CORPORATE
JANVIER 2026

#ACTUALITES

Cyberattaques : La Poste ciblée comme jamais

On vous dit tout !

Depuis le 22 décembre 2025, **La Poste a fait face à une cyberattaque d'une ampleur exceptionnelle,** après une succession de tentatives tout au long de l'année 2025. Elle a fortement perturbé plusieurs services, notamment La Banque Postale, Colissimo et Digiposte, impactant à la fois les clients, les postières et postiers.

Dans ce contexte, la CFE-CGC tient à saluer l'engagement remarquable des cadres, experts, ingénieurs, managers et fonctions support, qui ont été en première ligne pour sécuriser les systèmes, piloter les cellules de crise et garantir la continuité du service public, les collègues mobilisés au sein des bureaux de poste, des centres de distribution qui ont œuvré sans relâche pour assurer la continuité d'activité dans un contexte particulièrement dégradé.

UN DEFICIT D'INFORMATION

La CFE-CGC regrette une communication interne et externe insuffisante qui ne permet ni aux représentants du personnel ni aux salariés de disposer d'une vision claire de la situation.

La gestion de crise ne peut reposer durablement sur l'engagement individuel et le sens du devoir.

CE QUE LA CFE-CGC SAIT A CE STADE

Sur la base des éléments portés à notre connaissance :

- Il s'agit d'une attaque par déni de service distribué (DDoS), visant à saturer les infrastructures informatiques par un volume massif de requêtes.
- Selon le Directeur de la Sécurité de La Poste : « jusqu'à 2,5 milliards de paquets de données par seconde » ont été enregistrés *(source : article Clubic du 24 janvier 2026 — « La Poste a affronté la plus grande cyberattaque DDoS jamais enregistrée en France »).*
- Malgré cette attaque :
  - Les paiements par carte bancaire en bureau de poste sont restés opérationnels,
  - Les virements via la solution Wero ont continué à fonctionner.

QUELLES MOTIVATIONS POSSIBLES ?

Les cyberattaques contre une institution comme La Poste peuvent répondre à plusieurs objectifs :

- **Financiers :** tentative d'extorsion ou de revente de données ➜ à ce stade, aucune donnée n'aurait été volée.
- **Perturbation des services publics :** création de désorganisation et de mécontentement.
- **Espionnage :** intérêt potentiel pour des données sensibles.
- **Idéologiques ou politiques :** volonté de fragiliser un acteur majeur du service public.

CFE CGC Groupe La Poste

Dans l'attente des conclusions officielles, **la CFE-CGC observe que cette attaque intervient à un moment symbolique, en période de fêtes, avec pour effet possible de fragiliser la confiance et le moral des citoyens.**

REGLEMENTATIONS EUROPEENNES : DES ENJEUX MAJEURS

• DIRECTIVE NIS2

La directive européenne NIS2 (Network and Information Security) vise à **renforcer la sécurité des systèmes d'information des entreprises essentielles, dont La Poste.**
Elle impose notamment la prévention des incidents, la gestion des crises cyber, la protection renforcée des données.

• REGLEMENT DORA

Le règlement DORA (Digital Operational Resilience Act) concerne spécifiquement les acteurs financiers, dont La Banque Postale et CNP Assurances.
Il vise à **garantir une résilience numérique opérationnelle renforcée face aux cybermenaces.**
Ces réglementations impliquent des obligations fortes :

- **Protection** des données personnelles et sensibles
- **Garantie** de la continuité du service public
- **Prévention** des pertes financières
- **Préservation** de l'image et de la crédibilité du Groupe

LES ENJEUX STRATEGIQUES POUR L'AVENIR DU GROUPE

La cybersécurité n'est plus un sujet technique. **C'est un enjeu de souveraineté, de continuité du service public, d'attractivité des métiers cadres et experts.** Sans reconnaissance claire, sans parcours professionnels valorisés, sans conditions d'exercice soutenables, **le Groupe prend le risque d'un décrochage de ses compétences clés.**

LES DEMANDES DE LA CFE-CGC GROUPE LA POSTE

La CFE-CGC agit pour défendre les salariés face à ces risques croissants et demande :

- **Des moyens** humains, techniques et financiers renforcés en cybersécurité,
- **Une formation** et une sensibilisation de qualité pour l'ensemble des personnels,
- **Une évaluation** régulière des risques et vulnérabilités,
- **Une reconnaissance** financière de l'engagement des collègues mobilisés dans les cellules de crise au sein de la Maison de l'Innovation, en établissement BSCC comme en secteur BGPN/ DODT.

La CFE-CGC a également demandé un retour détaillé en CSE établissement, CSE Central et Conseil d'Administration, portant sur :

- **Les impacts** pour les collègues,
- **Le coût** global de ces cyberattaques (organisation, image, solutions),
- **Les mesures** structurelles envisagées pour éviter leur répétition.

On ne protège pas le Groupe La Poste sans protéger celles et ceux qui le font tenir.

La CFE-CGC restera pleinement mobilisée pour défendre les femmes et les hommes qui portent, au quotidien, la sécurité, la performance et l'avenir du Groupe La Poste.

100% CADRES

100% VOUS

CFE CGC Groupe La Poste

CFE-CGC GROUPE LA POSTE – 90 RUE LAFAYETTE – 75009 PARIS
cgclaposte@gmail.com