DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Vigilance sur l'escroquerie aux virements frauduleux

Ateliers des maires et des secrétaires de mairie

Les 05, 07, 11 et 12 septembre 2017

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

DDFiP de la Dordogne

UDM 24
UNION DEPARTEMENTALE DES MAIRES DE LA DORDOGNE

SOMMAIRE

SOMMAIRE

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 (y compris en zone SEPA). 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. Il peut également se faire passer pour un comptable ou un ordonnateur auprès du fournisseur pour récupérer des informations et documents.

Contexte, appel à la vigilance

Un point commun : la très bonne connaissance de l'environnement administratif

La confiance s'instaure grâce à une très fine connaissance de leurs victimes.

La connaissance de l'entreprise en plus d'un ton extrêmement convaincant sont les clés de réussite de ces arnaques.

L**es tentatives de fraude sont précédées de recherche d'informations et/ou de documents :**

- *Personne en charge des opérations (ordonnateur, comptable, ...) ;*
- *Existence de marchés publics ;*
- *États des dépenses (factures en instance, …) ;*
- *Circuit de communication de l'information ;*
- *Nom des applications ;*
- *Nom des structures ;*
- *Factures, baux ;*
- *Etc.*

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, … Il sera parfois également en mesure de présenter des pièces de dépenses (factures) préalablement obtenues frauduleusement auprès du fournisseur ... ;
- 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. Il peut dissuader habilement son interlocuteur de parler de leurs échanges à son entourage professionnel (« vous n'allez pas le déranger pour ça ... »).

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 (y compris en zone SEPA) ;
- 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 , société d'affacturage avec un compte bancaire domicilié hors France pour un fournisseur national ;
- Une facture sans commande (ex : inscription sur des annuaires/ registres…).

  - *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@dr.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.

Contexte, appel à la vigilance

Quelques illustrations

Exemple 1 – Changement de coordonnées bancaires d'un marché :

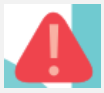
- Contact téléphonique de l'ordonnateur par l'escroc :

L'escroc se fait passer pour un salarié du service Finance & Contentieux du titulaire du marché. Il a utilisé le nom et le prénom d'un ancien salarié ;

- Envoi à l'ordonnateur par courriel de nouvelles coordonnées bancaires :

Le courriel fait référence à la conversation téléphonique et comprend plusieurs signes trompeurs tels le logo du titulaire du marché, le numéro du marché, le numéro du fournisseur tel que référencé dans les applications de gestion, les factures obtenues frauduleusement auprès du fournisseur suite à usurpation de l'identité de l'ordonnateur ou du comptable ;

- Demande, par l'ordonnateur, d'ajout des coordonnées bancaires frauduleuses sur la fiche tiers ;
- Ajout des coordonnées bancaires frauduleuses à partir des pièces justificatives frauduleuses et paiement à ce tiers sur les coordonnées frauduleuses.



Un point commun : paiement à l'étranger

Contexte, appel à la vigilance

Quelques illustrations

Exemple 2 – Faux affacturage... et variantes :

- Transmission à l'ordonnateur ou directement au comptable public d'une attestation/convention/notification d'affacturage frauduleuse avec usurpation d'identité du fournisseur demandant le paiement sur le compte frauduleux ;
- Enregistrement des coordonnées bancaires frauduleuses par l'ordonnateur ou le comptable dans le système d'information ;
- Paiement des factures sur le compte bancaire de l'escroc au lieu de celui du fournisseur.
- L'escroc peut adjoindre des factures (réelles ou fausses) voire y porter des mentions d'affacturage.

Un point commun : paiement à l'étranger

SOMMAIRE

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 ;
- Prendre en compte les alertes et communications de la direction générale des finances publiques/du comptable public ;
- En référer, au moindre doute, immédiatement à sa hiérarchie ;
- Échanger les informations entre ordonnateur et comptable, entre services en interne ;
- Ne pas céder à la pression et à l'urgence invoquée : ne pas rester seul face à une demande.

Comment déjouer la fraude ?

