Fraude au virement de salaire : comment réagir et que faire ?

23 juillet 2025

Régulièrement, la CNIL publie des exemples de violations de données inspirés de faits réels pour aider les professionnels à comprendre les risques et à mieux les prévenir. L'approche décrite reflète un cas réel vécu par un ***responsable de traitement****.*

Consulter la version PDF

L'histoire de Célestin

Le bon, la fraude et le truand

Célestin travaille pour un grand distributeur d'articles de sport et de loisirs, il n'aime pas particulièrement la technologie. Célestin affectionne les choses simples et essentielles : la montagne et la pêche.

Célestin fait tout de même quelques concessions et a adopté les téléphones dits intelligents, même s'il n'a pas besoin d'une IA pour reconnaitre un edelweiss ou une truite de banka.

Aujourd'hui, chez le boulanger du quartier, son paiement a été refusé. Heureusement, il a toujours du liquide sur lui et peut repartir avec ses pâtisseries.

Agacé par la situation, Célestin contacte son banquier afin de lui faire part de son mécontentement. Ce dernier vérifie les opérations et comptes de son client et découvre l'anomalie : Célestin n'a pas reçu son salaire ce mois-ci, les fonds sont donc insuffisants.

Célestin contacte alors immédiatement les ressources humaines de son entreprise et explique la situation.

Une première vérification est effectuée et les RH confirment que le salaire a bien été versé à Célestin . Et sur son nouveau compte, comme il l'avait demandé ! Célestin bondit de sa chaise : il n'a jamais demandé à changer de banque ! Il s'est fait « comptejacker » !

Comment réagir ?

L'enquête interne

Une solution va être trouvée rapidement.

Pendant que le service RH s'occupe de lui, Robert, le nouveau responsable de la gestion des risques de la société, enquête et reconstitue rapidement les circonstances de l'incident.

Robert vérifie tout d'abord la demande supposément envoyée par Célestin. Un mail a effectivement été reçu par le service RH de l'entreprise. Si le nom affiché dans l'outil courriel est bien Célestin, il provient en réalité d'une boîte aux lettres externe à l'entreprise. Effectivement, Robert découvre en analysant l'en-tête du courriel que le nom de domaine utilisé est celui d'une grande plateforme gratuite de courriel en ligne. Après vérification auprès de Célestin, ce dernier confirme que cette adresse ne lui appartient pas. Malheureusement, cette demande a bien été traitée. Robert analyse le courriel et note le RIB utilisé ainsi que l'organisme bancaire d'où il est issu.

Suivant son instinct, Robert continue son enquête. Accompagné par le service RH qui exploite cette boîte de service, il lance des recherches au sein des messages reçus concernant les demandes de changement de compte bancaire. À partir du RIB ainsi que du nom l'organisme utilisé par le fraudeur, ils découvrent trois autres demandes suspectes. La fraude n'a pas visé que Célestin. Heureusement pour l'entreprise, ces dernières demandes n'ont pas encore été traitées car reçues après la mise en paye des salaires. Le service RH va contacter les « demandeurs » afin de vérifier ce qu'il en est réellement.

Comment ces personnes ont-elles été ciblées ? Robert découvre rapidement que Célestin et les trois autres employés ont été mis en avant dans le magazine publicitaire de l'entreprise du mois précédent. Les identités ont été tirées de ce dernier.

Robert rassemble les éléments, remet son rapport et dépose une plainte auprès des forces de l'ordre. L'organisme ne dispose pas de **délégué à la protection des données (DPO)**, Robert réalise une analyse et identifie que l'incident constitue une **violation de données** personnelles engendrant un risque élevé pour les personnes.

La notification de la violation à la CNIL et l'information aux personnes concernées

En concertation avec sa direction, Robert se charge de gérer cette **violation de données personnelles**. Il dispose de **72 heures** depuis la découverte de l'incident afin de réaliser une notification de l'incident auprès de la CNIL.

Après consultation du site de la CNIL, Robert comprend comment s'y prendre :

1. Documenter et notifier à la CNIL

Il consolide les informations collectées et **documente cet incident comme une violation de données personnelles**. Après analyse et consultation des conseils de la CNIL sur le sujet, il lui notifie la violation de données.

2. Informer les personnes

Les données impactées ne sont pas sensibles au sens de la loi. Cependant, le risque est à considérer comme élevé, vu l'impact possible pour les droits et libertés des personnes. Il **rédige un message d'information à destination des employés concernés**, en donnant les informations obligatoires : les circonstances de l'incident, la nature des données concernées, le point de contact pour avoir des informations supplémentaires, les mesures déjà prises et envisagées ainsi que les conséquences possibles pour les personnes concernées, dans ce cas précis, le vol de données bancaires.

Après avoir contacté la cellule violation de la CNIL (violations@cnil.fr) pour s'assurer que l'information soit la plus claire possible pour les destinataires, il est décidé de l'écrire sous la forme de réponses aux questions suivantes :

- « Que s'est-il passé ? »
- « Comment avons-nous réagi ? »
- « Quelles données sont concernées ? »
- « Quelles sont les conséquences possibles ? »
- « Quelles sont nos recommandations ? »
- et « Qui contacter si vous avez des questions ? ».

3. Éviter que la situation ne se reproduise

Une fois la crise gérée, Robert et le service RH mettent en place une procédure qu'il conviendra maintenant de suivre :

- Lorsque des changements des données personnelles d'employés sont demandés au service RH, il faudra le faire via le portail RH sécurisé mis à disposition des employés et accessible depuis le réseau interne de l'entreprise (ou depuis l'accès VPN pour ceux bénéficiant du télétravail). Ce portail va être retravaillé afin de permettre aux employés d'effectuer les changements et corrections basiques de leur dossier RH.

- S'agissant des demandes de changements de RIB, la demande devra être faite en présentiel ou provenir obligatoirement d'une adresse interne de l'entreprise suivie d'une levée de doute par visio, notamment pour les personnes n'étant pas sur le site principal.

- Les services et Robert testent cette procédure puis la diffusent auprès des salariés.

Comment limiter ce risque ?

☐ Limiter l'exposition des données personnelles sur les réseaux. Moins d'exposition réduit le risque.

☐ Mettez en place des procédures organisationnelles, faites connaître les procédures et appliquez-les !

Pour approfondir

- Les violations de données personnelles
- Les violations du moment
- Tous les contenus sur la cybersécurité