



RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*



FINANCES PUBLIQUES

# Les risques d'escroqueries aux faux ordres de virement (FOVI)

*Direction générale des Finances publiques*

*Mission Responsabilité, Doctrine et Contrôle Interne Comptables*

*Août 2024*

# Sommaire

(1) Quelques éléments de contexte

(2) Quels signes doivent alerter ?

(3) Comment se prémunir des FOVI ?

(4) Que faire en cas d'escroquerie ?

(5) Les outils disponibles

# Sommaire

**(1) Quelques éléments de contexte**

**(2) Quels signes doivent alerter ?**

**(3) Comment se prémunir des FOVI ?**

**(4) Que faire en cas d'escroquerie ?**

**(5) Les outils disponibles**

## (1) Quelques éléments de contexte

### Qu'est-ce qu'un FOVI ?

L'acronyme FOVI signifie faux ordre de virement.

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

C'est un type de fraude.

## (1) Quelques éléments de contexte

➤ **Le rôle de la Mission responsabilité, doctrine et contrôle interne comptables (MRDCIC)**

Recensement des fraudes aux FOVI pour la DGFIP et pilotage du dispositif de lutte dans la sphère publique :

*État,*

*établissements publics,*

*secteur local et hospitalier.*

→ **Centralisation des signalements d'escroqueries aux FOVI (tentatives et cas avérés)**

→ **Sensibilisation et actions de communication** auprès du réseau DGFIP et des collectivités publiques.

## (1) Quelques éléments de contexte

### ▸ Les fraudes au FOVI

- sont identifiées depuis 2010 ;
- concernent l'ensemble des acteurs publics et privés ;
- sont en forte recrudescence pour le secteur public.

## (1) Quelques éléments de contexte

### L'usurpation d'identité du fournisseur ou d'un agent public



L'escroc contacte les services de l'ordonnateur ou du comptable, en se faisant passer pour un fournisseur

L'escroc transmet alors de nouvelles coordonnées bancaires et/ou une facture falsifiée afin de détourner les prochains règlements.

Dans le cadre de la rémunération ou la pension des agents publics, une variante consiste à usurper l'identité d'un agent afin de détourner la paye ou la pension qui lui est due.

## (1) Quelques éléments de contexte

La réussite de ces escroqueries repose sur une **très bonne connaissance de l'entreprise** (fournisseur) dont l'identité a été usurpée **et des contrats qu'elle a passés** avec l'administration.



Préalablement à tout contact, et afin de crédibiliser leur démarche, **les escrocs collectent un maximum de renseignements** sur la cible de l'escroquerie (réseaux sociaux, sites internet relatifs à la commande publique, etc).

Les escrocs peuvent également obtenir des informations directement, en **piratant la messagerie** du fournisseur et/ou de l'entité publique.



## (1) Quelques éléments de contexte

### La fraude au président



L'escroc **se fait passer pour un haut responsable ou pour une autorité** (président d'une université, commissaire aux comptes, banquier, fonctionnaire de police voire ministre...) et au moyen de pressions, demande à un agent **d'effectuer en urgence un virement important et confidentiel sur un compte**, souvent domicilié à l'étranger.

Ce mode opératoire est notamment répandu auprès des établissements publics.

*Par exemple* : un CHU a mandaté sur une facture lui ayant été adressée en urgence, après plusieurs relances reçues par messagerie de la part du directeur général du CHU ayant été usurpé via un mail avec ses nom et prénom mais venant en fait d'une autre adresse mail.

## (1) Quelques éléments de contexte

### A retenir

L'usurpation d'identité du fournisseur est le type d'escroquerie le plus répandu dans la sphère publique.

Préalablement à l'escroquerie, les escrocs cherchent à obtenir des informations sur l'organisation et le fonctionnement d'une entreprise et de ses clients, et parviennent à récupérer des factures en instance de paiement.

Ces factures sont ensuite falsifiées, puis envoyées aux services ordonnateurs (le plus souvent par mail), accompagnées d'une demande frauduleuse de changement de coordonnées bancaires.

