Fédération nationale des Ogec
Mission expertise de gestion

M contact@fnogec.org
T +33(0)1 53 73 74 40

À Paris, le 07 novembre 2025

Objet : Alerte tentative de fraude au faux conseiller bancaire

Contexte et actualité des fraudes en 2025

Les fraudes ciblant les Ogec, se sophistiquent et exploitent désormais des failles dans la chaîne de transmission des informations financières. Une tendance récente et particulièrement préoccupante concerne l'usurpation d'identité de conseillers bancaires, combinée à l'utilisation frauduleuse de fichiers de virements.

Récemment un établissement a été la cible d'une tentative de fraude organisée. Un individu se présentant comme un « conseiller bancaire » a contacté l'établissement par téléphone. Ce fraudeur disposait du fichier de virement des paiements fournisseurs qui venait d'être transmis à la banque. Sous prétexte d'une erreur sur certains destinataires, il a tenté d'obtenir un accès à distance aux comptes bancaires de l'organisme, dans le but de procéder à des virements frauduleux.
Cette méthode illustre une évolution inquiétante des techniques de fraude :

- Vol ou fuite de données internes : Les fraudeurs parviennent à se procurer des fichiers sensibles (virements, coordonnées bancaires) via des cyberattaques, des fuites internes ou des logiciels mal sécurisés.
- Ingénierie sociale poussée : L'utilisation d'informations précises (noms de fournisseurs, montants de virements) rend le discours du fraudeur crédible et augmente le risque de succès.
- Exploitation de l'urgence : Les escrocs jouent sur la pression et la nécessité d'agir rapidement pour éviter une « erreur » ou un « blocage », poussant les victimes à contourner les procédures de sécurité.

Transmission d'information et risques associés

Ce type de fraude met en lumière deux failles majeures dans la gestion des informations financières :

1. La sécurisation des fichiers de virements : Les logiciels de paie et de comptabilité contiennent des données critiques. Leur accès doit être strictement contrôlé et leur transmission sécurisée (chiffrement, accès restreint voir double authentification 2FA).

2. La vérification des interlocuteurs : Les fraudeurs exploitent la confiance accordée aux « conseillers bancaires » ou aux « services techniques ». Or, aucune banque ne demande jamais un accès à distance aux comptes ou une modification de virements par téléphone ou e-mail non sollicité.

Préconisations pour se prémunir contre ce type de fraude

1. Renforcer la sécurité des fichiers sensibles
   - Limiter l'accès aux fichiers de virements aux seuls collaborateurs habilités.
   - Chiffrer les échanges : Utiliser des protocoles sécurisés (SFTP, VPN) pour toute transmission de données financières.
   - Audit régulier : Vérifier les logs d'accès aux logiciels et signaler toute activité suspecte.
2. Instaurer des procédures de vérification systématique
   - Ne jamais communiquer d'informations bancaires ou autoriser un accès à distance sans une double validation (appel à un numéro officiel connu, confirmation écrite via un canal sécurisé).
   - Créer un mot de passe ou une phrase code avec votre banque pour authentifier tout échange téléphonique ou demande de virement.
   - Former les équipes à reconnaître les tentatives de fraude : insister sur les signes d'alerte (urgence, menace, demande inhabituelle, site non sécurisé 🔓).
3. Réagir rapidement en cas de suspicion
   - Couper immédiatement tout accès et contacter votre conseiller bancaire officiel via les coordonnées connues (pas celles fournies par l'appelant).
   - Bloquer les virements suspects en urgence via votre banque.
   - Signaler l'incident à la plateforme Cybermalveillance.gouv.fr et à votre fédération.
4. Sensibiliser en continu
   - Organiser des simulations d'attaques (phishing, faux appels) pour tester la réactivité des équipes.
   - Diffuser des alertes internes en cas de nouvelle menace identifiée (ex. : fraude au faux conseiller bancaire).
   - Ne jamais donner d'information sur l'arbre décisionnaire dans un Ogec : exemple un appel téléphonique pour collecter des données de « qui fait quoi ».

À retenir :
La vigilance collective et la culture de la sécurité sont les meilleurs remparts contre ces fraudes. Dans le cas de cet Ogec, la réactivité de la personne et du chef d'établissement ont permis d'éviter des pertes en contactant rapidement les vrais interlocuteurs bancaires. Cette réussite souligne l'importance d'une procédure claire et connue de tous pour réagir face aux tentatives de fraude.

Suivi et accompagnement :
Nous reviendrons vers vous avec les suites données à cette tentative, après l'enquête ou toute nouvelle tentative. Les Unions Départementales (Udogec), Unions Régionales (Urogec) et la Fédération Nationale (Fnogec) sont à votre disposition pour tout soutien, conseil ou accompagnement dans la gestion de ce type de situation.

Fédération des Ogec

277 rue Saint Jacques
75005 Paris
T +33(0)1 53 73 74 40
M contact@fnogec.org

www.fnogec.org