

## Cyberattaque contre la Caisse de compensation Swissmem – lettre d'information pour les collaborateurs/rices des entreprises affiliées

Mesdames, Messieurs,

Nous nous adressons à vous par ce courrier pour vous signaler un incident de sécurité survenu à la Caisse de compensation (CC) Swissmem. Vous êtes salarié/e d'une entreprise affiliée à la Caisse de compensation Swissmem.

Malgré des normes de sécurité accrues, notre organisation a été victime de ce que l'on appelle une cyberattaque. On entend par là la tentative de la part de groupes criminels d'accéder aux systèmes de technologie de l'information (TI) d'organisations ou d'entreprises afin de soustraire, d'effacer ou de crypter des données stockées sur des ordinateurs. Lorsque nos experts ont découvert l'incident le week-end du 4-5 janvier 2025, les systèmes ont été immédiatement débranchés du réseau extérieur. Après une interruption, les systèmes informatiques entièrement reconfigurés fonctionnent à nouveau normalement, depuis le jeudi 9 janvier 2025.

Des mesures d'analyse et de sécurité approfondies ont été immédiatement mises en place avec le soutien de spécialistes externes. Les instances juridiquement compétentes telles que le Préposé fédéral à la protection des données et à la transparence (PFPDT), l'Office fédéral des assurances sociales (OFAS) et l'Office fédéral de la cybersécurité (OFCS) ont été informées et consultées. La CC Swissmem a en outre déclaré cette attaque à la police cantonale de Zurich et a déposé une plainte pénale. L'analyse effectuée jusqu'à présent a montré que lors de l'attaque, des données de la CC Swissmem ont été cryptées et bloquées. Toutes les données ont cependant pu être restaurées. Il n'y a pas eu d'attaque sur les comptes bancaires et aucun argent n'a été détourné.

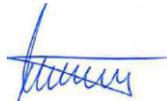
**Malheureusement, il est désormais certain que les auteurs de l'attaque ont soustrait des données.** Il pourrait s'agir de différents types de données : d'informations sur l'activité de gestion de la CC Swissmem jusqu'à des données personnelles, y compris les données sur les prestations ou les cotisations. Il n'est pas clair à ce stade de quelles données il s'agit. **Par conséquent, il est actuellement impossible de savoir si des données vous concernant personnellement ont été touchées ou non.** Jusqu'à présent, il n'existe aucun indice d'une utilisation abusive ou d'une publication des données par les cybercriminels.

**Néanmoins, nous vous recommandons une extrême vigilance : soyez particulièrement prudents envers des correspondances, des courriels, des messages ou des appels téléphoniques suspects qui vous réclament des informations personnelles ou vous incitent à des actions douteuses. Ne communiquez en aucun cas des données personnelles ou des coordonnées bancaires sans la moindre précaution. Vous trouverez des recommandations concrètes au verso.**

Nous regrettons sincèrement cet incident et nous excusons pour les inconvénients et les problèmes qui en découlent. Nous ne pouvons pas, en revanche, fournir davantage d'informations sur l'incident, notamment sur les données concernées.

Meilleures salutations

**Caisse de compensation Swissmem**



Thomas Sommer  
Président



Damian Keller  
Gérant

→ Veuillez consulter le verso / la page suivante

## Consignes de sécurité et de conduite

- **Soyez particulièrement prudent/e face aux correspondances, aux courriels, aux messages ou aux appels téléphoniques suspects qui vous demandent des informations personnelles ou vous incitent à des actions douteuses.**
- **Ne cliquez pas sur les liens contenus dans les courriels ou les SMS qui vous sont envoyés sans que vous les ayez réclamés ou qui vous donnent un sentiment étrange. Cela vaut en particulier si ces messages vous mettent sous pression et/ou vous menacent de représailles.**
- **Ne vous laissez pas intimider ou mettre sous pression.**
- **Ne communiquez jamais vos mots de passe ou votre code PIN par téléphone ou par courriel.**
- **Ne communiquez en aucun cas des données personnelles ou des coordonnées bancaires sans la moindre précaution.**
- **Ne permettez jamais à des inconnus d'accéder à votre ordinateur, même s'ils vous semblent dignes de confiance.**
- **Ne remettez jamais d'argent liquide ou d'autres objets de valeur à une personne qui vous est inconnue.**

**En cas de doute, l'Office fédéral de la cybersécurité (OFCS) est à votre disposition pour vous aider à évaluer la situation et vous donner des recommandations sur la marche à suivre : <https://www.report.ncsc.admin.ch/fr/>.**

**Si vous avez été victime d'une escroquerie et que vous avez subi une perte financière ou si vous êtes menacé(e) ou victime de chantage, portez plainte auprès de la police cantonale compétente, en cas d'urgence au [cckova@kapo.zh.ch](mailto:cckova@kapo.zh.ch), 112 ou au 117.**