# Sommaire

(1) Quelques éléments de contexte

**(2) Quels signes doivent alerter ?**

(3) Comment se prémunir des FOVI ?

(4) Que faire en cas d'escroquerie ?

(5) Les outils disponibles

## (2) Quels signes doivent alerter ?

➤ **Demandes de changement de coordonnées bancaires** au profit d'un compte de **néobanques** (banques mobiles, sans agence).

- Nickel,
- Revolut,
- Bunq,
- Qonto,
- Prepaid – PFS Card,
- Ma French Bank (la Banque postale),
- Anytime - Orange bank...

**Attention** : le nom de la banque pouvant être falsifié sur le RIB (mention d'une banque traditionnelle à la place de la néo banque), se fier plutôt au code BIC ou au code Banque pour identifier les néo banques.

## (2) Quels signes doivent alerter ?

NOM DE LA BANQUE	CODE BIC
FINANCIÈRE DES PAIEMENTS ÉLECTRONIQUES (NICKEL)	FPELFR21
PFS CARD SERVICES	PRNSFRP1
BUNQ	BUNQFRP2
REVOLUT	REVOFRP2
TREEZOR	TRZOFR21
BOURSORAMA	BOUSFRPP
MA FRENCH BANK	LBDIFRP1
OKALI (BLANK)	SFPEFRP2
PPS EU SA (ANYTIME)	PSSSFR22
SHINE	SNNNFR22
SOGEXIA	SOXAFR2L

## (2) Quels signes doivent alerter ?

- **Demandes de changement de coordonnées bancaires** au profit d'un **compte étranger**.

L'IBAN d'un compte ouvert dans une **banque française** commence toujours par **FR**.

L'IBAN d'un compte ouvert dans une **banque à l'étranger** commencera par exemple par :

**GB** : Grande Bretagne

**ES** : Espagne

**PT** : Portugal

**Doute à avoir si :  
IBAN à l'étranger  
pour une société  
située en France.**



	
<small>Identifiant national de compte bancaire - RIB</small>	
<small>Identifiant international de compte bancaire</small>	
<small>IBAN (International Bank Account Number)</small> <b>BE70 3630 7298 5430</b>	<small>Domiciliation</small> <b>BEBBBRUB</b>
<small>Domiciliation</small> <b>IGN Banque</b> Avenue Manix 24 1000 Bruxelles Belgique	<small>BIC (Bank Identifier Code)</small> <b>BEBBBRUB</b>
<small>Titulaire du compte (Account Owner)</small> <b>les Pros du BTP</b> 13 et 15 rue Jose BP 50018 Thorue 83800	
<small>Remettez ce relevé à tout autre organisme ayant besoin de connaître vos références bancaires pour la domiciliation de vos virements ou de prélèvements à votre compte. Vous éviterez ainsi des erreurs ou des retards d'exécution.</small>	

## (2) Quels signes doivent alerter ?

Exemple de RIB falsifié :

Le nom de la banque ne correspond pas au BIC/ IBAN qui devrait être CMC

**Crédit Mutuel**  
RELEVÉ D'IDENTITÉ BANCAIRE

Identifiant national de compte bancaire - RIB

Banque	Guichet	N° compte	Clé	Devise	CCM	Domiciliation
21	00001	0001 80	18	EUR		NORD SARTHE

Identifiant international de compte bancaire

IBAN (International Bank Account Number)						BIC (Bank Identifier Code)
FR76	21	000	0100	8	018	PRNSFRP1

Domiciliation  
CCM

Titulaire du compte (Account Owner)

☎ 0 820 02 67 63 (Service 0,12 €/min + prix appel)

