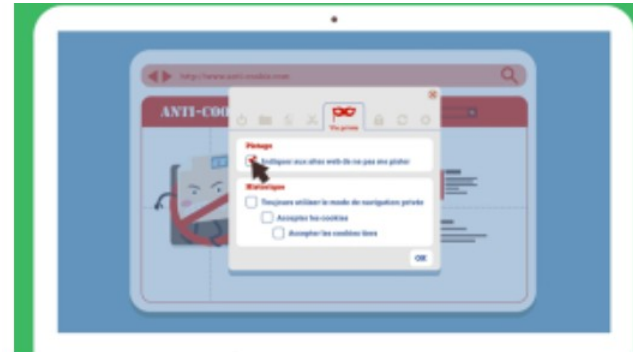
– **Cookieviz, une dataviz en temps réel du tracking de votre navigation**

Publié par le LINC

La CNIL a développé Cookieviz, un outil de visualisation qui mesure l'impact des cookies et autres traqueurs lors de votre navigation.

<https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-proteger>

et aussi...La CNIL propose un outil pour tester la robustesse de vos mots de passe

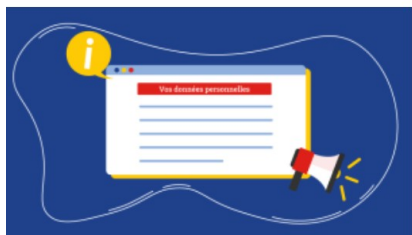


Les conseils de la CNIL pour maîtriser votre navigateur

La CNIL vous propose quelques outils et astuces pour surveiller les cookies présents sur votre ordinateur.

Les droits pour maîtriser vos données personnelles

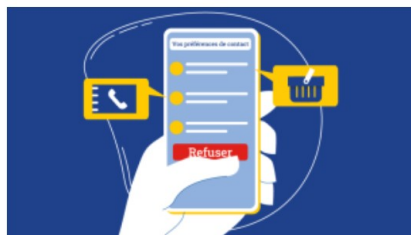
La CNIL vous informe sur les différents droits que vous pouvez exercer auprès des organismes qui utilisent vos données.



Rester informé

Un organisme qui collecte des informations sur vous doit vous proposer une information claire sur l'utilisation des données et sur vos droits.

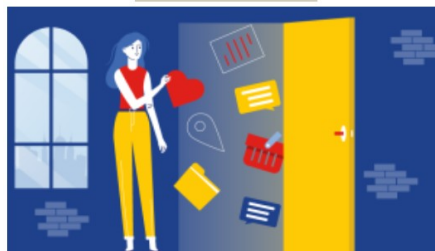
Exercer votre droit d'information



Vous opposer

Vous pouvez vous opposer à tout moment à ce qu'un organisme utilise certaines de vos données.

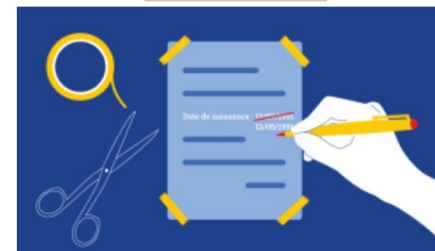
Exercer votre droit d'opposition



Vérifier vos données

Obtenir et vérifier les données qu'un organisme détient sur vous.

Exercer votre droit d'accès



Rectifier vos données

Rectifier les informations inexactes vous concernant.

Exercer votre droit de rectification

Les droits pour maîtriser vos données personnelles

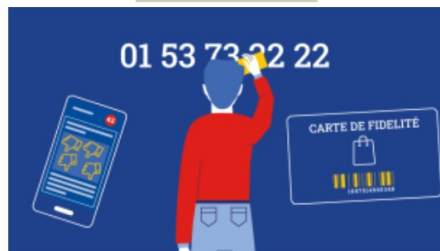
La CNIL vous informe sur les différents droits que vous pouvez exercer auprès des organismes qui utilisent vos données.



Déréférencer un contenu

Ne plus associer votre nom-prénom à un contenu visible dans un moteur de recherche.

Exercer votre droit au déréférencement



Effacer vos données

Effacer des données vous concernant.

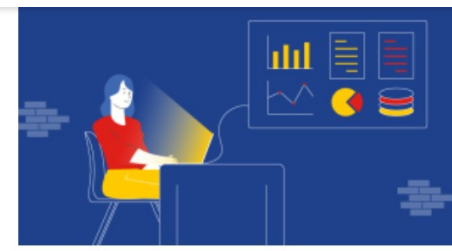
Exercer votre droit d'effacement



Emporter vos données

Emporter une copie de vos données pour les réutiliser ailleurs.

Exercer votre droit à la portabilité



Demander une intervention humaine

Remonter le fil de votre profilage, vous y opposer et demander l'intervention d'un humain dans une décision automatisée vous concernant.

