

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.



Ci 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 paraît 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



[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 ou...

[> 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

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

Origine ethnique

Etat de santé

Données biométriques

Appartenance syndicale

Données génétiques

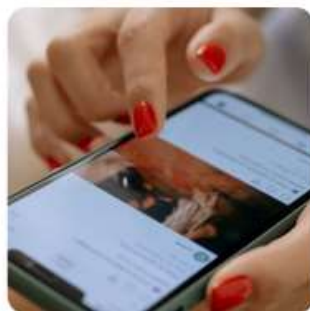
Opinions politiques

Orientation sexuelle

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

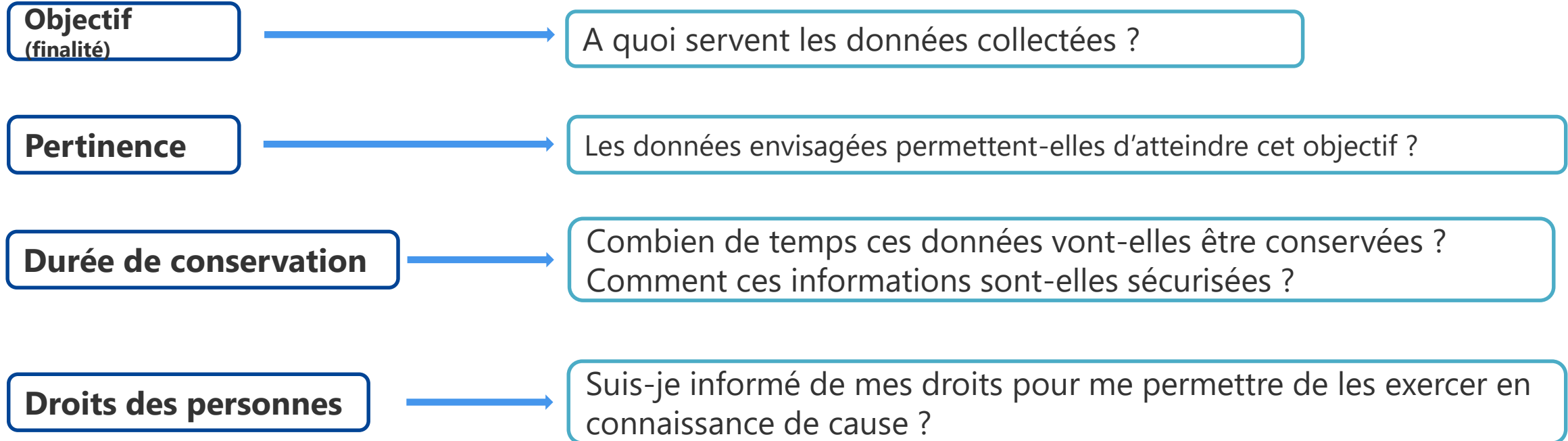
Traiter des données

- 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



CNIL.

