CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

Les principes de base de la protection des données personnelles

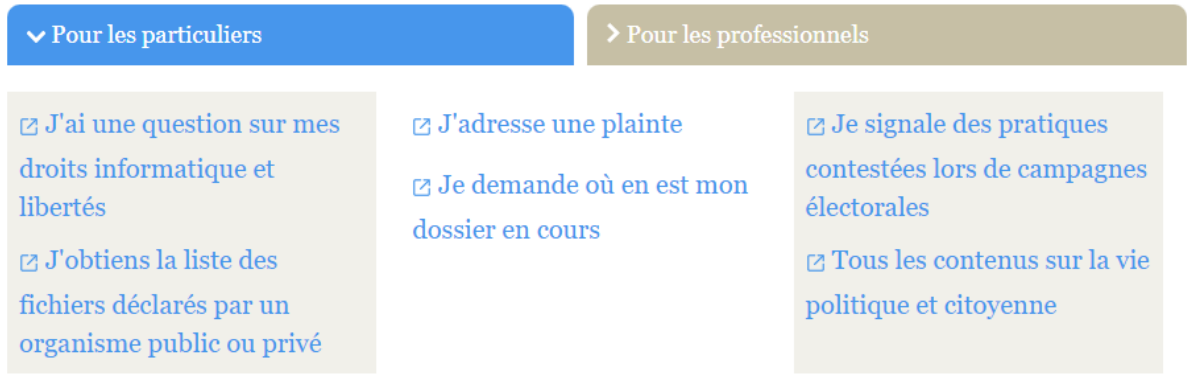
Webinaire pour les conseillers numériques
Mardi 28 juin 2022

CNIL.

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

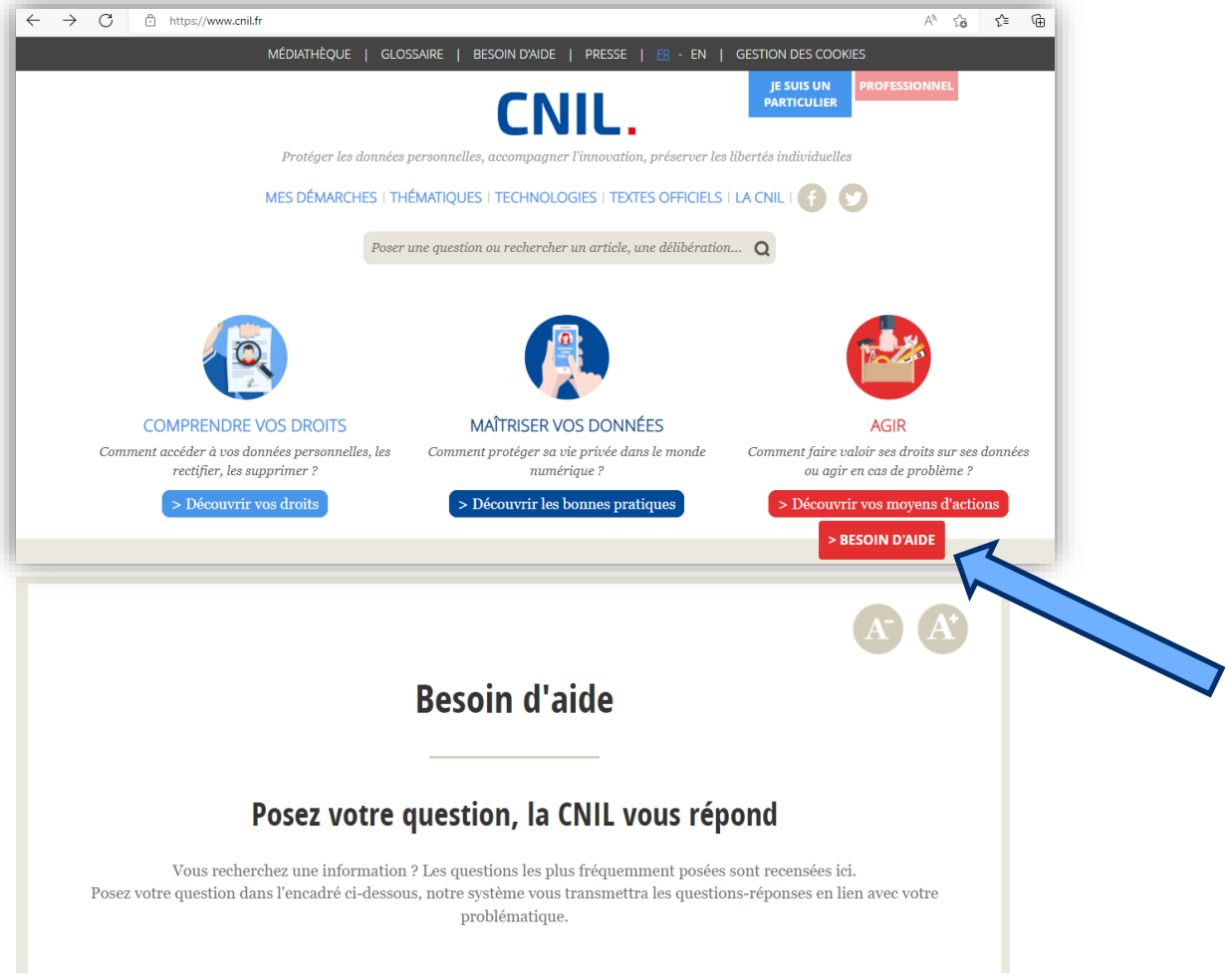
- **Autorité Indépendante**
- **Quatre missions principales**
  - Informer les personnes et protéger leurs droits
    - Lundi, mardi, jeudi, vendredi de 10h à 12h par téléphone : 01 53 73 22 22
    - En ligne : Contacter la CNIL : standard et permanences téléphoniques | CNIL
    - Par courrier postal :

