DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Sensibilisation à l'escroquerie aux virements frauduleux

Rencontre partenariale du 12 décembre 2017.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

SOMMAIRE

I - Contexte, appel à la vigilance

II - Comment déjouer la fraude

III - Règles simples pour se prémunir de l'escroquerie

IV - Comment réagir

V - Spécificités du secteur public local

SOMMAIRE

I - Contexte, appel à la vigilance

II - Comment déjouer la fraude

III - Règles simples pour se prémunir de l'escroquerie

IV - Comment réagir

V - Spécificités du secteur public local

Contexte, appel à la vigilance

Tentatives d'escroquerie dans le secteur public :

Les personnes publiques sont la cible de tentatives d'escroquerie via la « fraude au président » ou l'usurpation d'identité (d'un gestionnaire ou d'un fournisseur). Les tentatives sont généralement précédées de campagnes de prise de renseignements de la part des escrocs.

- **Fraude au président** : l'escroc se fait passer pour un haut responsable et au moyen de pressions, sous couvert du secret, exige un virement bancaire vers un établissement financier, le plus souvent situé à l'étranger, en général hors de l'Union Européenne. L'escroc insiste généralement sur le caractère urgent et exceptionnel de l'opération. Ces tentatives d'escroquerie ont souvent lieu par téléphone car les escrocs connaissent parfaitement l'organisation des services de l'État et des collectivités locales, ce qui permet de mettre en confiance les victimes potentielles.

- **Usurpation d'identité** : l'escroc peut se faire passer pour un responsable informatique souhaitant réaliser des tests à distance et réaliser des opérations frauduleuses sur le poste du gestionnaire. Il peut également se faire passer pour un fournisseur (souhaitant modifier son RIB) et déposer une demande en ce sens, ou se faire passer pour l'éditeur du logiciel de comptabilité utilisé.

Contexte, appel à la vigilance

Faits devant accroître la vigilance des agents

1/ Un contact inhabituel dans la forme :

- L'agent est contacté par un correspondant inhabituel ;
- Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise/l'administration et son environnement : données personnelles concernant l'ordonnateur, ses collaborateurs, le fournisseur et ses dirigeants... ;
- Contact direct d'un escroc (par courriel, par téléphone,...) se faisant passer pour un membre de la société ou un responsable qui va faire usage de flatteries ou de menaces dans le but de manipuler son interlocuteur.

Contexte, appel à la vigilance

Faits devant accroître la vigilance des agents

2/ Une demande inhabituelle dans son contenu :

- Demande de virement (par courriel, par téléphone,...) non planifiée, au caractère urgent et confidentiel et le plus souvent à l'international ;
- Demande de versement à un fournisseur national sur un compte bancaire domicilié à l'étranger ;
- Tout changement de coordonnées téléphoniques, électroniques et de coordonnées bancaires que ce soit du fournisseur, du factor ou du cessionnaire.
- Affiliation récente du fournisseur à une société d'affacturage.

Attention, la communication d'un nouveau numéro à l'indicatif français ou de coordonnées bancaires domiciliées en France n'est pas une garantie.

Contexte, appel à la vigilance

Points d'attention techniques sur le téléphone et le courriel

- **Escroquerie par téléphone:** pour ne pas éveiller les soupçons ou pour renforcer la confiance de leur interlocuteur, les escrocs peuvent afficher un faux numéro ou un faux nom sur l'écran du poste appelé.

- **Escroquerie par courriel:**
  - Modification des entêtes de messages.

    Exemple : lors d'une réponse à un courriel d'un escroc cherchant à se faire passer pour un employé de la sncf :

henri.dupontdurand@sncf.fr	<henri.dupontdurant@br.com>
Ce qui s'affiche	**L'adresse sur laquelle le message est envoyé « <> »**

  - Utilisation d'une adresse approchante : pascal.durantdupont@interieur-gouv.fr au lieu de pascal.durantdupont@interieur.gouv.fr ;
  - Utilisation du logo de l'entreprise ;
  - Fautes de syntaxe ou d'orthographe.

SOMMAIRE

I - Contexte, appel à la vigilance

II - Comment déjouer la fraude

III - Règles simples pour se prémunir de l'escroquerie

IV - Comment réagir

V - Spécificités du secteur public local

Comment déjouer la fraude

D'une manière générale :

- Rompre la chaîne pour les courriers/courriels douteux en saisissant soi-même l'adresse (physique, électronique) habituelle du donneur d'ordre, voire **en le contactant directement à son numéro de téléphone usuel ;**
- Prendre en compte les alertes et communications des fournisseurs indiquant faire l'objet d'escroquerie ;
- **En référer, au moindre doute, immédiatement à sa hiérarchie** ;
- Ne pas céder à la pression de l'escroc et à l'urgence qu'il invoque ;
- Porter un regard critique sur les demandes urgentes ou la transmission de nouvelles coordonnées à tous les niveaux de la chaîne de la dépense (des services prescripteurs au comptable) ;
- **Contacter son interlocuteur habituel avec les coordonnées déjà connues de la société (= procédure de contre-appel)** en cas de moindre doute sur des nouvelles coordonnées téléphoniques, électroniques ou bancaires. Ne pas contacter le fournisseur à partir des coordonnées téléphoniques, électroniques fournies par le potentiel escroc.