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



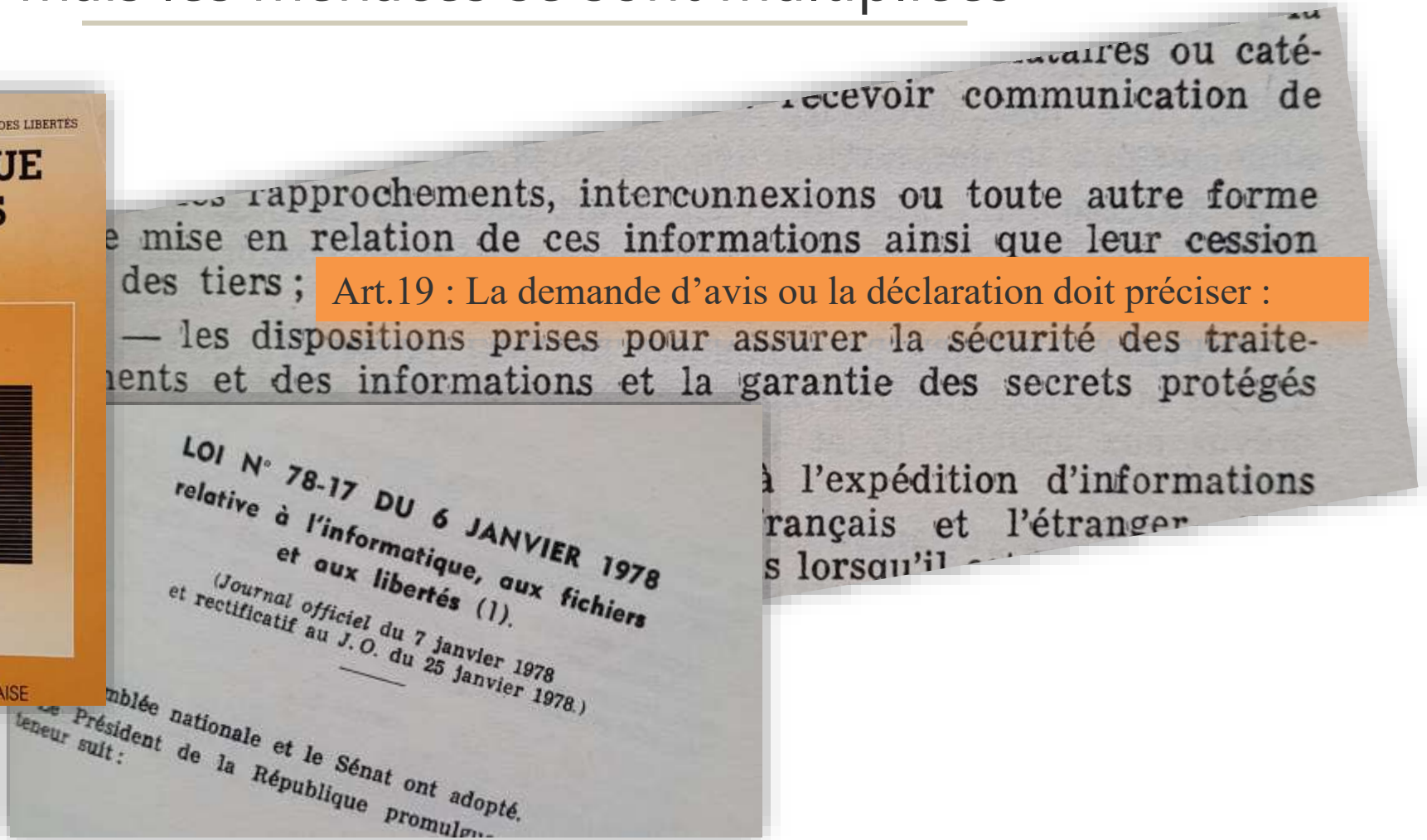
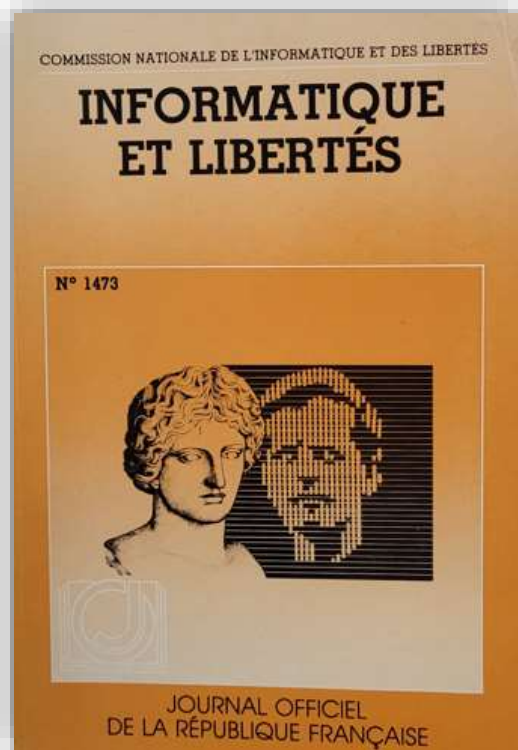
Images générées avec Midjourney par Gaston Gautreneau

La cybersécurité, c'est quoi ?