    Commission nationale de l'informatique et des libertés
    3 Place de Fontenoy
    TSA 80715 - 75334 PARIS CEDEX 07
  - Accompagner la conformité et conseiller
  - Anticiper et innover
  - Contrôler et sanctionner



Cnil.fr

Point d'entrée : particuliers (la personne concernée par le fichier)



Cnil.fr

Point d'entrée : professionnels

Les personnes ont des droits

EFFACEMENT

OPPOSITION

ACCÈS

DÉRÉFÉRENCEMENT

PORTABILITÉ

INFORMATION

RECTIFICATION

Les personnes ont des droits

- Droit d'**information** : un organisme qui collecte des données sur les personnes doit proposer une information claire sur l'utilisation des données et sur leurs droits
- Droit d'**accès** : obtenir et vérifier les informations qu'un organisme détient sur elles
- Droit de **rectification** : rectifier les informations inexactes qui les concernent
- Droit d'**opposition** : s'opposer à tout moment à ce qu'un organisme utilise certaines de leurs informations
- Droit au **déréférencement** : ne plus associer leur nom-prénom à un contenu visible dans un moteur de recherche
- Droit à **l'effacement** : effacer des informations qui les concernent
- Droit à la **portabilité** : emporter une copie de leurs informations pour les réutiliser ailleurs

MOTS DE PASSE

Doctrine CNIL

- Il n’existe pas de définition universelle d’un bon mot de passe, mais sa complexité et sa longueur permettent de diminuer le risque de réussite d’une attaque informatique.
- On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères.

👋 https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

Conseils CNIL

Conseils CNIL

Poster à votre disposition

Conseils CNIL

- Ne jamais donner par mails mots de passe, identifiants, numéro de carte bleue.
- Changer de mot de passe sans hésiter
- Avoir un mot de passe différent pour chaque service utilisé : courrier, réseaux sociaux, sites de vente en ligne etc…

PHISHING

Le phishing : détecter un message malveillant

- Par messagerie ou par mail, des personnes malintentionnées tentent de mettre la main sur les données personnelles en utilisant des techniques d'hameçonnage (phishing) ou d'escroquerie. Ces techniques évoluent constamment.

- L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

- Par exemple, le fraudeur se fait passer pour un organisme connu (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il envoie un mail demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment les coordonnées bancaires (numéro de compte, codes personnels, etc.).

  Attention : il ne faut jamais répondre à ces messages, ne pas cliquer sur les liens, ne pas ouvrir les pièces jointes !

Les étapes d'une attaque de phishing

- Une tentative de phishing se compose généralement de quatre phases :

1. Envoi de faux mails
En exploitant un botnet, le pirate envoie des dizaines de milliers d'e-mails qui simulent, dans les graphiques et le contenu, les communications d'une banque, d'un fournisseur Web, d'un site d'enchères en ligne ou de toute autre institution connue de l'utilisateur.

2. Réception du message
Dans le message électronique, on vous signale un problème de sécurité, une demande de validation de remboursement ou encore une confirmation de facture. Il est alors demandé de vérifier votre compte ou de vous connecter en cliquant sur un lien dans le texte du courrier électronique.

3. Accès au faux site
Le lien fait cependant référence à un site fictif, hébergé sur un serveur contrôlé par le phisher, et qui reproduit parfaitement l'apparence du site institutionnel, de la banque ou du portail d'enchères en ligne.

4. Réception des informations d'identification
Une fois connecté sur le site de copie, les données sont stockées dans la base de données du serveur de l'attaquant, qui peut en disposer à sa guise et les revendre. Il se peut aussi qu'en visitant le faux portail, il soit infecté par des chevaux de Troie et des logiciels malveillants de différents types : dans ce cas, l'objectif est de prendre possession de nouveaux ordinateurs afin d'enrichir la machinerie de botnet utilisée pour mener l'attaque.

CNIL non compétente

- Ces procédés ne sont pas liés à la protection des données personnelles : ce sont des tentatives d'escroquerie ou d'extorsion de fonds.
- La CNIL n'est donc pas compétente.
- Que faire ?
  - **Signaler les escroqueries auprès du site www.internet-signalement.gouv.fr**, la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements.
  - **Pour s'informer sur les escroqueries** ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : contacter Info Escroqueries au 0 805 805 817 (numéro vert - appel gratuit depuis la France) du lundi au vendredi de 9 h à 18 h 30.
  - **Rendez-vous sur cybermalveillance.gouv.fr** , la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance.

Arnaques par courriel (scam, phishing) : quelles précautions prendre ?

- Voici **quelques règles simples** à respecter pour éviter de communiquer des informations à des groupes criminels :
  - Ne jamais **communiquer d'informations importantes** (numéro de carte bancaire, mot de passe, etc.) en cliquant sur un lien reçu par courrier électronique ;
  - Ne jamais **répondre aux messages suspects** : une banque ne vous demandera jamais de lui communiquer vos coordonnées bancaires par simple courriel. Et il est peu probable qu'un inconnu vous propose réellement de bénéficiez d'un héritage ;
  - **Partez toujours de la page d'accueil d'un site** pour accéder aux autres pages, notamment celles où sont demandés des identifiants ;
  - Quand vous êtes sur un site sécurisé, comme un site bancaire, **vérifiez que le chiffrement des données est activé** : l'adresse du site doit commencer par "https://" (et non "http://") avec un petit cadenas affiché sur la gauche ou en bas de votre navigateur ;
  - En cas de doute, **prenez contact directement avec l'entreprise ou**

Conseils CNIL

Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?

- Est-ce que le message/courriel vous est réellement destiné ? Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.
- Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.
- Attention aux expéditeurs inconnus : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
- Soyez attentif au niveau de langage du courriel : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration ...).

Conseils CNIL

Vérifier les liens dans le courriel : avant de cliquer sur les éventuels liens, laissez votre souris dessus*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouvv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.* *A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.*

Se méfier des demandes étranges : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.

L'adresse de messagerie source n'est pas un critère fiable : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami - par exemple pour récupérer l'accès à son compte - contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

CNIL.

CYBERSECURITE

Sécuriser son poste de travail

Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent un des principaux points d'entrée.

Les précautions élémentaires :

- Prévoir un mécanisme de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné.
- Installer un **« pare-feu »** (*« firewall »*) logiciel, et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
- Utiliser des **antivirus régulièrement mis à jour** et prévoir une politique de **mise à jour régulière des logiciels**
- Configurer les logiciels pour que les **mises à jour de sécurité se fassent automatiquement** dès que cela est possible.

Sécuriser son poste de travail

- **Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme** plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation.
- **Limiter la connexion de supports mobiles** (clés USB, disques durs externes, etc.) à l'indispensable.
- Désactiver l'exécution automatique (« *autorun* ») depuis des supports amovibles.
- Pour l'**assistance sur les postes de travail :**
- Les outils d'administration à distance doivent **recueillir l'accord** de l'utilisateur avant toute intervention sur son poste, par exemple en répondant à un message s'affichant à l'écran ;
- L'utilisateur doit également pouvoir **constater si la prise de main à distance est en cours** et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

Gestionnaires de mots de passe

- Les coffres-forts numériques (comme Keepass) sont des logiciels installés sur votre ordinateur. Pour vous connecter à vos comptes en ligne, ouvrez le gestionnaire en entrant votre mot de passe maître, puis copiez-collez votre identifiant et mot de passe dans le champ de connexion.
- D'autres gestionnaires sont directement intégrés ou intégrables à votre navigateur et hébergent vos mots de passe dans le *cloud* ou sur votre disque dur. Certains remplissent automatiquement les champs « identifiant » et « mot de passe » de vos comptes en ligne en vous demandant simplement, une fois par session, votre mot de passe maitre pour ouvrir votre base.

Conseils CNIL

L'éducation au numérique, un axe stratégique

- La CNIL

« favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement. Les activités spécifiquement destinées aux enfants font l'objet d'une protection particulière ». (art. 57 b du RGPD)

L’atelier RGPD de la Cnil

- Le MOOC de la CNIL est de retour dans une nouvelle version enrichie
- L’atelier RGPD est une formation en ligne gratuite, illimitée et ouverte à tous (Mooc).
- Elle permet de sensibiliser les professionnels à la protection des données et d’accompagner leur mise en conformité.
- Dans cette nouvelle version, la CNIL propose un nouveau module dédié aux collectivités territoriales.