RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

LE POINT SUR

LES ESCROQUERIES AUX

FAUX ORDRES DE VIREMENT FOVI

Les FINANCES PUBLIQUES Vous accompagnent

Qu'est-ce qu'un FOVI ?

Une fraude au FOVI est le détournement d'un virement attendu sur le compte bancaire d'un créancier, par usurpation de son identité.

Elle touche toutes les collectivités, quelle que soit leur taille.

LE MODE OPÉRATOIRE LE PLUS RÉPANDU : LE CHANGEMENT DE RIB VIA USURPATION D'IDENTITÉ

Le fraudeur contacte (par téléphone, courrier, courriel) les services de l'ordonnateur en se faisant passer pour un fournisseur, un pensionné, un agent public ou en mettant en place un faux affacturage.

Il transmet de nouvelles coordonnées bancaires, d'un compte souvent ouvert dans une néo banque (banque sans agence) ou à l'étranger et/ou une facture falsifiée pour en détourner les règlements.

La collecte en amont des renseignements sur internet ou par piratage des adresses de messagerie permet aux escrocs d'avoir une très bonne connaissance de l'entreprise et des contrats qu'elle a passés.

Dans des cas plus rares de **« fraude au président »**, l'escroc se fait passer pour la direction et demande à un agent de la collectivité d'effectuer en urgence un virement important à un tiers.

Les bons gestes de prévention

- LE CONTRE-APPEL au fournisseur ou à l'agent qui demande le changement de son RIB pour paiement de sa paye, à partir de coordonnées fiables (dossier, site internet de l'entreprise ou pages jaunes), et non à partir de coordonnées dans un mail ou dans les pièces justificatives jointes au paiement (factures…) ;
- LE RÉFLEXE CHORUS PRO pour la transmission des factures ou les changements de RIB ;
- Restez discrets sur le fonctionnement de la collectivité ou de ses fournisseurs ;
- Soyez vigilants pendant les périodes de congés et de forte charge de travail ;
- Mentionnez les coordonnées bancaires sur l'ensemble des documents contractuels ;
- Pensez à **sensibiliser régulièrement** l'ensemble des agents concernés : service financier, comptabilité, gestionnaire RH, secrétariat et standard…
- RISQUE DE PIRATAGE DE MESSAGERIE :

  → **changer de mot de passe régulièrement et au moindre doute ;**
  → **ne jamais cliquer sur des liens ;**
  → **ne pas prendre contact à partir de messages suspects ;**
  → **ne jamais communiquer d'informations d'authentification de messagerie (y compris au fournisseur d'accès).**

En cas d'escroquerie, réagissez vite !

1. **Informez immédiatement le comptable public de votre collectivité.**

   Lui communiquer :

   - les coordonnées bancaires présumées frauduleuses ;
   - les pièces (courriels, etc.) avec le nom de l'escroc présumé, son adresse de messagerie, son numéro de téléphone.

2. **Identifiez les paiements déjà réalisés, à venir ou en instance,** pour effectuer les **rejets et blocages** nécessaires et en avertir le comptable.

3. **Bloquez les coordonnées bancaires frauduleuses dans les applications informatiques de la collectivité locale.**

4. **Portez plainte auprès d'un service de police ou de gendarmerie,** le plus rapidement possible.

Les signaux d'alerte

Vigilance à avoir :

- lors d'une demande de **changement de RIB au profit d'une néo banque** ou d'une banque étrangère
- lors de toute transmission de factures ou de nouveaux RIB par courriel, hors Chorus Pro

- sur les **adresses mails d'envoi** :
  - adresses électroniques de type : @gmail.com, @servicecomptabilite.net par exemple
  - adresses quasiment similaires à l'adresse habituelle

- sur la **rédaction des courriels** : fautes d'orthographe, syntaxe, logo flou...

Pour en savoir plus

LES SITES À CONSULTER :

collectivites-locales.gouv.fr

cybermalveillance.gouv.fr

Retrouvez les Finances publiques sur

Direction générale des Finances publiques
Octobre 2024