Quelques règles de prévention

- **Sensibiliser** régulièrement l'ensemble des agents concernés (service financier, comptabilité, 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 traitement 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.**

- **Prendre en compte les coordonnées bancaires** figurant sur la facture du fournisseur issue de Chorus Pro ou, à défaut, déposées dans Chorus Pro.

- **Réaliser un contre-appel** au fournisseur qui a transmis ses coordonnées bancaires ou a demandé leur changement par courriel (à partir de coordonnées téléphoniques recherchées sur Internet et non de celles contenues 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. **Renforcez les actions de sensibilisation de l'ensemble des acteurs.**

CONSULTEZ :

www.collectivites-locales.gouv.fr

Retrouvez les Finances publiques sur

Direction générale des Finances publiques
Novembre 2022

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

LE POINT SUR

SE PRÉMUNIR CONTRE LES ESCROQUERIES AUX FAUX ORDRES DE VIREMENT

Les collectivités locales, des cibles de choix

Parmi les trois 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

Les fraudeurs contactent (par téléphone, courrier, courriel) un agent des services de la collectivité ou de la direction générale des Finances publiques (DGFiP) en se faisant passer pour un fournisseur, un pensionné, un agent public, ou en mettant en place un faux affacturage. Ils demandent que les versements soient dirigés vers un nouveau compte bancaire, le plus souvent domicilié dans une néobanque (ou « banque mobile ») ou à l'étranger.

Les escrocs collectent en amont de nombreux renseignements sur le fournisseur, sur la collectivité et sur leurs liens respectifs. Cette connaissance, associée à des éléments convaincants (ton persuasif, utilisation des logos du fournisseur, etc.), est la clé de la réussite de la fraude.

L'ESCROQUERIE À L'INFORMATIQUE

Les escrocs peuvent se faire passer pour l'éditeur du logiciel de comptabilité ou pour un responsable informatique, afin de réaliser des opérations frauduleuses en prenant le contrôle du poste informatique d'un agent.

LA « FRAUDE AU PRÉSIDENT »

Les escrocs demandent à un agent de la collectivité ou de la DGFiP 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 !

UN INTERLOCUTEUR INHABITUEL MAIS TRÈS CONVAINCANT

La personne se faisant passer pour le fournisseur ou pour une société d'affacturage n'est pas le correspondant habituel de la collectivité. Pour asseoir sa crédibilité, l'usurpateur apporte une abondance de détails sur l'entreprise, le marché public, la collectivité et son environnement. Il peut être en mesure de présenter des factures obtenues frauduleusement auprès du fournisseur. L'escroc peut même faire usage de flatteries ou de menaces pour mieux parvenir à manipuler.

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 lorsque le fournisseur n'est pas une TPE/PME et que son compte précédent était domicilié dans une banque traditionnelle
- demande de versement à un fournisseur national sur un compte bancaire domicilié à l'étranger (y compris en zone SEPA)
- adhésion récente d'un fournisseur à une société d'affacturage
- toute demande de virement international non planifiée, urgente et/ou confidentielle

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@dr.com)
- une adresse de messagerie comportant un nom de domaine de type @mail.com, @protonmail.com ou @financier.com
- une incohérence avec les pièces justificatives de la dépense (adresse du fournisseur, numéro SIRET, dénomination ou logo de l'entreprise, etc.)
- des fautes d'orthographe ou de syntaxe dans la rédaction de la demande de changement de coordonnées bancaires.

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.
- 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 contactant soi-même le donneur d'ordre avec les coordonnées récupérées dans un annuaire public (Pages Jaunes).

LES MEILLEURS MOYENS DE SE PRÉMUNIR CONTRE LES FAUX ORDRES DE VIREMENT SONT LE CONTRE-APPEL ET L'UTILISATION DE CHORUS PRO POUR LE DÉPÔT DES FACTURES ET LE CHANGEMENT DES COORDONNÉES BANCAIRES DES FOURNISSEURS.