- État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace 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.

Solenn Le Her
Radio France

Publié le 11/02/2024 10:00



Sur les 581 incidents informatiques recensés l'an dernier par l'Agence du numérique en santé dans les hôpitaux et établissements médico-sociaux, la moitié environ concerne des cyberattaques. (DROUOT / AGF / FRANCE PRES / AP) / © Tempus de la culture - Anis

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

franceinfo
Cybersécurité : trois questions après la cyberattaque contre Free et la fuite de données bancaires
Caroline Louchard
Radio France
Publié le 02/02/2024 09:45

franceinfo senior
Philippe Huet
Le dimanche 6 10h25
Abonner

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

Philippe Huet
Radio France

Publié le 25/02/2024 23:40



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 AP
France Télévisions

Publié le 26/02/2024 12:48



L'adoption des Nations Unies au siège de l'Organisation Internationale à New York (Etats-Unis), le 26 juillet 2024. (MAGUS KUNZECKI / AP) / © Tempus de la culture - Anis



Free a été victime d'une cyberattaque d'ampleur qui a entraîné "l'accès non autorisé" à de nombreuses données personnelles de ses clients, dont leur IBAN.

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

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 de dirigeants.

Nouveau monde
Benoît Vignat
Le samedi 2 10h25, 17h30, 19h30 et 21h30, le dimanche 3 10h25 et 19h30
Abonner

franceinfo - Nicolas Arpagian
Radio France

Publié le 02/02/2024 10:34



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.



A partir d'ici, l'Europe impose à davantage d'entreprises de garantir une cybersécurité forte aux hackers. (MAGUS KUNZECKI / AP) / © Tempus de la culture - Anis

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
- [Utiliser des adresses e-mail professionnelles](#)
 - Usurpation d'identité simplissime permettant de générer toutes sortes d'attaques

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

Remédiation

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

Exemples de phishing (e-mail ou SMS)

NETFLIX
Votre compte est suspendu.
Cher(e) utilisateur,
Désolé pour l'interruption, mais nous rencontrons des problèmes avec vos informations de facturation actuelles.
Nous réessaierons, mais en attendant, vous devrez peut-être mettre à jour vos informations de paiement. Vous pourrez récupérer votre compte juste après avoir mis à jour vos informations.
[Mettre à jour vos informations](#)
Besoin d'aide ? Nous sommes là. Visitez le [Centre d'aide](#) ou [contactez-nous](#) dès maintenant.
L'équipe Netflix

BNP Paribas : Plus que 24h pour activer votre nouvelle Clé Digitale.
Procédez en cliquant ici:
[https://notif-bnp.\[redacted\]](https://notif-bnp.[redacted])

Ameli : Votre carte vitale expire. Effectuez son renouvellement avant le 08/10/22. Rendez-vous sur : assurancemaladie-profil.com/?id=1

Assurance Maladie : Expiration de votre carte vitale, un agissement de votre part est requis. Cliquez ci-dessous: [assur-ame\[redacted\]](https://assur-ame[redacted])

île de France mobilités
Bonjour,
Nous vous contactons pour vous informer que le prélèvement automatique pour votre Pass Navigo a été rejeté.
Pour continuer à bénéficier de nos services, nous vous demandons de régler votre abonnement via carte bancaire.
Vous pouvez accéder à votre compte en ligne sur le lien ci-dessous pour mettre à jour vos informations de paiement.
Nous nous excusons pour tout inconvenient causé et nous vous remercions de votre compréhension.
Équipe IDF-Mobilités
[Régler mon abonnement](#)

