CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

Sécurité des données, si on en parlait ?

LA MEDNUM

Mardi 5 novembre 2024

CNIL.

LA CNIL

C.N.I.L


Ça veut dire quoi « CNIL » ?
A Cercle neuronal des idées libérées.
B Centre naturel des iguanes du Languedoc.
C Commission nationale de l'informatique et des libertés.
RÉPONSE • CONSEIL
C ! La Commission nationale de l'informatique et des libertés (CNIL) est une administration de l'État.
Une de ses missions :
aider les personnes à faire effacer des images ou des renseignements qui sont en ligne et qui les concernent.

Un peu d'Histoire

Le Monde | ACTUALITÉS | ÉCONOMIE | VIDÉOS | DÉBATS | CULTURE | LE GOÛT DU MONDE | SERVICES

ARCHIVES

Une division de l'informatique est créée à la chancellerie " Safari " ou la chasse aux Français

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une " division de l'informatique " au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grappillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un " identifiant ", qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne parait pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

Par PHILIPPE BOUCHER.

https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html

Les missions de la CNIL

- Informer les personnes, protéger leurs droits
- Accompagner la conformité, conseiller
- Anticiper et innover
- Contrôler et sanctionner

Cnil.fr


https://www.cnil.fr/fr/mon-quotidien/ma-securite-numerique
PARTICULIERS
PROFESSIONNELS
PRESSE
Fr - En | Gestionnaire de cookies
CNIL.
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles
MON QUOTIDIEN | EXERCER MES DROITS | À TÉLÉCHARGER | LA CNIL
> Ma sécurité numérique
Ma sécurité numérique
Pour protéger ses données, il est essentiel de sécuriser son ordinateur
> BESOIN D'AIDE

Sanctions et contrôles liés à la CYBER

1/3 des sanctions prononcées par la CNIL en 2022
vise des manquements à l'obligation de sécurité

1/3 des contrôles réalisés par la CNIL en 2023
concerne des manquements à l'obligation de sécurité

CNIL.

LE RGPD

Donnée personnelle

- **Information permettant d'identifier ou de caractériser une personne identifiée ou identifiable**

Prénom Nom

Visage

Adresse postale

Voix

Numéro de téléphone

Adresse IP

Email

Plaque d'immatriculation

Bulletin scolaire

Donnée personnelle sensible

- Certaines de ces données sont dites « sensibles », au sens de la loi

Religion

Etat de santé

Appartenance syndicale

Opinions politiques

Orientation sexuelle

Origine ethnique

Données biométriques

Données génétiques

Mes traces sur Internet

Les données traitées par défaut dans mes réglages :

Accès au micro, géolocalisation, partage d'informations, etc.

Les données que je donne de moi-même

- Prénom, Nom
- Adresse de messagerie
- Numéro de téléphone
- Date de naissance
- Géolocalisation
- Photographies
- Vidéos
- Carte de crédit

Les données interprétées de mes actions

- Goûts musicaux, vestimentaires...
- Désirs
- Religion, foi
- Orientation sexuelle
- Opinions politiques
- Temps passé sur une application

Les données de mon entourage

- Amis
- Famille, parents
- Situation amoureuse
- Goûts de mon entourage
- Photos / vidéos
- Domiciliation, lieux de vie et déplacements

Traiter des données

- Toute opération portant sur des données personnelles, quel que soit le procédé, telles que :

Collecter, traiter, stocker

- **La collecte, le traitement, le stockage, la transmission et l'interconnexion des données sont encadrés par la loi Informatique et Libertés et par le RGPD**

Objectif (finalité)	A quoi servent les données collectées ?
Pertinence	Les données envisagées permettent-elles d'atteindre cet objectif ?
Durée de conservation	Combien de temps ces données vont-elles être conservées ? Comment ces informations sont-elles sécurisées ?
Droits des personnes	Suis-je informé de mes droits pour me permettre de les exercer en connaissance de cause ?

QUI A LE(S) DROIT(S) ?