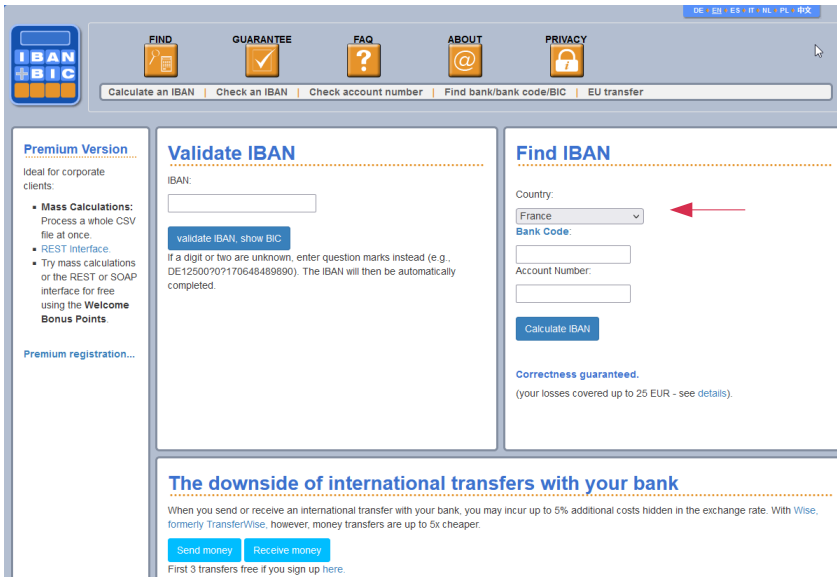
Remettez ce relevé à tout autre organisme ayant besoin de connaître vos références bancaires pour la domiciliation de vos virements ou de prélèvements à votre compte. Vous éviterez ainsi des erreurs ou des retards d'exécution.

PARTIE RESERVEE AU DESTINATAIRE DU RELEVÉ

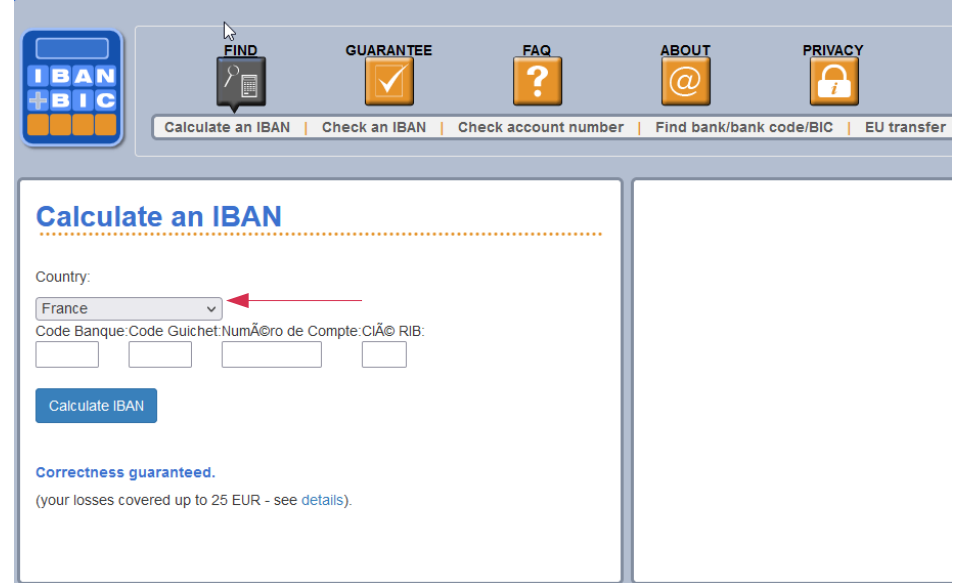
## (2) Quels signes doivent alerter ?

En cas de doute sur une **demande de changement de coordonnées bancaires**, il est possible de consulter le site [IBANCALCULATOR](https://www.ibancalculator.com)

Il permet de contrôler l'association banque/IBAN pour le bénéficiaire du paiement :  
si la **banque est différente de celle indiquée sur le RIB**, il y a risque de falsification.



