RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

LE POINT SUR

SE PRÉMUNIR CONTRE LES ESCROQUERIES AUX **FAUX ORDRES DE VIREMENT**

Les FINANCES PUBLIQUES Vous accompagnent

Les collectivités locales, des cibles de choix

Parmi les grands types de faux ordres de virement (FOVI), forte recrudescence du changement de RIB via l'usurpation d'identité

LE CHANGEMENT DE RIB VIA L'USURPATION D'IDENTITÉ

Le fraudeur contacte (par téléphone, courrier ou courriel) les services de la collectivité en se faisant passer pour un fournisseur, un pensionné, un agent public, ou en mettant en place un faux affacturage. Il demande que les versements soient dirigés vers un nouveau compte bancaire, le plus souvent domicilié dans une néobanque (ou « banque mobile ») ou à l'étranger. Souvent, il falsifie les coordonnées bancaires directement dans les factures ou dans les RIB.

Les escrocs collectent en amont des renseignements par piratage des adresses de messagerie. Cette connaissance, associée à des éléments convaincants (ton persuasif, etc.), est la clé de la réussite de la fraude.

LA « FRAUDE AU PRÉSIDENT »

Les escrocs demandent à un agent de la collectivité d'effectuer en urgence un virement important à un tiers, pour obéir à un prétendu ordre de la hiérarchie.

Toutes les collectivités locales, quelle que soit leur taille, peuvent être la cible de ces types de fraudes.

Comment reconnaître et déjouer une fraude ?

Soyez particulièrement vigilant dans les cas suivants !

PAR TÉLÉPHONE, UN INTERLOCUTEUR INHABITUEL MAIS TRÈS CONVAINCANT

L'usurpateur apporte une abondance de détails : il peut être en mesure de présenter des factures obtenues frauduleusement et même faire usage de flatteries ou de menaces.

UNE DEMANDE INHABITUELLE DANS SON CONTENU

Certaines demandes doivent susciter la plus grande vigilance :

- transmission de factures ou de nouveaux RIB par courriel et non par Chorus Pro
- demande de confirmation de paiement suite à un changement de coordonnées bancaires
- demande de changement de coordonnées vers un compte de néobanque, notamment en cas de paye et quand le compte précédent était domicilié dans une banque traditionnelle
- demande de versement à un fournisseur national sur un compte bancaire domicilié à l'étranger
- adhésion récente d'un fournisseur à une société d'affacturage
- toute demande de virement non planifiée, urgente et/ou confidentielle

Les meilleurs moyens de se prémunir contre les FOVI sont le contre-appel et l'utilisation de Chorus Pro pour le dépôt des factures et le changement des coordonnées bancaires des fournisseurs.

LES SIGNES QUI DOIVENT ATTIRER L'ATTENTION

- une adresse de messagerie à la forme particulière (exemple : contact.noreplyXXX@gmail.com)
- une adresse de messagerie se rapprochant de l'adresse habituelle (exemple : pascal.durand@interieur-gouv-fr au lieu de pascal.durand@interieur.gouv.fr)
- une adresse de messagerie qui change lorsque l'on répond au courriel (par exemple, l'adresse affichée henri.dupontdurand@sncf.fr devient henri.dupontdurand@xyz.com)
- une adresse de messagerie comportant un nom de domaine de type @mail.com, @protonmail.com, @virgilio.it, @dr.com ou @financier.com
- une incohérence avec les pièces de la dépense (adresse, numéro SIRET, dénomination ou logo de l'entreprise, etc.)
- un ton trop familier ou trop formel en cas de changement de coordonnées de paye
- une demande de changement de coordonnées bancaires sous prétexte d'un audit financier ou d'un problème sur le compte habituel
- des fautes d'orthographe ou de syntaxe

LES RÉFLEXES À ADOPTER

- **Ne pas céder à la pression de l'interlocuteur souhaitant un paiement rapide. En référer immédiatement à sa hiérarchie.**
- **Porter un regard critique** sur toute transmission de nouvelles coordonnées bancaires et toute demande urgente, à tous les niveaux de la chaîne de la dépense, y compris le service assurant la relation avec les agents en matière de paye.
- La communication d'un nouveau numéro de téléphone à l'indicatif français ou de nouvelles coordonnées bancaires domiciliées en France n'est pas une garantie.
- **Rompre la chaîne de communication** en réalisant un contre-appel à partir de coordonnées téléphoniques recherchées sur Internet ou dans les ressources internes du service

Quelques règles de prévention

- **Sensibiliser** régulièrement l'ensemble des agents concernés (service financier, comptabilité, gestionnaire RH, secrétariat et standard, etc.) à ce type d'escroquerie.

  Informer systématiquement les remplaçants sur ces postes.

- **Accroître la vigilance pendant les périodes de congés et de forte charge de travail**.

- **Diffuser les alertes** transmises par les fournisseurs déjà cibles d'une escroquerie à l'ensemble des acteurs de la chaîne de la dépense (services à l'origine des dépenses, services financiers et trésorerie).

- **Ne pas divulguer**, notamment à un contact inconnu, des informations sur le fonctionnement de la collectivité et sur ses fournisseurs (organigramme, contacts, documents comportant des signatures, procédures internes, etc.).

  Dans le cadre professionnel, divulguer ces informations en les restreignant au strict nécessaire.

- **Avoir un usage prudent des réseaux sociaux privés et professionnels**.

- **Prendre en compte uniquement les factures transmises par Chorus Pro.**

- **Réaliser un contre-appel** au fournisseur ou à l'agent qui a transmis ses coordonnées bancaires ou a demandé leur changement par courriel (à partir de coordonnées téléphoniques recherchées sur Internet ou dans les ressources internes du service, et non de celles figurant dans le courriel reçu).

En cas d'escroquerie, réagissez vite !

1. **Informez immédiatement le comptable public de votre collectivité.**

   En cas de fraude suspectée ou avérée, l'ordonnateur et le comptable public doivent échanger leurs informations sans tarder.

2. **Identifiez les paiements déjà réalisés, à venir ou en instance, pour effectuer les rejets et blocages nécessaires.**

   Si le paiement n'est pas encore intervenu, le comptable public suspend immédiatement le mandat et bloque la mise en paiement.

   Si le paiement a été réalisé, le comptable public actionne les procédures bancaires pour tenter de récupérer les fonds versés.

3. **Bloquez les coordonnées bancaires frauduleuses dans les applications informatiques de la collectivité locale.**

4. **Portez plainte auprès d'un service de police ou de gendarmerie.**

5. **Contactez l'assistance informatique afin de sécuriser la messagerie de la collectivité.**

6. **Renforcez les actions de sensibilisation de l'ensemble des acteurs.**

CONSULTEZ :

collectivites-locales.gouv.fr

Retrouvez les Finances publiques sur

Direction générale des Finances publiques
Novembre 2023