



CIRCULAIRE N° 2026-085

CIRCULAIRE

AUX ADMINISTRATIONS COMMUNALES,
AUX SYNDICATS DE COMMUNES,
AUX OFFICES SOCIAUX,
AUX AUTRES ÉTABLISSEMENTS PUBLICS PLACÉS SOUS LA SURVEILLANCE DES COMMUNES

Vigilance par rapport aux escroqueries dites « au président » ou Fovi

Luxembourg, le 13 octobre 2026

Madame la Bourgmestre, Monsieur le Bourgmestre,
Madame la Présidente, Monsieur le Président,

Les escroqueries aux faux ordres de virement (Fovi), dites également « arnaques au président » sont susceptibles de causer des dommages importants dans le chef d'entreprises, de collectivités et d'établissements publics. Le secteur communal n'est pas à l'abri de telles tentatives. Par la présente, je vous prie de bien vouloir rendre attentifs tous vos collaborateurs, particulièrement le receveur et tous ceux qui sont en charge des finances et impliqués dans le processus de paiement des factures, aux risques d'escroqueries et de les inviter à redoubler de vigilance dans l'exercice de leurs tâches.

1. Le mode opératoire

Le but d'un Fovi est d'obtenir la réalisation d'un virement, souvent à l'international, au profit d'un escroc.

Il existe plusieurs modes opératoires similaires :

- L'escroc se fait passer pour le président d'une entreprise, d'un prestataire de services ou d'un fournisseur lors d'un contact téléphonique ou par courriel avec les services comptables de l'administration; il crédibilise sa demande et met en confiance la victime grâce à de l'ingénierie sociale¹; il utilise des ressorts psychologiques visant à abolir le discernement de la victime pour lui faire prendre des décisions sous le coup de l'urgence et de la confidentialité.

¹ L'ingénierie sociale est une technique de manipulation psychologique qui vise à tromper des individus pour obtenir des informations confidentielles, des accès informatiques ou de l'argent.





- La fraude au « changement de RIB² » : l'escroc s'adresse aux services communaux en se faisant passer pour un prestataire de services ou fournisseur de la commune en demandant le règlement de factures du prestataire ou fournisseur sur un compte bancaire autre que le compte habituel de ce dernier.
- La fraude au « faux technicien » : l'escroc se présente comme un technicien informatique venant réaliser une opération de maintenance sur l'outil de gestion des comptes et virements.

2. Mesures préventives

Pour se prémunir contre de telles escroqueries ou arnaques, il y a lieu de prendre des mesures tant au niveau organisationnel qu'au niveau technique et comportemental :

2.1. Au niveau organisationnel

- Sensibiliser régulièrement l'ensemble des agents de l'administration sur les différents types d'escroquerie.
- Informer sur les principales vulnérabilités associées à l'usage des réseaux sociaux et la nécessité de ne pas divulguer des informations susceptibles d'être utilisées dans le cadre d'un Fovi (déplacements des élus et des agents, organigramme trop détaillé, informations comptables, etc.). Dans ce contexte je rappelle les obligations de discrétion des agents des communes découlant de l'article 12 de la loi modifiée du 24 décembre 1985 fixant le statut général des fonctionnaires communaux³.
- Mettre en place des procédures de vérification multiples pour les paiements internationaux et même nationaux (danger du money muling⁴).
- S'assurer de l'existence de procédures de paiement adaptées aux risques de fraude et de détournement de fonds et veiller à ce que tous les agents concernés aient accès à ces procédures.

2.2. Au niveau technique

- Maintenir à jour le système de sécurité informatique et assurer la gestion des droits d'accès des utilisateurs.
- Surveiller et accompagner les interventions de prestataires externes sur les systèmes informatiques des entités communales.
- Lors de la création d'un nouveau fournisseur dans le système comptable, le receveur communal devrait systématiquement exiger un relevé d'identité bancaire (RIB). Si cette

² RIB: le relevé d'identité bancaire est un document émis par une banque, qui contient l'identité du titulaire d'un compte bancaire et ses coordonnées bancaires.

³ Art. 12.

