DIRECTION GÉNÉRALE DES
FINANCES PUBLIQUES

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES FINANCES
ET DES COMPTES PUBLICS

Face aux tentatives d'escroquerie, soyons plus vigilants !

Des cas d'escroqueries ont déjà été rencontrés par des ordonnateurs et des comptables publics. Certaines fraudes ont été déjouées grâce à la vigilance des agents, mais d'autres n'ont pu être évitées. Il peut être considéré, à tort, que cela n'arrive qu'aux autres. Dans ce contexte, les actions de préventions régulières sont déterminantes.

Qui est concerné ?

Réalisée par téléphone ou par courriel, l'escroquerie aux faux ordres de virement concerne les entreprises de toute taille et de tous les secteurs **ainsi que l'État, les établissements publics nationaux, les collectivités et établissements publics locaux ou les établissements publics de santé.**

De quoi s'agit-il ?

Il existe deux grands types d'escroquerie.

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. 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 courrier ou un courriel ou téléphonent à un agent des services de l'ordonnateur ou du comptable en se faisant passer pour un fournisseur ou une société d'affacturage.

Ils lui demandent de diriger désormais ses versements vers un autre compte bancaire, le plus souvent domicilié à l'étranger.

Les escrocs collectent en amont un maximum de renseignements sur le fournisseur et l'administration (noms des agents, fonctions...) et sur leurs relations (exemple : existence d'un marché public de tel service de l'État avec tel fournisseur).

Cette connaissance des structures et du contexte associée à des éléments convaincants (ton persuasif, utilisation de logo, de noms des interlocuteurs chez le fournisseur...) est la clé de leur réussite.

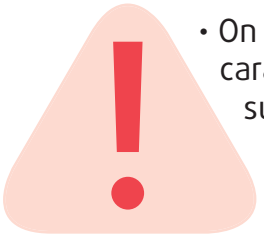
Comment reconnaître une escroquerie ?

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'entreprise/ l'administration et son environnement (données personnelles concernant l'ordonnateur, ses collaborateurs, le fournisseur et ses dirigeants…) ceci 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 :



• On demande à l'agent 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 nécessite un **renforcement de la vigilance**.

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.

Ils peuvent être minimes :

exemple : *pascal.durand@intérieur-gouv-fr* au lieu de *pascal.durand@intérieur.gouv.fr*.

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 ?

- Ne pas divulguer à l'extérieur, ou à un contact inconnu, d'informations concernant l'administration et ses fournisseurs (organisation, employés, procédures...). 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 (services à l'origine de la dépense, services ordonnateurs, CSP, services financiers, comptable...) les alertes et communications transmises par les fournisseurs indiquant faire l'objet d'escroquerie

Comment déjouer la fraude ?

- **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 au comptable)**
- **Il ne faut pas hésiter à contacter son interlocuteur habituel avec les coordonnées déjà connues de la société ou recherchées sur un annuaire officiel - type « Pages Jaunes » - (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'ordonnateur doit **immédiatement en informer le comptable.** 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 pour effectuer les rejets et blocages nécessaires**
- Demander immédiatement le **blocage des coordonnées bancaires** frauduleuses dans les applications métiers
- **Si le paiement n'est pas encore intervenu,** le comptable doit immédiatement suspendre le mandat de paiement ou la demande de paiement concerné
- Renforcer les actions de sensibilisation de l'ensemble des acteurs de la chaîne afin d'éviter que le cas ne se reproduise

Direction générale des Finances publiques

Juin 2016