The screenshot shows the top navigation bar with icons for FIND, GUARANTEE, FAQ, ABOUT, and PRIVACY. Below the navigation bar, there are two main sections: 'Validate IBAN' and 'Find IBAN'. The 'Validate IBAN' section has a text input field for the IBAN, a 'validate IBAN, show BIC' button, and a note about unknown digits. The 'Find IBAN' section has a 'Country' dropdown menu (set to France), a 'Bank Code' input field, an 'Account Number' input field, and a 'Calculate IBAN' button. A red arrow points to the 'Country' dropdown. Below these sections, there is a section titled 'The downside of international transfers with your bank' with a 'Send money' button and a 'Receive money' button.



The screenshot shows the top navigation bar with icons for FIND, GUARANTEE, FAQ, ABOUT, and PRIVACY. Below the navigation bar, there is a 'Calculate an IBAN' section. It features a 'Country' dropdown menu (set to France), a 'Code Banque: Code Guichet: Numéro de Compte: CI@ RIB:' label, and four input fields for the code. A 'Calculate IBAN' button is located below the input fields. A red arrow points to the 'Country' dropdown. Below the section, there is a 'Correctness guaranteed.' note with a link to 'details'.



## (2) Quels signes doivent alerter ?

### ➤ Focus Affacturage :

**Rappel** : une convention par laquelle une entreprise transfère ses créances (factures, mémoires, situations de travaux...) à un établissement spécialisé (factor ou société d'affacturage ou société de factoring).

Vigilance à avoir pour :

→ **Demandes de changements de coordonnées bancaires** pour un affacturage, particulièrement un compte de **néo-banque** ou un **compte étranger**.

→ **Aux affacturages par subrogation** pour lesquels des contrats d'adhésion seraient joints aux pièces justificatives; ces contrats n'étant pas requis, de tels cas de figure doivent questionner et attirer l'attention.

Les escrocs peuvent également se présenter en tant qu'**organisme financier bénéficiaire** d'un affacturage (affactureur ou factor).

→ en cas de doute, le site [REGAFI](https://www.regafi.fr) (*Registre des agents financiers de la Banque de France*) permet de s'assurer que l'organisme dispose bien d'un agrément de la Banque de France.

## (2) Quels signes doivent alerter ?



français | english

### Activité d'agrément des banques

L'agrément des  
entreprises du secteur  
financier

Les types d'agrément

Les informations  
contenues dans  
REGAFI

### Informations ACPR

Décisions de retrait  
d'agrément

Mises en garde du  
public

Autorité de contrôle  
prudentiel et de  
résolution

### Conseil pour la recherche

Aide

[Glossaire](#) [Liens utiles](#)

## Bienvenue sur le site

Le registre des agents financiers

Dernière mise à jour du registre : 28 juin 2023

Vous pouvez rechercher dans le registre les entreprises autorisées à exercer une activité bancaire, financière, de monnaie électronique ou de services de paiement, réglementée conformément au code monétaire et financier.

### Recherche simple

Vous effectuez une recherche sur la dénomination pour une personne morale ou sur le nom pour une personne physique. Vous saisissez soit la dénomination entière, soit un des mots contenus dans la dénomination.

Dénomination / Nom :

Lancer la recherche

### Recherche avancée

Vous effectuez une recherche à partir de plusieurs critères. Le moteur de recherche restitue les établissements référencés dans le registre qui correspondent aux critères que vous avez choisis. Le résultat de la recherche comporte un ou plusieurs établissements et vous avez la possibilité d'afficher des informations complémentaires sur chacun d'entre eux.

