

# Tentatives d'escroquerie : Renforcement de la vigilance de l'ordinateur et de l'agent comptable

---



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

Les escroqueries aux faux ordres de virements (FOVI) perdurent en France dans la sphère publique. Plusieurs ordonnateurs et leurs agents comptables ont été la cible de ce type d'agissements. Certaines fraudes ont pu être déjouées mais d'autres n'ont pas pu être évitées.

## De quoi s'agit-il ?

Il existe quatre grands types d'escroquerie pouvant frapper les organismes publics nationaux (OPN) :

### 1) 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.

### 2) 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.

### 3) 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).


### 4) L'escroquerie à l'informatique

Consiste à ce que des escrocs se fassent passer pour un responsable informatique ou pour un éditeur de logiciel de comptabilité, afin de réaliser des opérations frauduleuses en prenant le contrôle du poste informatique d'un ou plusieurs agents de l'OPN.

# 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'adresses 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'orthographe et de syntaxe.

**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.

## Modification des entêtes de messages :

Exemple :

`henri.dupontdurand@sncf.fr`

Adresse habituelle

`henri.dupontdurand@br.com`

Adresse de l'escroc

# 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 prescripteurs 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.

## 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 pendant 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.



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

- L'agent comptable doit **immédiatement en informer l'ordonnateur**. D'une manière générale, en cas de fraude suspectée 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 disponible sur <http://ulyse.dgfip/metier/controle-interne-comptable-et-bancaire-accueil>.
- 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](mailto: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.





Retrouvez la DGFIP sur



Direction générale des Finances publiques

Juillet 2020