QUELQUES RÈGLES SIMPLES DE PRÉVENTION

Sensibiliser régulièrement l'ensemble des agents concernés (service financier, comptabilité, secrétariat et standard, etc.) à ce type d'escroquerie. Prendre l'habitude d'informer systématiquement les remplaçants sur ces postes.

Instaurer des procédures de vérification pour les paiements internationaux.

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 à l'extérieur ni à un contact inconnu des informations sur le fonctionnement de la collectivité et sur ses fournisseurs (organigramme, contacts, documents comportant la signature d'acteurs-clés, procédures internes, etc.). Dans le cadre professionnel, divulguer ces informations avec mesure et en les restreignant au strict nécessaire.

Avoir un usage prudent des réseaux sociaux privés et professionnels.

EN CAS DE RÉALISATION DE L'ESCROQUERIE : RÉAGISSEZ VITE !

1 - Informez immédiatement la trésorerie

En cas de fraude suspectée ou avérée, ordonnateur et trésorier 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 trésorier suspend immédiatement le mandat et bloque la mise en paiement.

Si le paiement a été réalisé : le trésorier actionne les procédures bancaires pour tenter de récupérer les fonds versés.

3 - Bloquez les coordonnées bancaires frauduleuses dans les applications informatiques de la collectivité

4 - Renforcez les actions de sensibilisation de l'ensemble des acteurs

Retrouvez la DGFiP sur

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Septembre 2017

FINANCES PUBLIQUES

SE PRÉMUNIR CONTRE LES ESCROQUERIES AUX FAUX ORDRES DE VIREMENT (FOVI)

UNE VIGILANCE RENFORCÉE DE L'ORDONNATEUR ET DU COMPTABLE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

LES COLLECTIVITÉS LOCALES UNE CIBLE DE CHOIX

On constate actuellement la recrudescence de deux grands types de FOVI.

Le changement de RIB via usurpation d'identité

Les fraudeurs téléphonent, ou envoient un courrier ou un courriel à un agent de la collectivité ou de la trésorerie, en se faisant passer pour un fournisseur ou pour une société d'affacturage. Ils demandent que **les versements de la collectivité soient dirigés vers un nouveau compte bancaire**, le plus souvent domicilié 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, mention du numéro et du reste à payer sur le marché public, etc.), est la clé de la réussite de la fraude.

La « fraude au président »

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

Ils peuvent aussi se faire passer pour l'éditeur du logiciel de comptabilité ou pour un responsable informatique, afin de réaliser des opérations frauduleuses sur le poste informatique d'un agent.

Attention : Toutes les collectivités locales, quelle que soit leur taille, peuvent être victimes de ce type de fraude.

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 la 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

Doivent susciter la plus grande vigilance :

- toute demande de virement à l'international non planifiée, soi-disant urgente et confidentielle ;
- toute demande de versement à un fournisseur national sur un compte bancaire domicilié à l'étranger (y compris en zone SEPA) ;
- toute adhésion récente d'un fournisseur à une société d'affacturage ;
- tout changement de coordonnées téléphoniques, électroniques et bancaires du fournisseur, du factor ou du cessionnaire.

Attention : Les paiements à l'étranger doivent susciter la plus grande vigilance.

Doivent attirer l'attention :

- une incohérence des noms et prénoms ;
- une adresse de messagerie à la forme particulière,
  - approchant l'adresse habituelle :
    pascal.durand@interieur-gouv-fr
    au lieu de pascal.durand@interieur.gouv.fr
  - ou qui change lorsque l'on répond au courriel :
    L'adresse affichée henri.dupontdurand@sncf.fr
    devient <henri.dupontdurand@dr.com>
- une incohérence avec les pièces justificatives de la dépense (adresse du fournisseur, numéro SIRET, dénomination de l'entreprise, etc.)

Les réflexes à avoir

L'agent ne doit **pas céder à la pression** de l'interlocuteur souhaitant un paiement rapide. Au moindre doute, il doit **en référer immédiatement à sa hiérarchie**.

À tous les niveaux de la chaîne de la dépense (des services de la collectivité jusqu'à la trésorerie), les agents doivent **porter un regard critique** sur toute demande urgente et toute transmission de nouvelles coordonnées bancaires.

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.

Il faut alors **rompre la chaîne de communication** en répondant aux courriers ou courriels douteux en saisissant soi-même l'adresse (physique ou électronique) habituelle du donneur d'ordre, ou en le contactant directement avec les coordonnées déjà connues de la société ou récupérées dans un annuaire public de type Pages Jaunes (procédure du contre-appel).