Droits numériques / données personnelles

Nos droits, dès la naissance :

- Être informé
- S'opposer
- Vérifier ses données
- Rectifier ses données
- Déréférencer un contenu
- Effacer un contenu
- Emporter ses données
- Demander une intervention humaine

Pour exercer ses droits :

- Contacter le responsable de traitement
- Le délai de réponse légal est de 1 mois
- Si vous n'obtenez pas de réponse : plainte auprès de la CNIL

LES BASES DE LA CYBERSÉCURITÉ

Images générées avec Midjourney par Gaston Gautreneau

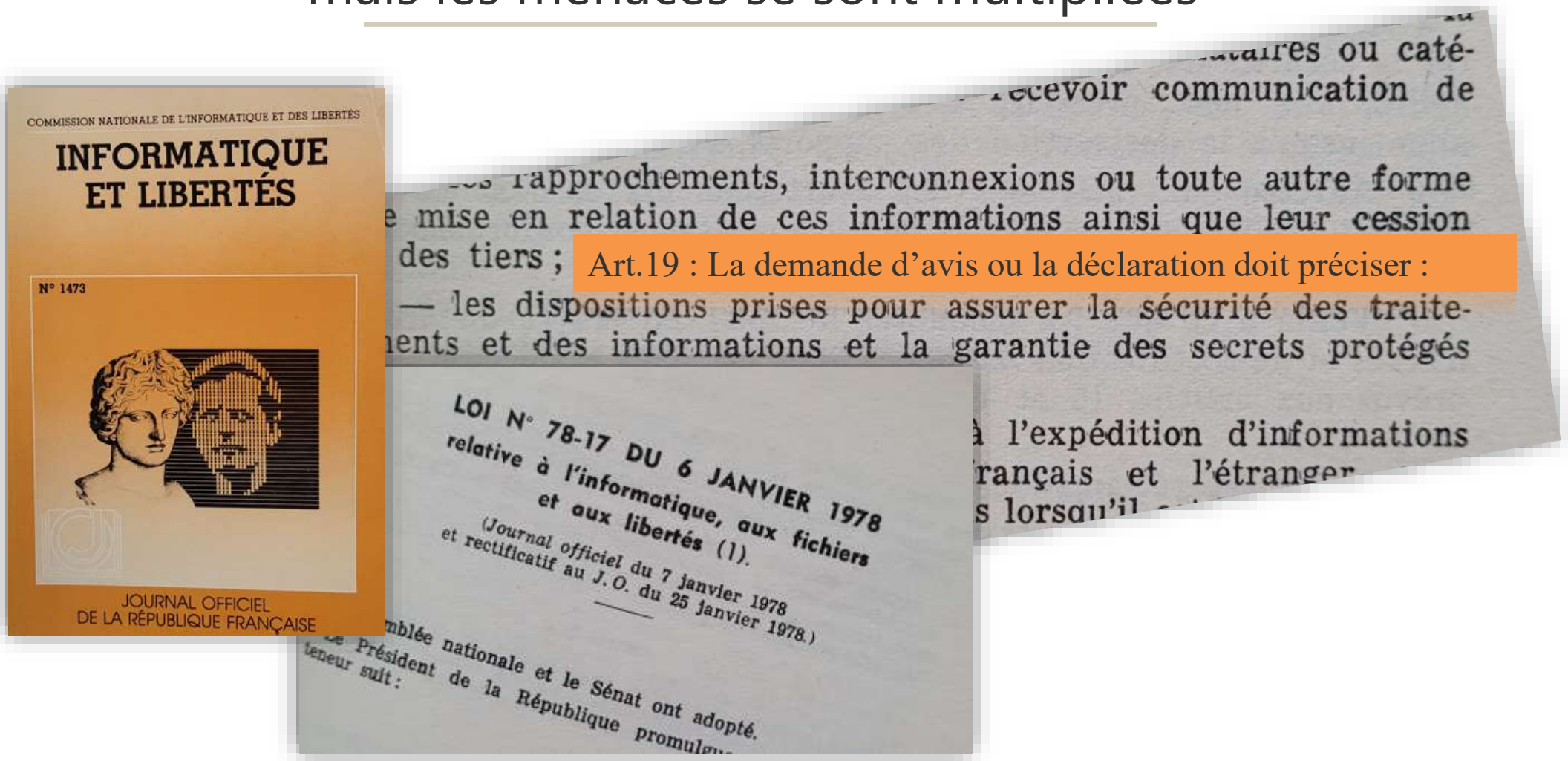
La cybersécurité, c'est quoi ?

