RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Escroqueries aux faux ordres de virement : renforcement de la vigilance de l'ordonnateur et du comptable

Face aux tentatives d'escroquerie aux FOVI, soyons plus vigilants !

Apparues pour la première fois en France en 2010, **les escroqueries aux faux ordres de virement** (les « FOVI ») visent à pousser un salarié ou un agent public à effectuer un **virement bancaire sur un compte frauduleux**, en usurpant l'identité du véritable **créancier.**
Ce phénomène perdure en France à un niveau élevé, y compris au préjudice de la sphère publique. **Plusieurs ordonnateurs et leur comptable public** ont en effet été la cible de ce type d'escroqueries. Certaines fraudes ont été déjouées grâce à la vigilance des agents, mais d'autres n'ont pu être évitées.
Dans ce contexte, les actions de prévention régulières sont déterminantes.

Qui est concerné ?

Réalisée par courrier, 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 **les collectivités locales, les établissements publics et les services de l'État.**

De quoi s'agit-il ?

Il existe trois grands types d'escroquerie.

Le changement de RIB, via usurpation d'identité

Les escrocs contactent un agent des services ordonnateurs ou du comptable, en se faisant passer pour un fournisseur, ou pour une société d'affacturage. Ils demandent que les versements soient dirigés vers un nouveau compte bancaire.

La « fraude au président »

Les escrocs demandent à un agent des services ordonnateurs ou du comptable d'effectuer en urgence un virement important à un tiers, pour obéir à un prétendu ordre de la hiérarchie.

L'escroquerie à l'informatique

Les escrocs peuvent se faire passer pour l'éditeur du logiciel de comptabilité ou pour un responsable informatique, afin de réaliser des opérations frauduleuses en prenant le contrôle du poste informatique d'un agent.

Comment reconnaître une escroquerie ?

Les faits devant accroître la vigilance des agents :

Un interlocuteur inhabituel

Un agent des services ordonnateurs, ou du comptable, est contacté par un correspondant inhabituel qui **se fait passer pour un fournisseur, ou pour une société d'affacturage.** Pour asseoir sa crédibilité, l'usurpateur apporte une abondance de détails sur l'entreprise, le marché public, l'administration et son environnement. Il peut être en mesure de **présenter des factures obtenues préalablement de manière frauduleuse.** L'escroc peut même faire usage de flatteries ou de menaces pour mieux parvenir à manipuler.

Une demande inhabituelle dans son contenu

Doivent susciter la plus grande vigilance :
- toute demande de **virement à l'international** non planifiée, **prétendument** urgente et confidentielle ;
- toute demande de versement à un fournisseur national sur un compte bancaire domicilié **à l'étranger ;**
- toute demande de **changement** des coordonnées téléphoniques, électroniques et bancaires du fournisseur, du factor ou du cessionnaire;
- toute adhésion récente d'un fournisseur à une société d'**affacturage.**

À noter : l'affichage d'un numéro de téléphone avec un indicatif français, et/ou la production de coordonnées bancaires domiciliées en France, ne constituent pas des garanties.

Une demande inhabituelle dans sa forme

La demande de changement de coordonnées bancaires adressée par l'escroc présente des **incohérences avec les pièces justificatives de la dépense** (facture, acte d'engagement, acte de cession...).
Les écarts (parfois minimes) peuvent porter notamment sur les adresses du fournisseur (ou du factor, du cessionnaire), le numéro SIRET, la dénomination ou le logo de l'entreprise. La demande peut également contenir des **fautes d'orthographe et de syntaxe.**

L'escroc peut utiliser une **adresse de messagerie très proche de l'adresse habituelle** de l'entité dont l'identité a été usurpée :

Exemple :

s.charrier@les_pros_du_btp.com	*s.charrier@les_pros_btp.com*
Adresse habituelle	**Adresse de l'escroc**

ou qui change lorsque l'on répond au courriel :

Exemple :

s.charrier@les_pros_du_btp.com	*compta@financier.com*
Adresse qui s'affiche	**Adresse sur laquelle la réponse est en réalité envoyée**

Comment se prémunir de l'escroquerie ?

• **Sensibiliser régulièrement l'ensemble des agents concernés** (services prescripteurs, services financiers, comptables, secrétariat et standard, ...) à ce type d'escroquerie. Prendre l'habitude d'informer systématiquement les remplaçants sur ces postes.

• Accroître la vigilance pendant les **périodes de congés** et de forte **charge de travail.**

• Instaurer des procédures de **vérifications complémentaires** pour les **paiements internationaux.**

• **Diffuser les alertes** transmises par les fournisseurs déjà cibles d'une escroquerie à l'ensemble des acteurs de la chaîne de traitement de la dépense.

• **Ne pas divulguer** à l'extérieur, ou à un contact inconnu, des informations sur le fonctionnement de l'administration et sur ses fournisseurs (organigramme, contacts, documents comportant la signature d'acteurs-clés, procédures internes, ...). Dans le cadre professionnel, divulguer ces informations avec mesure et en les restreignant au strict nécessaire.

• Avoir un **usage prudent** des réseaux sociaux privés et professionnels.

Comment déjouer la fraude ?

- **L'agent ne doit pas céder à la pression d'un interlocuteur qui souhaiterait un paiement rapide. Au moindre doute, il doit en référer immédiatement à sa hiérarchie.**
- **À tous les niveaux de la chaîne de la dépense (des services prescripteurs au comptable), les agents doivent porter un regard critique sur toute demande urgente ou transmission de nouvelles coordonnées bancaires.**
- **En cas de doute sur des nouvelles coordonnées téléphoniques, électroniques ou bancaires, il faut rompre la chaîne des échanges de courriels ou d'appels téléphoniques, en saisissant soi-même l'adresse électronique du donneur d'ordre, ou en le contactant directement avec les coordonnées déjà connues de la société ou récupérées dans un annuaire public (procédure du contre-appel).**

Que faire face à une escroquerie ?

• L'ordonnateur doit **immédiatement en informer le comptable.**

D'une manière générale, en cas de fraude suspectée ou avérée, l'ordonnateur 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.

  • Si le paiement n'est pas encore intervenu : le comptable suspend immédiatement le mandat ou la demande de paiement, et bloque la mise en paiement.

  • Si le paiement a été réalisé : le comptable actionne les procédures bancaires pour tenter de récupérer les fonds versés.

• **Demander immédiatement le blocage** des coordonnées bancaires frauduleuses dans les applications métiers.

• **Renforcer les actions de sensibilisation** de l'ensemble des acteurs de la chaîne de la dépense, afin d'éviter que le cas ne se reproduise.

Retrouvez la DGFiP sur

Direction générale des Finances publiques

Juillet 2020