N°11
Jeudi 26
Février 2026

IDirection

Cyberattaque contre la plateforme nationale « Choisir le Service Public »

La plateforme « Choisir le service public » a été victime d'une cyberattaque le 28 janvier 2026. Les données personnelles de plus de 377 000 candidats ont été dérobées et mises en vente sur le dark web.

La Fédération des Fonctionnaires FO (FGF-FO) exige des garanties immédiates pour les agents et des moyens renforcés

⇒ **Lire le communiqué (page suivante)**

FÉDÉRATION GÉNÉRALE
DES FONCTIONNAIRES
FORCE OUVRIÈRE

FONCTION PUBLIQUE

46 rue des Petites Écuries - 75010 Paris
01 44 83 65 55
secretariat@fo-fonctionnaires.fr

COMMUNIQUE
Paris, le 17 février 2026

Cyberattaque de la plateforme « Choisir le Service Public »

La FGF-FO exige des garanties immédiates pour les agents et des moyens renforcés

La Fédération Générale des Fonctionnaires Force Ouvrière (FGF-FO) a été informée de la cyberattaque ayant touché la plateforme nationale « Choisir le Service Public », entraînant la divulgation non autorisée de données personnelles et professionnelles d'utilisateurs.

Les données concernées – identité complète, coordonnées, date de naissance, parcours académique et professionnel, aspirations et préférences de mobilité – sont particulièrement sensibles.

Même en l'absence de compromission de mots de passe, les risques d'hameçonnage, d'usurpation d'identité ou de démarchages frauduleux ciblés sont réels.

Cet incident pose plus largement la question de la robustesse des plateformes numériques utilisées par l'administration.

La FGF-FO rappelle que la confiance dans les outils numériques de l'État est essentielle, notamment lorsqu'ils sont mobilisés pour des procédures sensibles telles que le vote électronique lors des élections professionnelles.

Sans préjuger des dispositifs spécifiques mis en place pour ces scrutins, cet événement démontre qu'un haut niveau d'exigence en matière de sécurité, d'audit et de transparence doit être garanti.

La FGF-FO rappelle que la transformation numérique de l'action publique, accélérée notamment par le développement des outils d'intelligence artificielle, impose un renforcement massif et durable des moyens humains, techniques et budgétaires consacrés à la cybersécurité.

La FGF-FO demande :

- La transparence complète sur les circonstances de la violation et ses conséquences réelles ;
- La communication des conclusions de l'analyse en cours ;
- Le renforcement immédiat des moyens dédiés à la cybersécurité dans la Fonction publique ;
- La mise en place d'une information personnalisée et d'un accompagnement effectif des agents concernés.

La FGF-FO exige également que cette cyberattaque n'ait strictement aucune incidence sur les procédures de mobilité en cours.

Aucune candidature ne doit être écartée, retardée ou refusée en raison de dysfonctionnements liés à cette cyberattaque. Les agents ne peuvent être pénalisés pour une défaillance dont ils ne sont en rien responsables.

Dans un contexte où la loi de finances 2026 impose à nouveau des restrictions budgétaires qui fragilisent les services publics, réduisent les effectifs et contraignent les investissements, les systèmes d'information et leur sécurisation ne peuvent être les victimes silencieuses de ces coupes.

La FGF-FO continuera d'exiger que les budgets alloués à la Fonction publique garantissent réellement la sécurité des agents, la fiabilité des plateformes nationales et la protection effective des données personnelles.