- État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

- La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

L'obligation de sécurité ne date pas d'hier …

mais les menaces se sont multipliées



Une cyberattaque, c'est quoi ?

- Une cyberattaque consiste à porter atteinte à un ou plusieurs systèmes informatiques dans le but de satisfaire des intérêts malveillants.

- Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou liés par réseaux, connectés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des moyens de communication comme les smartphones, les tablettes et les objets connectés. La sécurité de ces dispositifs informatiques est mise en danger soit par voie informatique (virus, logiciel malveillant, etc.), soit par manipulation, soit par voie physique (effraction, destruction).

- Les quatre grandes finalités des cyberattaques sont : l'appât du gain, la déstabilisation, l'espionnage et le sabotage.

- Types d'attaques :
  - Hameçonnage, *phishing* en anglais
  - Rançongiciel, *ransomware* en anglais

Un sujet d'actualité

"Ils s'équipent et s'outillent mieux" : plus de 250 cyberattaques recensées l'an dernier dans les hôpitaux, un chiffre stable

Environ la moitié des 581 incidents informatiques recensés l'an dernier dans les hôpitaux et établissements médico-sociaux par l'Agence du numérique en santé consiste en des cyberattaques.

Cyberattaque à l'hôpital d'Armentières : une réouverture des urgences espérée lundi dans la journée

Les pirates demandent une rançon. C'est la première fois que l'hôpital d'Armentières est victime d'une telle attaque.

franceinfo - avec France Bleu Nord
Radio France

Publié le 11/02/2024 11:07 | Mis à jour le 11/02/2024 18:35

franceinfo:

Cybersécurité : trois questions après la cyberattaque contre Free et la fuite de données bancaires

Les seniors, cibles préférées des cybermenaces

franceinfo senior

Pour informer les seniors et les protéger, la CNIL et le site gouvernemental Cybermalveillance publient un guide sur les cybermenaces.

Les Etats membres de l'ONU se mettent d'accord sur un premier traité pour lutter contre la cybercriminalité

Le texte vise à "combattre plus efficacement la cybercriminalité" et à renforcer la coopération internationale sur le sujet.

franceinfo avec AFP

Cybersécurité : une directive européenne (NIS-2), en vigueur en octobre 2024, fixe des obligations à 30 000 entreprises et collectivités françaises

Nouveau monde

Face à des cyberattaques en constant développement, l'Europe impose d'importantes exigences de sécurisation pour les entreprises et les collectivités jugées majeures pour l'activité de leur pays. Avec des amendes et la mise en cause des dirigeants.

Paris 2024 : 40 musées français visés par des cyberattaques

Une cyberattaque sur 40 musées français a eu lieu mardi 6 août. Le gouvernement tient à rassurer les Français sur l'ampleur de cette attaque.

Qu’est-ce qu’une violation de données ?

- Il s’agit de tout incident de sécurité, d’origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l’intégrité, la confidentialité ou la disponibilité de données personnelles.

- Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

- Sachez par ailleurs que l’organisme concerné doit également notifier la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques

Violation de données = Incident de sécurité, d'origine malveillante ou non

- Une cyberattaque est donc considérée comme une violation de données,
- Mais en cas de perte ou de vol d'un ordinateur portable par l'organisme traitant les données personnelles de clients ou de membres d'une association,

- De perte ou le vol d'un support de stockage externe (de type disque dur, SSD externe ou clé USB) contenant des données des personnes concernées par un organisme (non protégé / pas de chiffrement),

- D'envoi d'un message électronique à tous les destinataires en omettant de les mettre en copie cachée (accès à toute la liste de destinataire pour tous), etc.

Ces cas constituent également des situations de violations de données

Évolution des menaces

- Professionnalisation de la sphère cybercriminelle;
- Aux attaques ciblées s'ajoutent les attaques en masse
  - Tous les secteurs sont impactés;
  - Les données financières et les données de santé ne sont plus les seules données recherchées;
- Vecteur #1 : Le *phishing*;
- Attaques #1 *rançongiciel* et #2 *messagerie électronique (piratage de comptes)*;
- Constat : Évolution des attaques de type rançongiciel incluant désormais quasi systématiquement, au-delà du chiffrement des données, une phase d'exfiltration des données.

