RÉGION ACADÉMIQUE
LA RÉUNION
Liberté
Égalité
Fraternité

Secrétariat général

SG4
Contrôle de gestion-coordination paye
Affaire suivie par :
Coordination paye
Mél : paye@ac-reunion.fr

24 Avenue Georges Brassens CS 71003
97743 ST DENIS CEDEX 9

Saint-Denis, le 31 mars 2025

Le recteur

à

L'ensemble des personnels

Objet : Sensibilisation aux escroqueries et mesures de sécurité mises en place pour changement de RIB

Références :

- Note DAF-D2024-012352 du 13 décembre 2024 relative à la sécurisation des changements de coordonnées bancaires par un espace sécurisé de transmission de documents

Annexe :

- Fiche réflexe « L'escroquerie aux Faux Ordres de virement (FOVI) » de l'agence nationale de la sécurité des systèmes d'information (ANSSI)

La présente note a pour objet de vous présenter les dispositions mises en œuvre pour sécuriser les changements de coordonnées bancaires face à la multiplication des cas d'usurpation d'identité en matière bancaire. Ces pratiques frauduleuses, souvent utilisées par des individus malveillants, visent à détourner des fonds en modifiant les coordonnées bancaires des agents piratés.

Il est essentiel que chacun soit particulièrement vigilant face à ces tentatives de fraude, qui peuvent avoir des conséquences graves tant sur le plan personnel que professionnel.

Le faux ordre de virement : définition et mesures de prévention

L'escroquerie aux faux ordres de virement (FOVI) désigne un type de fraude qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié.

Plusieurs techniques sont utilisées par les fraudeurs pour obtenir des informations utiles pour procéder à une demande de changement de RIB frauduleuse. Les escroqueries les plus courantes incluent :

- Des messages prétendant provenir d'institution officielle, demandant de modifier les coordonnées bancaires ;
- Des messages incitant à cliquer sur des liens ou à ouvrir des pièces jointes malveillantes.

Vous trouverez en annexe de la note, la fiche Réflexe « L'escroquerie aux Faux Ordres de Virement (FOVI) » réalisée par l'Agence nationale de la sécurité des systèmes d'information.

Sécurisation des changements de RIB

Pour lutter contre ces risques, les gestionnaires de ressources humaines sont sensibilisés et pleinement mobilisés dans une nouvelle procédure pour les demandes de changement de coordonnées bancaires. A cette fin, un espace sécurisé dématérialisé est mis en place et un formulaire Colibris « Demande de changement de RIB » est désormais accessible en permanence. Il devient le **canal exclusif** pour ce type

de demande concernant la rémunération principale à compter du 31 mars 2025.

Pour accéder au formulaire, rendez vous sur le portail de l'intranet académique Métice Rectorat, rubrique « Enquêtes et Pilotage » et cliquez sur « Colibris – Portail des démarches ».
Cliquez sur « Se connecter » pour initier votre démarche. Une fois connecté à votre portail agent, vous retrouverez dans l'onglet « RH- Vie de l'agent » et la rubrique « Demande de changement de coordonnées bancaires » le formulaire à renseigner.
Le formulaire dûment complété parviendra directement à la coordination paie qui, après un premier contrôle, le transmettra à votre gestionnaire. Vous serez informé(e) du traitement de votre demande par un message sur votre boîte mail académique.

A compter de la publication de cette note, les demandes émises via les canaux autres que COLIBRIS (mail, courrier postal…) ne seront pas traitées.

Mes services se tiennent à votre disposition pour toute information complémentaire.

Pour le recteur de région académique,
recteur d'académie et par délégation
le secrétaire général de région académique
secrétaire général d'académie

SIGNÉ
Erwan POLARD

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

L'ESCROQUERIE AUX **FAUX ORDRES DE VIREMENT (FOVI)**

COMPRENDRE LES RISQUES

L'escroquerie aux faux ordres de virement (**FOVI**) désigne un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « d'arnaque au Président ». Une variante consiste à usurper l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement. Une autre variante consiste à usurper l'identité d'un salarié de l'organisation pour demander le changement des coordonnées bancaires où virer son salaire. Le compte bancaire appartenant à l'escroc est souvent situé à l'étranger. Cette catégorie d'escroquerie est généralement réalisée par téléphone et/ou par messages électroniques, voire les deux, et concerne tous les types d'organisation.

BUT RECHERCHÉ

Escroquerie financière en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé visant à faire verser de l'argent sur un compte bancaire détenu par les cybercriminels. Dans certains cas, cette fraude fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée.

SI VOUS ÊTES VICTIME

IDENTIFIEZ LES VIREMENTS FRAUDULEUX. Identifiez tous les virements exécutés, en instance ou à venir à destination de l'escroc. Informez votre hiérarchie ainsi que le service comptable et demandez le blocage des coordonnées bancaires frauduleuses dans les applications métiers.

DEMANDEZ LA SUSPENSION DU VIREMENT. Si le virement n'est pas encore effectué, contactez immédiatement votre service comptable pour suspendre la demande de virement frauduleuse.

ALERTEZ IMMÉDIATEMENT VOTRE BANQUE ET DEMANDEZ LE RETOUR DES FONDS. Si le virement a été réalisé, contactez au plus vite votre banque pour demander le retour des fonds. Votre dépôt de plainte pourra être exigé de votre banque pour récupérer les sommes.

CONSERVEZ LES PREUVES et en particulier les numéros de téléphones, les messages reçus, les ordres de virement, les factures et toutes informations qui pourront vous servir pour signaler l'escroquerie aux autorités.

SI LA FRAUDE A PU ÊTRE PERMISE PAR LE PIRATAGE D'UN COMPTE DE MESSAGERIE, CHANGEZ IMMÉDIATEMENT SON MOT DE PASSE. Utilisez des mots de passe différents et complexes pour chaque site et application utilisés (tous nos conseils pour gérer vos mots de passe).

DÉPOSEZ PLAINTE. En parallèle des démarches auprès de votre banque, déposez plainte sans tarder au commissariat de police ou à la gendarmerie dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Sensibilisez vos collaborateurs et cadres aux risques notamment de réception de messages frauduleux d'hameçonnage (*phishing*) visant à leur dérober leurs mots de passe et en particulier si vos services de messagerie sont hébergés ou accessibles en externe.

Diffusez des procédures claires aux collaborateurs mandatés sur les règles d'authentification des émetteurs et de confirmation des demandes de virement imprévues ou de validation des changements de coordonnées bancaires.

Mettez en place une procédure de vérification et de validation hiérarchique interne non dérogeable des demandes de virement imprévues ou d'acceptation de changements de coordonnées bancaires.

Veillez à limiter la publication d'informations (site Internet, réseaux sociaux…) permettant d'identifier et de contacter vos collaborateurs habilités à réaliser des demandes de virement ou des modifications de coordonnées bancaires.

Généralisez l'utilisation de mots de passe solides pour les comptes de messagerie et activez la double authentification pour limiter les risques de piratage (tous nos conseils pour gérer vos mots de passe).

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Escroquerie (article 313-1 du code pénal).** L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (**article 313-3 du code pénal**).

- **Usurpation d'identité (article 226-4-1 du code pénal).** Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (**article 225-5 du code pénal**).

- **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal).** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine encourue est de cinq ans d'emprisonnement et de 150 000 euros.
  La tentative de cette infraction est punie des mêmes peines (**article 323-7 du code pénal**).

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V230417