DIRECTION GÉNÉRALE DES
FINANCES PUBLIQUES

Tentatives d'escroquerie : renforcement de la vigilance de l'ordonnateur et de l'agent comptable

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

Face aux tentatives d'escroquerie frappant les organismes publics nationaux, soyons plus vigilants !

De quoi s'agit-il ?

Il existe trois grands types d'escroquerie pouvant frapper les organismes publics nationaux.

La « fraude au président »

les escrocs demandent d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre de la hiérarchie, sous prétexte d'une facture à régler, de provision de contrat ou autres. Les escrocs se font passer pour des hauts responsables et au moyen de pressions, sous couvert du secret, exigent un virement vers un établissement financier, le plus souvent situé à l'étranger, y compris en zone SEPA. Ils peuvent également se faire passer pour l'éditeur de logiciel de comptabilité, un responsable informatique souhaitant réaliser des tests à distance et réaliser des opérations frauduleuses sur le poste de l'agent.

Le « changement de RIB », via usurpation d'identité

les fraudeurs envoient un courriel ou téléphonent à un agent des services de l'ordonnateur ou de l'agent comptable en se faisant passer pour un fournisseur ou une société d'affacturage, et lui demandent de diriger ses versements vers un autre compte bancaire le plus souvent domicilié à l'étranger, dont zone SEPA. Un relevé d'identité bancaire mentionnant les nouvelles coordonnées bancaires et, le cas échéant, une facture y sont joints. Les escrocs ont collecté en amont un maximum de renseignements sur le fournisseur et l'organisme. Cette connaissance des structures (nom des agents et salariés, leur fonction au sein de l'organisme et de ses fournisseurs...) et du contexte (exemple : existence d'un marché public de tel organisme avec tel fournisseur) associée à un ton persuasif et convaincant est la clé de leur réussite.

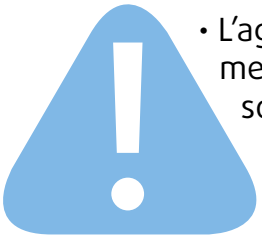
Le faux contrat d'affacturage

consiste pour un escroc à convaincre l'agent comptable et/ou ses collaborateurs de suspendre le paiement de factures à un fournisseur afin que ces factures soient payées au profit d'une pseudo société d'affacturage (factor) avec laquelle ce fournisseur aurait conclu un contrat. Les escrocs transmettent par courriel à l'organisme des factures falsifiées par l'ajout de fausses formules d'affacturage (mention de comptes bancaires et de RIB frauduleux). Afin d'empêcher ce type de fraude, l'agent comptable doit rapidement prendre contact avec le fournisseur cité par l'escroc afin qu'il confirme par écrit qu'il a bien conclu un contrat avec une société d'affacturage. Cette prise de contact doit se faire au moyen des coordonnées déjà connues dont il dispose (et non pas de celles transmises par l'escroc).

Comment reconnaître une escroquerie frappant un organisme public national ?

Les faits devant accroître la vigilance des agents :

Un contact inhabituel dans la forme :



• L'agent est contacté par un correspondant inhabituel, se faisant passer pour un membre de la société ou un responsable qui l'abonde de détails sur l'organisme, son agence comptable et son environnement (données personnelles concernant l'ordonnateur, ses collaborateurs, le fournisseur et ses dirigeants…), afin d'asseoir sa crédibilité. L'interlocuteur peut même faire usage de flatteries ou de menaces dans le but de mieux le manipuler.

Une demande inhabituelle dans son contenu :

• Il est demandé d'effectuer un virement à l'international non planifié, au caractère urgent et confidentiel, de faire un versement à un fournisseur national sur un compte bancaire domicilié à l'étranger ou de changer les coordonnées téléphoniques, électroniques et bancaires du fournisseur, du factor ou du cessionnaire. L'affiliation récente du fournisseur à une société d'affacturage peut être suspecte.

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

• La demande écrite ou orale de l'escroc comporte plusieurs incohérences de noms, de prénoms, d'adresse de messagerie (exemples : adresses décomposées en plusieurs parties entre «<>»…), ainsi qu'avec les pièces justificatives de la dépense (facture, acte d'engagement, acte de cession). Les écarts peuvent porter notamment sur les adresses du fournisseur (ou du factor, du cessionnaire), les références SIRET, la dénomination de l'entreprise. La demande peut également contenir des fautes d'orthographes et de syntaxe.

• 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 « <> »

À noter : La demande peut être trompeuse du fait de sa « qualité » avec utilisation du logo du fournisseur ou affichage d'un faux numéro sur le poste téléphonique de l'agent.

Comment se prémunir de l'escroquerie frappant un organisme public national ?

- Ne pas divulguer à l'extérieur (dont réseaux sociaux) et à un contact inconnu d'informations concernant le fonctionnement de l'organisme, de son agence comptable 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 ;
- 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, services financiers, agence comptable...) les alertes et communications transmises par les fournisseurs indiquant faire l'objet d'escroquerie.

Comment déjouer la fraude frappant un organisme public national ?

- **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 ;**
- **Il faut 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 à l'origine de la dépense à l'agent comptable) ;**
- **Il ne faut pas hésiter à 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 ;**
- **Il faut 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.**

Que faire si l'on s'est fait escroquer ?

- L'agent comptable de l'organisme public national doit immédiatement en informer l'ordonnateur. D'une manière générale en cas de fraude suspecte ou avérée, l'ordonnateur et l'agent comptable doivent échanger leurs informations sans tarder.
- Identifier l'ensemble des paiements déjà réalisés, à venir, ou en instance pour effectuer les rejets et blocages nécessaires.
- Tenter très rapidement l'annulation des virements déjà exécutés.
- Prévenir la direction générale des Finances publiques via la rédaction d'une fiche de signalement.
- L'organisme a seul qualité pour déposer plainte. La DGFiP ne peut se substituer à lui pour ce faire. Il pourra néanmoins prendre l'attache du bureau RH-2B (*bureau.rh2b-epn@dgfip.finances.gouv.fr*).
- Renforcer les actions de sensibilisation de l'ensemble des acteurs de la chaîne et le contrôle interne afin d'éviter que le cas ne se reproduise.

Direction générale des Finances publiques

Janvier 2017