La Banque Postale: Veuillez réactiver le service Certicode Plus sur [certi\[redacted\]](https://certi[redacted]) pour éviter la suspension de votre compte

edf CHANGER L'ENERGIE ENSEMBLE
Cher(e) Client(e),
Nous avons remarqué que votre dernière facture est impayée.
Afin de régler votre situation veuillez vous référer ci-dessous :
[Pour résoudre ce problème maintenant](#)
En cas d'échec de règlement de votre situation, nous procéderons à la suspension de votre fourniture d'énergie. Cette intervention vous sera facturée.
Cordialement,
edf bleu ciel

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 pièce 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 « Carte de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la vérification d'un moyen d'identification électronique dénommé « Identification en ligne certifiée sur mobile »

Direction du programme interministériel 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.

Gardez la maîtrise de vos données d'identité

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.

**Sur Internet aussi vous pouvez être témoin
ou victime d'une infraction**

Violence, mise en danger des personnes, menace ou apologie du terrorisme, injure ou diffamation,
incitation à la haine raciale ou discrimination, atteintes aux mineurs :

je ne partage pas, je signale à PHAROS !

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.



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](#).

Signaler une fraude à la carte bancaire (Perceval) (Démarche en ligne)

Ministère chargé de l'intérieur

Service accessible via [FranceConnect](#). Préparez vos identifiants et votre numéro de carte bancaire.

Ce service permet de signaler une fraude à la carte bancaire si vous remplissez les conditions suivantes :

- Vous êtes toujours en possession de votre carte bancaire
- Vous n'êtes pas à l'origine des achats en ligne
- Vous avez déjà fait opposition à la carte auprès de votre banque



Accéder à la démarche en ligne

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.

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.

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 opérations.

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 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. [↗](#)

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.

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.

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

Les bons réflexes

The screenshot displays a grid of application cards from an Android app store. The top row features three cards: 'KEEPASS 2 ANDROID' by Philipp Crocoll (Croco Apps) with a 4.4 star rating; 'KPass: password manager' by Korovan with a 4.7 star rating; and 'KeePassDX - FOSS Password Safe' by Kunzisoft with a 4.4 star rating. The bottom row shows 'Keepass2Android Offline' by Philipp Crocoll (Croco Apps) with a 4.6 star rating, 'KeePassDroid' by Brian Pellin with a 4.0 star rating, and 'KeyPass' by Yogesh Paliyal. A large, semi-transparent window for 'KeePass Password Safe' is overlaid on the right side, showing the official website with navigation links like 'Home & News', 'Forums', 'Feature List', and 'Screenshots', and news items such as 'KeePass 2.57.1 released' and 'KeePass 2.57 released'.

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.

Tous concernés par ces enjeux



Comment protéger ses enfants des risques numériques ?



LES BONNES PRATIQUES

- Parlez régulièrement de sécurité en ligne avec eux,
- Apprenez-leur à ne pas partager leurs mots de passe, à identifier les menaces et à respecter les bonnes pratiques de sécurité,
- Aidez-les à bien paramétrer leurs comptes en ligne,
- Activez le contrôle parental sur les appareils utilisés par vos enfants en leur expliquant que c'est pour limiter et contrôler leur exposition aux risques.

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.



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

4 EN LIEU SÛR, UNE COPIE DE VOS DONNÉES VOUS CONSERVEREZ



BONNE PRATIQUE

- Penser à faire régulièrement des sauvegardes de vos données sur un autre support (clé USB, disque externe, cloud...) pour pouvoir les retrouver en cas de problème.

CNIL.

CYBER RÉFLEXES

Se protéger sur Internet

2 LES MISES À JOUR DE VOS APPAREILS SANS TARDER VOUS FEREZ

Les fabricants de logiciels, applications et matériels vous proposent des mises à jour régulières pour les protéger. Ils peuvent les utiliser pour améliorer vos données personnelles ou les logiciels.