[Source]: CNIL – Rapport annuel 2023

Quelques exemples d'attaques Impacts et recommandations (1/2)

- *Phishing Netflix par téléphone*
  - Validation numéro de téléphone
  - Validation personne
  - Tentative d'usurpations d'identité sur les services connus (script / Action immédiate

Remédiation

- Utiliser des mots de passe différents par service
- A défaut modifier tous les mots de passe

- *Attaque au Président ou Attaque aux faux ordres de virement*
  - Demande de modification d'un RIB
  - Paiement urgent
  - *Usurpation de la voix*
  - *Usurpation d'identité sur une messagerie*

Remédiation

- *Ne pas appeler le numéro en bas du message*
- *Avoir une liste de contacts ou à défaut chercher le numéro sur un site officiel*
- *Valider la qualité de la demande avant de l'exécuter*

Quelques exemples d'attaques
Impacts et recommandations (2/2)

- *Tentative de Phishing via Linkedin*
  - Phishing caché derrière une invitation Linkedin
  - Tentative d'usurpation d'identité sur un compte Linkedin

Remédiation

- Ne jamais cliquer sur le lien dans l'e-mail, aller sur l'application (application ou site web)
- Utiliser des mots de passe différents par service
- A défaut modifier tous les mots de passe

- *Utiliser des adresses e-mail professionnelles*
  - Usurpation d'identité simplissime permettant de générer toutes sortes d'attaques

Remédiation

- *Créer/Écrire à une adresse professionnelle (par ex.* prenom.nom@votre-structure-médiation.fr et non ~~prenom.nom@messagerieenligne.fr~~)

Exemples de phishing (e-mail ou SMS)

Attention ! Phishing/hameçonnage

-------- Message d'origine --------
De: **"France-identite.gouv.fr"** <noreply@france-identite.gouv.fr>
Date: 21 oct. 2024 00:49:15
Objet: Conformité : Décret n° 2022-676
À:

Bonjour,

Dans le cadre de la vérification et pour des raisons de sécurité et de performances.

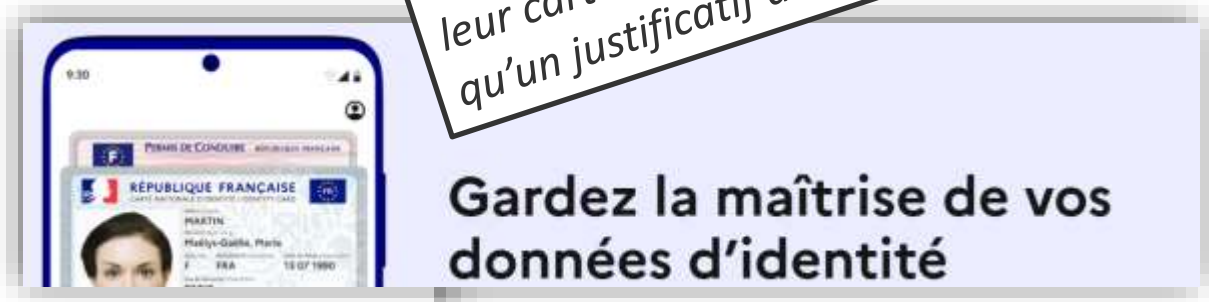
Merci de bien vouloir nous envoyer par retour de mail, la copie de votre piece d'identité scanner en recto-verso et un justificatif de domicile valide.

Décret n° 2022-676 du 26 avril 2022 autorisant
la vérification d'un moyen d'identification électronique dénommé « [illegible]ce de garantie de l'identité numérique »
(SGIN) et abrogeant le décr[illegible]2019-452 du 13 mai 2019
autorisant la vérification d'[illegible]oyen d'identification électronique dénommé [illegible]thentification en ligne certifiée sur mobile »

Direction du programme interminist[illegible]iel France identité numérique
Place Beauvau
75008 Paris

21 octobre 2024 – attaque en cours !!!