D'une manière générale :

- 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 gestionnaires 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.
  - Dans ce contexte de suspicion de fraude, il convient d'éviter d'utiliser les informations client référencées dans Chorus Pro (afin de circonscrire le risque, bien que limité, de création de compte Chorus Pro frauduleux et de fausse facturation associée).

  - Attention : Ne jamais contacter le fournisseur à partir des coordonnées fournies par le potentiel escroc.

SOMMAIRE

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 ;
- Ne pas divulguer à un contact inconnu d'informations concernant l'exécution d'un marché, le montant des restes à payer, les informations sur les paiements à venir et les factures attendues ;
- Ne pas transmettre, à un contact extérieur, des imprimés, des formulaires administratifs qui servent de support pour donner un ordre de payer ou de virement.
- Avoir un usage prudent des réseaux sociaux privés et professionnels ;
- Accentuer la vigilance sur les périodes de congés et de forte charge de travail ;
- 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, ainsi que celles transmises par le comptable public.

Règles simples pour se prémunir de l'escroquerie

D'une manière générale :

- 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 (y compris en zone SEPA), exemple : mise en place d'une procédure de contre appel, à partir des coordonnées connues du fournisseur pour vérifier la véracité :
  - d'une demande de modification des coordonnées bancaires sur lesquelles les futurs paiements doivent être opérés ; (NB : Pour les dépenses de l'État, ce contre appel est mis en œuvre par le comptable public (PNST) pour les tiers sirétés français demandant un paiement à l'étranger).
  - de la mise en œuvre d'un affacturage ;
- 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 ;

Règles simples pour se prémunir de l'escroquerie

Mise à disposition d'une plaquette de communication généraliste disponible sur le site collectivites-locales.gouv.fr :

SOMMAIRE

Comment réagir

D'une manière générale :

Réagir très vite/immédiatement :

- Signaler la tentative d'escroquerie ou l'escroquerie réalisée à la hiérarchie selon les procédures définies en interne ;
- L'ordonnateur doit immédiatement en informer le comptable et inversement, ce qui peut permettre une intervention avant la mise en paiement voire après la mise en paiement ;
- 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) ;
- Demander immédiatement le blocage des coordonnées bancaires frauduleuses dans les applications informatiques ;
- Dans le cas où le paiement a été réalisé, l'ordonnateur contacte immédiatement le comptable public pour que ce dernier actionne les procédures bancaires pour tenter de récupérer les fonds versés au présumé escroc.

Comment réagir

D'une manière générale :

Mettre en œuvre des actions à court, moyen et long terme qui permettront de se prémunir contre des tentatives d'escroquerie ultérieures :

- Échanger en interne avec les autres services concernés ;
- Renforcer les actions de sensibilisation de l'ensemble des acteurs de la chaîne afin d'éviter que le cas ne se reproduise ;
- Intégrer le risque d'escroquerie dans les formations des agents ;
- Renforcer les contrôles sur des points de fragilité identifiés ;
- Mettre en œuvre des bonnes pratiques telle la procédure de contre-appel du fournisseur à partir de ses coordonnées habituelles.

SOMMAIRE

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 .

Dans le cadre du comité de fiabilité des comptes locaux, les représentants des associations d'élus ont préconisé la création d'une « cellule tiers » chargée de :

- créer les tiers dans la base du système d'information financière,
- contrôler les demandes de modification des coordonnées bancaires ou postales,
- gérer les tiers pour éviter les doublons.

Cette « bonne pratique » est mentionnée pour le processus « commande publique » comme pour celui relatif aux « interventions »
(Cf.http://www.collectivites-locales.gouv.fr/files/files/finances_locales/fiabilisation/ci/rci_interventions_oct15.pdf et http://www.collectivites-locales.gouv.fr/files/files/finances_locales/fiabilisation/ci/Referentiel_commande_publique_oct13.pdf)

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.

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Merci de votre attention

Ateliers des maires et des secrétaires de mairie

Les 05, 07, 11 et 12 septembre 2017

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

DDFiP de la Dordogne

UDM 24
UNION DEPARTEMENTALE DES MAIRES DE LA DORDOGNE