BONNES PRATIQUES

- Faire les mises à jour des logiciels, applications et matériels, dès qu'elles sont proposées pour corriger leurs failles de sécurité.
- Activer les options de mises à jour automatiques chaque fois que c'est possible.

4 FAIRE UNE COPIE DE VOS DONNÉES EN SÛR

Copier les données, c'est les sauvegarder pour éviter de les perdre en cas de problème, de vol, de panne ou de casse de vos appareils.

BONNE PRATIQUE

- Prendre à l'aise régulièrement des sauvegardes de vos données sur un autre support (clé USB, disque externe, cloud...) pour pouvoir les retrouver en cas de problème.

6 LES CONTENUX PRÉVUS DE VOS APPAREILS EN SÛR

Des virus peuvent pénétrer les appareils de nos ordinateurs sans même nous en rendre compte. Ils peuvent voler nos données, les transmettre de proche en proche, les utiliser pour commettre des actes de malveillance.

BONNES PRATIQUES

- Ne pas télécharger des contenus logiciels et des applications non vérifiées.
- Vérifier régulièrement les paramètres de sécurité des appareils de nos ordinateurs.

1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE VOUS CHOISIREZ

Un mot de passe n'est efficace que si on ne le partage pas, s'il est suffisamment long, complexe et différent des autres mots de passe que vous utilisez.

BONNES PRATIQUES

- Utiliser des mots de passe suffisamment longs, complexes et différents des autres mots de passe que vous utilisez.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

3 EN LIGNE, LE MOINS POSSIBLE SUR VOTRE IDENTITÉ VOUS DIREZ

Publier ou partager des données personnelles en ligne (photo, vidéo, adresse mail, adresse, numéro de téléphone, etc.) peut être risqué si on ne vérifie pas les paramètres de confidentialité.

BONNES PRATIQUES

- Éviter de divulguer vos données personnelles en ligne (photo, vidéo, adresse mail, adresse, numéro de téléphone, etc.) si on ne vérifie pas les paramètres de confidentialité de ses comptes pour définir ce qui peut être visible par les autres.

5 DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS VOUS MÉFIEREZ

L'arnaque est le principal moyen de fraude en ligne. Elle consiste à tromper les victimes en leur faisant croire qu'elles ont gagné un concours, qu'elles ont gagné un prix, qu'elles ont gagné un concours, etc.

BONNES PRATIQUES

- Toujours se méfier et ne pas se précipiter pour cliquer ou répondre.
- Vérifier toujours l'information par vous-même, en vous connectant à votre compte sur le service concerné.



3 EN LIGNE, LE MOINS POSSIBLE SUR VOTRE IDENTITÉ VOUS DIREZ



BONNES PRATIQUES

- Éviter de divulguer vos données personnelles et celles de vos connaissances.
- Vérifier les paramètres de confidentialité de vos comptes pour définir ce qui peut être visible par les autres.

CNIL.

5 DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS VOUS MÉFIEREZ



BONNES PRATIQUES

- Toujours se méfier et ne pas se précipiter pour cliquer ou répondre.
- Vérifier toujours l'information par vous-même, en vous connectant à votre compte sur le service concerné.

CNIL.

1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE VOUS CHOISIREZ



BONNES PRATIQUES

- Utiliser des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

CNIL.

2 LES MISES À JOUR DE VOS APPAREILS SANS TARDER VOUS FEREZ



BONNES PRATIQUES

- Faire les mises à jour des logiciels, applications et appareils, dès qu'elles vous sont proposées pour corriger leurs failles de sécurité.
- Activer les options de mises à jour automatiques chaque fois que c'est possible.

CNIL.

Ressources pour les particuliers

<https://www.cnil.fr/fr/se-protger-sur-internet-avec-les-cyber-reflexes>



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

Ressources pour vous

Autres ressources



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

Faites des mises à jour régulières

Utilisez des mots de passe différents par service

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

CNIL.

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>