Depuis quelques jours, des usagers reçoivent des courriels expédiés par noreply@france-identite.gouv.fr leur demandant de transmettre une copie de leur carte d'identité recto-verso ainsi qu'un justificatif de domicile.



MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

PHAROS

Portail officiel de signalement des contenus illicites de l'Internet

La Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (**Pharos**) du ministère de l'Intérieur procède prioritairement au traitement des signalements de contenus illicites mis en ligne. Chacun peut effectuer un signalement depuis son portail dédié dès lors que le contenu incriminé est public. Arnaques, discriminations, menaces d'atteintes aux personnes, faits liés au terrorisme, urgences vitales, pédopornographie, peuvent notamment être portées à la connaissance des autorités grâce à ce dispositif. **Pharos** initie des enquêtes judiciaires chaque fois que nécessaire.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Ma Sécurité

La police et la gendarmerie nationales vous accompagnent dans vos démarches.

Cette plateforme est le premier service public de **dépôt de plainte en ligne** du ministère de l'Intérieur pour les victimes d'arnaques sur internet. Le dispositif de traitement harmonisé des enquêtes et signalements pour les e – escroqueries (THESEE) permet de porter **plainte** ou de **signaler** l'**infraction en ligne**.

La plainte en ligne pour les arnaques sur internet (THESEE)

Pour les victimes d'escroqueries sur internet : faux sites de vente, piratage de comptes de messagerie, extorsion d'argent pour débloquer un ordinateur... vous pouvez déposer plainte en ligne grâce au dispositif THESEE.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Service-Public.fr
Le site officiel de l'administration française

Cette plateforme vise à lutter contre la **fraude à la carte bancaire** sur internet. Elle permet à tout internaute de signaler à la police un ou plusieurs usages frauduleux de sa carte bancaire. Pour signaler une fraude, si vous êtes toujours en possession de la carte, **accédez à la démarche**.

Les bons réflexes

Bien choisir mon mot de passe

Entrer un mot de passe permet de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable, c'est un geste quotidien de sécurité.

Choisir un mot de passe difficile est un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

- Ne pas utiliser pas le même mot de passe pour tout. Un mot de passe = un compte.
- Pour me souvenir de l'ensemble de mes mots de passe, j'utilise un coffre-fort à mots de passe.

Entretenir ses appareils numériques

Mettre à jour régulièrement les logiciels de mes appareils numériques est essentiel. Dans chaque système d'exploitation (Android, MacOS, Linux, Windows,etc.), logiciel ou application, des mises à jour de sécurités ont proposées. Si elles ne sont pas faites régulièrement, les attaquants peuvent plus facilement mener à bien leurs opérati

Effectuer des sauvegardes régulières

Sauvegarder quotidiennement ou hebdomadairement, permet, par exemple, de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur.

Être prudent avec son smartphone, sa tablette

> Alexandre possède un smartphone. Au moment de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, les éditeurs peuvent accéder à tous les SMS présents sur son téléphone.

Être prudent lors de l'ouverture de messages électronique

> À la suite de la réception d'un courriel semblant provenir d'un de ses amis, Madame Michel a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Madame Michel le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

4. Protégez-vous des virus et autres logiciels malveillants

Sur Internet, les logiciels malveillants (virus, vers, cheval de Troie, logiciel espion, etc.) représentent un risque réel. Pour vous protéger de ces intrusions, les outils suivants sont de précieux alliés.

> Un antivirus dont vous respectez les recommandations chaque fois qu'il vous demande de mettre à jour les bases virales ou de supprimer ou mettre en quarantaine un fichier suspect.
> Un pare-feu bien configuré qui bloquera les connexions non désirées depuis votre ordinateur.

Télécharger des programmes, logiciels sur les sites officiels des éditeurs

Si je télécharge du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, je prends le risque d'enregistrer sur mon ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie.

Être vigilant lors d'achats en ligne

Lorsque je réalise des achats en ligne, mes coordonnées bancaires sont susceptibles d'être interceptées par les attaquants.

