SAFPT INFO

# Comment prévenir et gérer les fraudes au virement de salaire dans la fonction publique territoriale ?

La fraude au virement de salaire, encore peu médiatisée dans la fonction publique territoriale, constitue pourtant un risque réel et croissant. Elle s'appuie sur l'usurpation d'identité et des techniques d'ingénierie sociale destinées à tromper les services des ressources humaines. Les conséquences peuvent être lourdes : pertes financières pour l'agent, responsabilité juridique de l'employeur, atteinte à la confiance des agents, et violation de données personnelles. Comment un employeur public peut-il anticiper, contenir et réagir efficacement face à cette menace ? Voici des mesures concrètes et opérationnelles à mettre en œuvre.

## 1. Renforcer les procédures internes de traitement des changements de RIB

Le changement de coordonnées bancaires constitue l'une des principales failles exploitées par les fraudeurs. Il est indispensable d'établir une procédure stricte, sécurisée et traçable.

**Mesures recommandées :**

-Exiger que toute demande de changement de RIB soit effectuée via un **portail RH sécurisé**, accessible depuis le réseau interne ou par VPN.

-Interdire formellement les demandes adressées par email personnel ou par des canaux non authentifiés.

-En cas d'impossibilité, imposer un **contact en présentiel** ou une **vérification en visioconférence**, avec pièce d'identité.

-Demander une **pièce d'identité valide** accompagnée d'un **justificatif de compte bancaire** à jour.

## 2. Sensibiliser les agents et les gestionnaires RH

La vigilance humaine demeure la meilleure défense contre l'ingénierie sociale.

**Actions possibles :**

-Proposer des sessions annuelles de **formation à la cybersécurité**, ciblant prioritairement les gestionnaires RH.

-Intégrer une **fiche de sensibilisation** numérique dans le livret d'accueil des nouveaux agents, détaillant les bonnes pratiques.

-Mettre en place une **alerte automatique** en cas de demande de changement de RIB.

-Communiquer régulièrement sur les techniques de fraude courantes et les bons réflexes à adopter.

## 3. Définir un protocole clair de réaction en cas de fraude avérée

La réactivité est essentielle pour limiter les impacts financiers et juridiques.

**À mettre en œuvre immédiatement :**

**-Suspendre sans délai** tout paiement vers le compte frauduleux.

**-Notifier la CNIL** sous 72 heures en cas de violation de données personnelles.

**-Documenter l'incident** : date, nature, méthode, agents concernés.

**-Informer les agents victimes** de manière claire et transparente : risques, conséquences, mesures prises, recours possibles.

**-Déposer plainte** au nom de la collectivité et **désigner un référent** pour accompagner l'agent dans ses démarches.

**4. S'appuyer sur la DSI et les outils de cybersécurité**

La direction des systèmes d'information joue un rôle clé dans la prévention des fraudes.

**Bonnes pratiques :**

-Mettre en place un **système d'authentification forte** (MFA) pour les applications RH.

-Déployer des **protocoles de sécurité de messagerie** : SPF, DKIM, DMARC.

-Réaliser des **audits de sécurité** réguliers des processus RH et des flux d'information.

**5. Intégrer la lutte contre la fraude dans la stratégie globale de gestion des risques**

La prévention doit s'inscrire dans une logique de résilience organisationnelle.

**Recommandations :**

- Intégrer la **fraude au virement** dans le **plan de continuité d'activité**.
- Désigner un **référent cybersécurité RH** pour centraliser l'information et actualiser les pratiques.
- Compléter la **charte informatique** avec un chapitre dédié à la sécurité des données RH.

**Conclusion**

Dans un contexte de multiplication des cyberattaques, les directions des ressources humaines doivent adopter une posture proactive. En instaurant des procédures rigoureuses, en formant leurs équipes et en collaborant avec la DSI, elles renforcent la protection des agents et la crédibilité de l'institution publique. Adopter ces mesures, c'est faire un pas décisif vers une administration plus résiliente et protectrice de ses agents.