« 1. Le fonctionnaire doit, dans l'exercice comme en dehors de l'exercice de ses fonctions, éviter tout ce qui pourrait (...) compromettre les intérêts du service public. »

⁴ Le money muling (ou blanchiment d'argent par « mulet ») consiste à prêter ou à utiliser son compte bancaire personnel pour transférer, retirer ou blanchir des fonds provenant d'activités criminelles (escroqueries en ligne, trafic, piratage) à la demande de tiers.



procédure n'a pas été appliquée par le passé, le receveur devrait veiller à régulariser progressivement la situation afin de disposer d'un RIB pour chaque destinataire de fonds communaux. A ajouter que la création d'un fournisseur dans le système comptable devrait être initiée par le service à l'origine de l'engagement d'une dépense, le secrétariat communal ou le service financier.

- En cas de modification des coordonnées bancaires d'un fournisseur existant, un contrôle renforcé s'impose. Une telle modification ne doit jamais être opérée sur la seule base d'un courriel, d'une facture ou d'un autre document reçu. Dans ce cas, un contre-appel doit systématiquement être effectué auprès du fournisseur afin de confirmer la modification. Si la modification concerne une facture existante, le fournisseur doit être invité à soumettre une nouvelle facture électronique. Toute demande de modification de coordonnées bancaires doit être accompagnée d'un RIB établi par la banque ou l'institut financier en bonne et due forme.
- Par ailleurs, les receveurs communaux sont priés de veiller à la stricte application du système *Verification of Payee (VoP)* qui permet de vérifier que les données du bénéficiaire saisies (le nom et l'IBAN) correspondent à celles détenues par la banque du bénéficiaire. En cas de divergence ou de correspondance partielle, un message d'alerte s'affiche. Dans ces cas, il ne faut pas valider le paiement et il y a lieu de contacter le bénéficiaire via un canal vérifié (téléphone connu, site officiel, courriel certifié) pour confirmer ses coordonnées bancaires. Cette observation vaut également pour les virements multiples transmis par fichier.

2.3. Au niveau comportemental

- Respecter les procédures mises en place malgré les pressions d'interlocuteurs qui insistent sur des paiements urgents.
- Effectuer systématiquement un contre-appel auprès du prestataire ou du fournisseur. Ce contre-appel doit impérativement être réalisé à l'aide d'un numéro de téléphone d'une source préexistante et fiable, déjà disponible dans les dossiers de la commune.
- Être attentif aux demandes inhabituelles de transmission de nouvelles coordonnées bancaires et, plus largement, faire remonter toute information jugée inquiétante aux services concernés.
- Redoubler de vigilance pendant les périodes de congés scolaires, les jours fériés, les vendredis soir, les week-ends et les périodes de remplacement.
- Se rapprocher de son organisme bancaire et suivre les procédures indiquées.

3. Comment réagir à une opération frauduleuse aboutie

- Identifier immédiatement les virements exécutés, les mandats de paiement ou les demandes de paiement en instance ou à venir concernés.
- Demander le blocage des coordonnées bancaires frauduleuses dans les applications métiers.
- Si le paiement n'est pas encore intervenu, suspendre le mandat ou la demande de paiement.
- Si le paiement est déjà intervenu, demander le blocage ou le retour des fonds auprès de la banque ou de l'institut financier.



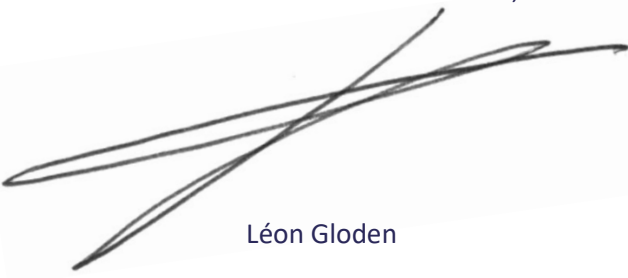
- Déposer le plus vite possible plainte auprès de la Police Grand-Ducale, en apportant un maximum d'éléments (références des virements, coordonnées des personnes contactées).
- Un dépôt de plainte rapide augmente les chances de récupérer les fonds versés.

4. Liens utiles

Je vous prie de trouver ci-dessous des liens vers des sites permettant de vous renseigner davantage sur les opérations frauduleuses.

- Guichet.lu : [Protection contre les arnaques](#)
- Chambre des métiers : [Service aux entreprises – Prévention des arnaques](#)
- Police Grand-Ducale :
[#Cyberscams: Sensibilisation aux escroqueries financières en ligne les plus courantes](#)
<https://police.public.lu/fr/prevention/arnaques/arnaque-au-president.html>
- Fondation Restena : [Fiche-conseil – Les attaques d'ingénierie sociale](#)
- National Cybersecurity Competence Center : [\(NC3.lu\)](#)

Le Ministre des Affaires intérieures,



Léon Gloden