Ainsi, avant d'effectuer un paiement en ligne, je vérifie sur le site :

- La présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur (remarque : ce cadenas n'est pas visible sur tous les navigateurs).
- L'apparition de la mention « https:// » au début de l'adresse du site.
- L'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.
- Je privilégie la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.
- Je ne transmets jamais le code confidentiel de ma carte bancaire.

5. Évitez les réseaux Wi-Fi publics ou inconnus

S'ils peuvent s'avérer très utiles, les réseaux Wi-Fi publics sont une aubaine pour les attaquants. Très faciles d'accès, ces réseaux peuvent être contrôlés pour intercepter vos informations personnelles.

Les bons réflexes

Attention à l'éditeur du logiciel ou de l'application que l'on télécharge, même sur un magasin officiel d'applications

Les bons réflexes

free

VIOLATION DE DONNÉES

L'exploitation frauduleuse d'IBAN (coordonnées bancaires)

L'IBAN est un identifiant bancaire que vous avez utilisé pour payer un abonnement ou un service.

Cet identifiant peut dans certains cas **permettre à un pirate d'émettre des ordres de prélèvement illégitimes** qui ciblent les IBAN obtenus frauduleusement. Le pirate peut aussi, plus directement, usurper l'IBAN d'une autre personne en les communiquant lors de la **création d'un mandat de prélèvement** dans le cadre d'une souscription à un service.

Afin de diminuer les risques d'exploitation frauduleuse de votre IBAN et de minimiser ses conséquences :

- **Surveillez régulièrement les opérations sur votre compte bancaire** et faites opposition si nécessaire. Rapprochez-vous de votre conseiller bancaire habituel en cas de doute ;
- **Vérifiez la liste des créanciers autorisés** (c'est-à-dire les bénéficiaires des prélèvements) dans votre espace de banque en ligne ;
- Lors de la réception d'un mandat de prélèvement prérempli, ou d'une prétendue mise à jour de celui-ci, **soyez vigilant quant aux informations décrivant le créancier** afin d'éviter un détournement de vos paiements.

La CNIL a constaté plusieurs violations de données personnelles concernant des organismes connus du grand public ces dernières semaines, comme celle ayant touché l'entreprise FREE récemment. Usurpation d'identité, vol de l'IBAN … quels sont les risques ? Que pouvez-vous faire ?

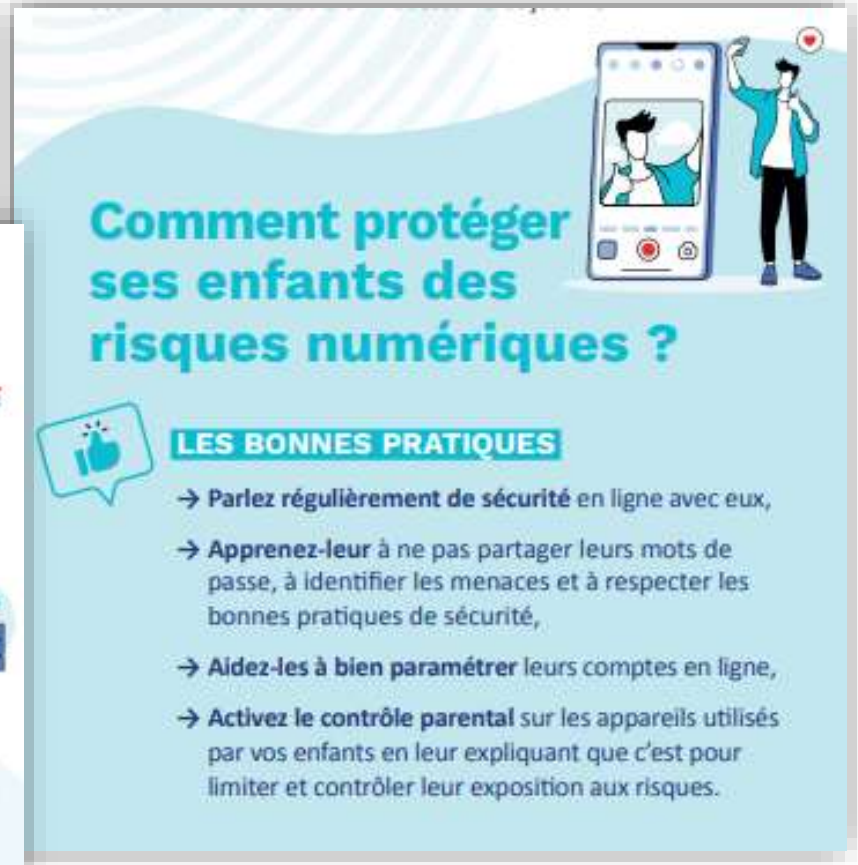
Comment porter plainte ?