SOMMAIRE

I - Contexte, appel à la vigilance

II - Comment déjouer la fraude

III - Règles simples pour se prémunir de l'escroquerie

IV - Comment réagir

V - Spécificités du secteur public local

Règles simples pour se prémunir de l'escroquerie

D'une manière générale :

- Ne pas divulguer à l'extérieur (dont réseaux sociaux) et à un contact inconnu d'informations concernant le fonctionnement de l'administration et de ses fournisseurs : organigrammes, adresses électroniques et documents ou images comportant la signature des acteurs-clés, des procédures internes... Dans le cadre professionnel, divulguer ces informations avec prudence en les restreignant au strict nécessaire ;
- Avoir un usage prudent des réseaux sociaux privés et professionnels ;
- Informer/Sensibiliser régulièrement l'ensemble des agents des services financiers, comptabilités, trésoreries, secrétariats, standards, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les remplaçants sur ces postes ;
- Instaurer des procédures de vérifications pour les paiements internationaux ;
- Rompre la chaîne des mails pour les courriels se rapportant à des virements internationaux en saisissant soi-même l'adresse habituelle du donneur d'ordre ;
- Accentuer la vigilance sur les périodes de congés d'été et des fortes charges;
- Diffuser à l'ensemble de la chaîne de traitement des dépenses (service prescripteur, CSP, services financiers, comptable...) les alertes et communications transmises par les fournisseurs indiquant faire l'objet d'escroquerie.

SOMMAIRE

I - Contexte, appel à la vigilance

II - Comment déjouer la fraude

III - Règles simples pour se prémunir de l'escroquerie

IV - Comment réagir

V - Spécificités du secteur public local

Comment réagir

D'une manière générale :

- Réagir vite ;
- L'ordonnateur doit immédiatement en informer le comptable ce qui peut permettre une intervention avant la mise en paiement voire après la mise en paiement. D'une manière générale en cas de fraude suspecte ou avérée, les ordonnateurs et le comptable public doivent échanger leurs informations sans tarder ;
- Identifier l'ensemble des paiements déjà réalisés, à venir, ou en instance utilisant les coordonnées bancaires frauduleuses pour effectuer les blocages nécessaires (travaux nécessitant le cas échéant une collaboration entre l'ordonnateur et le comptable) ;
- Échanger en interne avec les autres services concernés ;
- Demander immédiatement le blocage des coordonnées bancaires frauduleuses ;
- Renforcer les actions de sensibilisation de l'ensemble des acteurs de la chaîne afin d'éviter que le cas ne se reproduise.

SOMMAIRE

I - Contexte, appel à la vigilance

II - Comment déjouer la fraude

III - Règles simples pour se prémunir de l'escroquerie

IV - Comment réagir

V - Spécificités du secteur public local

Attention à apporter par l'ordonnateur pour toute demande de changement de RIB

Rappel des contrôles réglementaires du comptable en matière de cessions et d'oppositions.

Attitude du comptable face à la modification par l'ordonnateur du RIB du titulaire d'un marché public, dans le cadre d'une cession de créance.

Attention à apporter par l'ordonnateur pour toute demande de changement de RIB

Que l'on se situe dans le cadre d'un marché public, où les règles de notification d'un changement de RIB sont enserrées dans des conditions de forme très précises, ou dans le cadre du paiement d'une subvention ou d'une paye, le changement de RIB doit être toujours effectué avec beaucoup de prudence.

Cela implique pour l'ordonnateur de disposer d'une base tiers « propre » dans son système d'information .

En tout état de cause, un changement de coordonnées bancaires est un acte très important pouvant avoir des conséquences financières majeures et répétées.
Il importe de ne pas céder sur le formalisme pour de simples questions de facilités ou d'urgence.

Rappel des contrôles réglementaires du comptable en matière de cessions et d'oppositions

En vertu des articles 18, 19 et 37 du décret n°2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique (GBCP), **le comptable public est seul chargé de la suite à donner aux oppositions à paiement et autres significations**.

Il est tenu d'exercer le contrôle du caractère libératoire du paiement et toute opposition, ou toute autre signification ayant pour objet d'empêcher un paiement, doit être faite entre ses mains.

S'agissant de la notification des oppositions, l'article 107 al.1 du code des marchés publics indique que le bénéficiaire d'une cession ou d'un nantissement de créance au titre d'un marché public notifie ou signifie cette cession ou ce nantissement au comptable public assignataire.

Il ressort de tous ces éléments qu'**il appartient au seul comptable de gérer les oppositions à paiement et d'exercer le contrôle du caractère libératoire du paiement.**