Exercer votre droit lié au profilage

Les droits pour maîtriser vos données personnelles

La CNIL vous informe sur les différents droits que vous pouvez exercer auprès des organismes qui utilisent vos données.



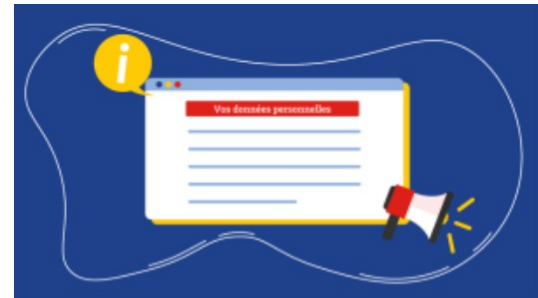
Geler l'utilisation de vos données

Exercer votre droit à la limitation des données

Envoyer un courrier

La CNIL met à votre disposition des modèles de courrier afin de vous accompagner dans vos démarches.

Découvrir les modèles



Comprendre mes droits

Retrouvez toutes les vidéos explicatives sur l'exercice de vos droits.

Ressources vidéo

Apprendre : Se protéger, se défendre, être aidé



L'UFC-Que Choisir : informer, conseiller et défendre l'intérêt des consommateurs, est agréée en qualité d'organisation de consommateurs en application des articles L. 411-1 et suivants du code de la consommation :

L'UFC-Que Choisir s'est impliquée dans la création du nouveau règlement européen sur la protection des données personnelles. Validé le 15 décembre 2016 par le Parlement, le Conseil et la Commission européens, [ce texte renforce la protection de la vie privée](#), permettant à chacun de mieux maîtriser ses données personnelles. Il est entré en vigueur le 25 mai 2018

Et vous propose un outil pour reprendre le contrôle de vos données/data

The screenshot shows the website interface for UFC Que Choisir. At the top, there is a red navigation bar with the following menu items: ACCUEIL, ANALYSER VOS DONNÉES, EXERCER VOS DROITS, and DEMARCHAGE TELEPHONIQUE. Below the navigation bar, the UFC Que Choisir logo is visible on the left, along with the text 'Fonds de dotation'. The main content area features a prominent red button that says 'je ne suis pas une data'. Below this, the text 'REPRENEZ LE CONTRÔLE' is displayed in large, bold letters. A row of social media icons (Facebook, Instagram, Twitter, LinkedIn, and Google) is positioned below the text. On the right side of the main content area, there is a video player with a play button. The video player has a title '#JeNeSuisPasUneData : présentation de l'outil' and a subtitle 'EXERCEZ VOS DROITS ET MAITRISEZ VOS DONNEES PERSONNELLES'. Below the video player, there is a section titled 'Exercez vos droits' with a list of bullet points: '• Exercer vos droits', '• Faire...', and '• Utiliser...'. A red play button is overlaid on the video player. At the bottom of the video player, there is a 'Regarder sur YouTube' button. The page number '30' is visible in the bottom right corner.

Apprendre : Se protéger, se défendre, être aidé



<https://respectemesdatas.fr/>



ANALYSER MES DONNÉES



SUPPRIMER MES DONNÉES

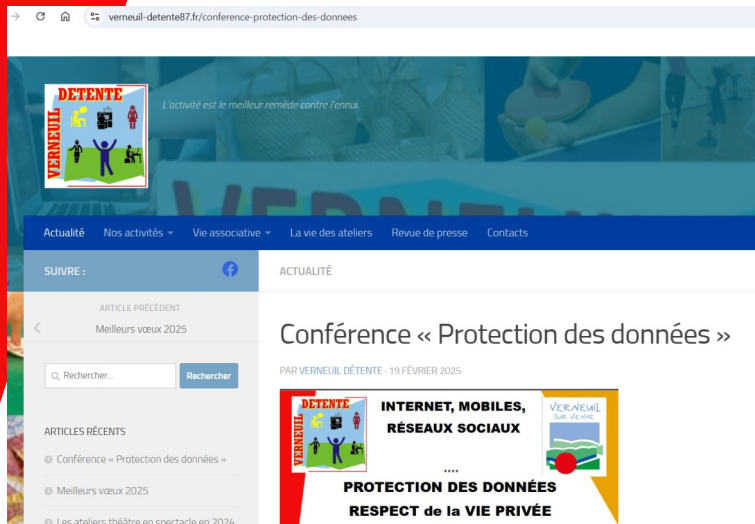


EXERCER MES DROITS



DEMARCHAGE TELEPHONIQUE

Apprendre : Se protéger, se défendre, être aidé



La section informatique vous propose des ateliers d'apprentissage au numérique.

Prenez contact !

Prochain forum des associations début septembre

Début des ateliers : fin septembre début octobre

restez curieux, informé et veillez sur vos clics ...
sauf sur les sites

CNIL, Cybermalveillance.fr, UFC que choisir,

et bien sur **votre association !**

Face au renard soyez le hérisson !