Vous pouvez porter plainte de deux manières :

- Auprès de la CNIL si vous estimez que vos données personnelles n'ont pas été suffisamment sécurisées.
- Auprès de la police ou de la gendarmerie si vous êtes victime d'une usurpation d'identité, d'une arnaque ou de paiements frauduleux.

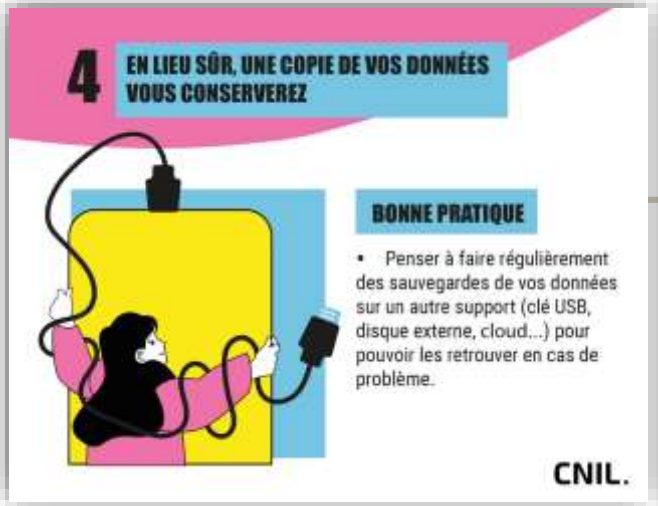
https://www.cnil.fr/fr/fuite-de-donnees-sur-internet-et-vol-de-votre-iban-comment-vous-proteger-si-vous-etes-concerne

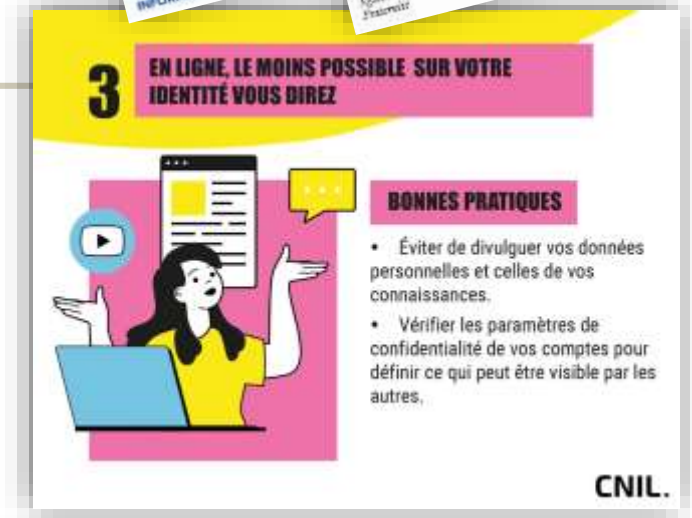
Tous concernés par ces enjeux



https://www.cnil.fr/fr/cybermalveillance-la-cnil-et-lunaf-publient-deux-guides-sur-les-cybermenaces

Ressources pour les particuliers





https://www.cnil.fr/fr/se-proteger-sur-internet-avec-les-cyber-reflexes

Ressources pour vous

http://www.cnil.fr/ -- https://cyber.gouv.fr/ -- https://www.cybermalveillance.gouv.fr/

Autres ressources

https://www.cybermalveillance.gouv.fr/

Utilisez des mots de passe différents par service

Faites des mises à jour régulières

Chiffrez vos données

Utilisez un antivirus

Faites des sauvegardes

Verrouillez votre poste de travail

Chiffrez votre poste de travail

Réfléchissez avant de cliquer sur un lien dans un message

EN SAVOIR PLUS

Le MOOC de la CNIL

https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie