En direct du CSE Exceptionnel du 28 janvier 2026

Protection des données, sécurité et conditions de travail

Concernant la CONSERVATION des données, France Travail sépare ses données en 2 sous catégories :

- Les données SYSTEME liées aux dossiers des Demandeur d'Emploi et de ChatFT qui sont domiciliées en France dans nos propres serveurs en France
- Les données liées à Microsoft (Office, Excel, Teams,…) qui elles sont quant à elles sur les serveurs privés.

Pour ces dernières, nous sommes comme tous les autres utilisateurs soumis au régime d'extraterritorialité des Etats Unis, avec tout ce que cela peut signifier au regard de l'actualité récente…

Les cyberattaques, c'est quoi ?

On en identifie 3 grands types :

- Vol de données (informations personnelles parfois sensibles)
- Fraude financière (usurpation d'identité, transaction illégales)
- Blocages du système (interruption de service contre rançon)

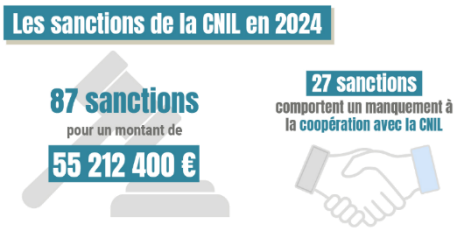
Et 3 types d'acteurs

- Groupes criminels (recherche d'argent)
- Menace étatique (espionnage et déstabilisation)
- Menace isolée (idéologie, vengeance, …)

A **titre personnel, nous sommes tous aussi exposés** à ce risque par le biais des mails ou SMS frauduleux, QR codes piégés, liens suspects dans les messages, voire la perte du téléphone. D'après les données de la CNIL, **le coût moyen pour un particulier est de 700€**

A France Travail

Nous subissons des attaques régulièrement, les systèmes de détection repèrent plus facilement les attaques de grande ampleur (transfert massif de données) et horaires incongrus. Dans ce cas le transfert est immédiatement stoppé. Les systèmes évoluent en permanence pour s'adapter aux différentes menaces. Une veille est également faite sur le darkweb pour identifier des éventuelles apparitions de données.



En cas de cyberattaque, FT informe la CNIL et les usagers concernés. Suite aux attaques de 2025, **la CNIL est cours d'investigations pour une éventuelle sanction** qui pourrait se chiffrer en millions d'euros si on se réfère à celle de 42 M€ infligée à Free au début du mois.

Le partage de données erroné fait l'objet d'une déclaration à la CNIL via la DG.

La **responsabilité d'un agent** qui activerait par mégarde un lien corrompu **n'est pas engagée à titre individuel**, c'est l'Etablissement qui en portera la responsabilité. D'où les moyens de sensibilisation et de formation mis en œuvre depuis plusieurs années pour éviter à chacun de tomber dans le piège.

Lors du télétravail, la connexion obligatoire via IVANTI garantit la sécurité des transferts de données des usagers, la double authentification via les téléphones professionnels également.

En 2025

France Travail a subi 4 attaques majeures :

- Juillet : KAIROS fuite de données de 340.000 DE (via un centre de formation en Rhone Alpes)
- Aout : KAIROS fuite de données de 571.000 recruteurs (via un autre centre de formation en Rhone Alpes)
- Octobre : 34.000 espaces personnels piratés via des logiciels malveillants installés dans les ordinateurs des DE
- Novembre : 1,6 millions de dossiers de jeunes (via la Mission Locale à la Réunion)

3 de ces 4 attaques ont été faites par **l'obtention des codes d'accès et mots de passe d'un opérateur**. Les intrusions dans le système informatique directement par un hacker sont rares et exigent des compétences pointues et peu répandues.
Pour réduire ces risques, les usagers doivent maintenant utiliser une **double authentification** ce qui va réduire les risques puisque toute tentative de connexion sera accompagnée d'un mail d'information.

Retrouvez nos informations : http://www.cfecgc-metiersdelemploi.fr

bez ici]

En direct du CSE Exceptionnel du 28 janvier 2026

Protection des données, sécurité et conditions de travail

CFE-CGC Métiers de l'Emploi Centre-Val-de-Loire

Le Plan d'action

Plusieurs mesures d'ordre technique sont en cours de déploiement :

- Mise en place d'une double authentification pour l'accès à notre SI pour les partenaires
- Limitation de l'accès aux dossiers des demandeurs d'emploi radiés depuis plus de 10 ans
- Mise en place d'une double authentification pour la connexion sur les espaces personnels demandeurs d'emploi (janvier 2026 pour CVL)
- Suivi obligatoire pour les partenaires d'une formation tous les 6 mois sous peine de perdre son habilitation au SI (déploiement premier semestre)
- Autres mesures à venir :
    - Compartimentation (Restriction d'accès aux demandeurs d'emploi du territoire)
    - Minimisation (Suppression de la recherche individu par NIR)

Et des mesures de sensibilisation et de formation interne et externe :

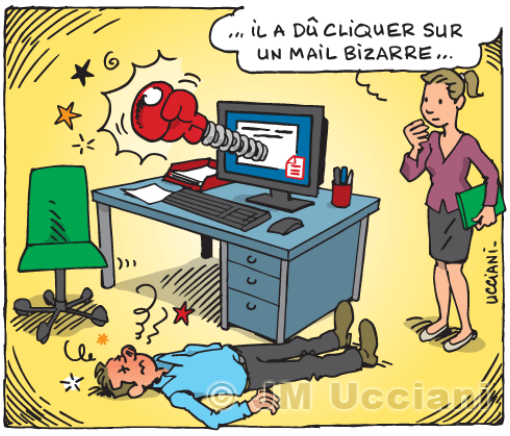
- Intervention en réunion de service en agence (100 % des agences sensibilisées en 2024 et 2025)
- Article Intranet sur les appels frauduleux publié en mars et republié en septembre 2025
- Promotion de la formation RGPD : Protégez les données, comprenez les enjeux disponibles sur l'académie France Travail
- Inscription de la formation « Cybermalveillance tous concernés » dans le Plan de Développement de Compétences Régional de 2026
- Sensibilisation des partenaires sur les enjeux et risques liés à la cybersécurité (1er semestre 2026).
- Information des usagers sur francetravail.fr sur les actes de cybermalveillance
- Sensibilisation des organismes de formation sur les appels au faux technicien support
- Campagne de communication interne via l'intranet

Le Cybermois

En 2025, un test auprès de 15.000 conseillers de France Travail a été mis en place par l'envoi de faux mails frauduleux :

- **41,02 % des personnes ont cliqué sur un lien qui aurait pu être malveillant**
- **59,02 % des personnes ont téléchargé un code (malveillant) ou ont donné leur mot de passe**

On se rend bien compte que malgré la sensibilisation et la formation, nous restons collectivement fragiles sur le sujet ! Ce genre de test de grande ampleur est un moyen fiable de mesurer nos progrès en la matière.



Prochain CSE ordinaire cet après midi

bez ici]