## (2) Quels signes doivent alerter ?

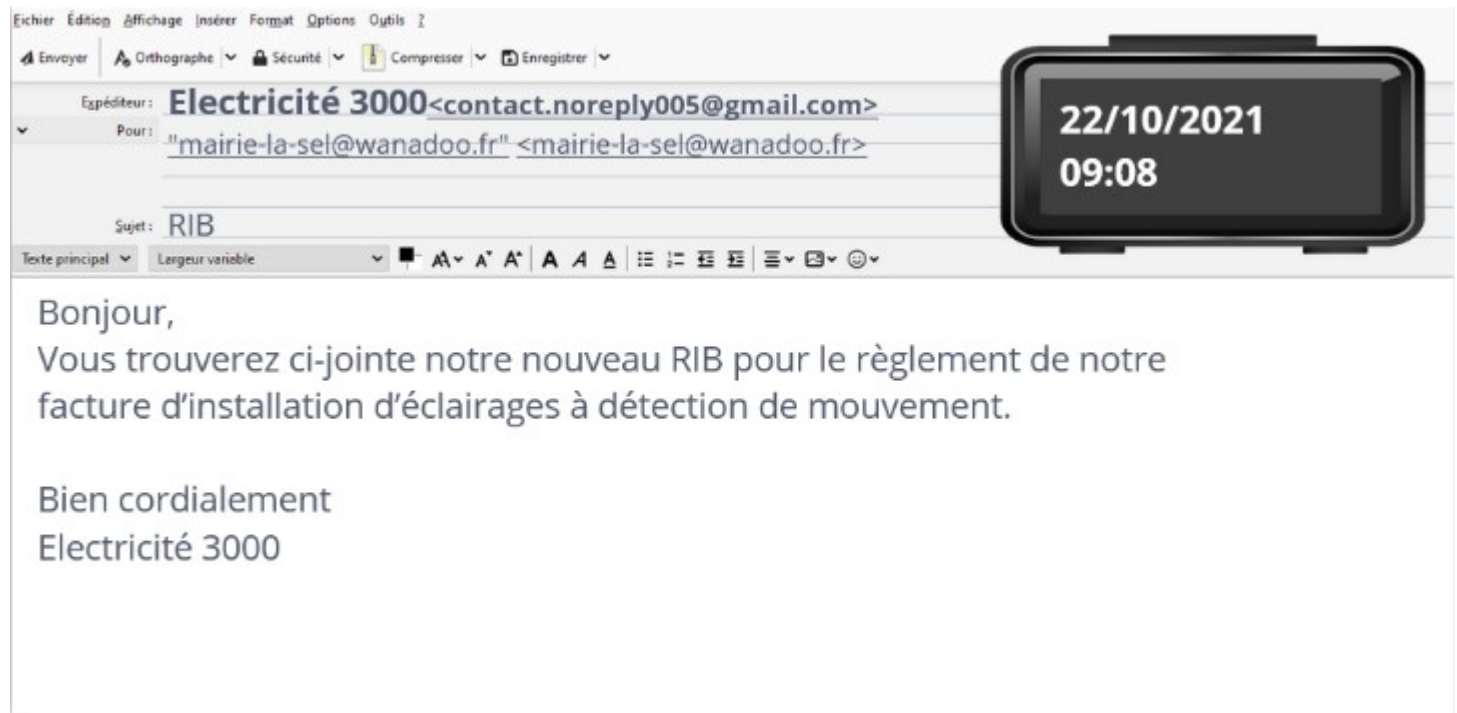
### ➤ Quelques éléments de contact incohérents :

- adresses électroniques de type : contact.noreplyXXX@gmail.com ou noms de domaine de type :
    - @dr.com,
    - @mail.com,
    - @servicecomptabilite.net,
    - @financier.com ,
    - @proton.me,
    - @protonmail.com,...
  - courriels avec des fautes d'orthographe, le logo et/ou l'adresse de messagerie légèrement modifiés, etc.
- **Demandes de confirmation** de virement/date de paiement, pressions.

## (2) Quels signes doivent alerter ?

### Usurpation d'identité du fournisseur

Exemple de demande de changement de coordonnées bancaires adressée par l'escroc après piratage de la boîte mel du fournisseur.



## (2) Quels signes doivent alerter ?

Expéditeur : Anne BEJAR <annebejar@collectivite.fr>  
Pour : compta@financier.com  
Sujet : Re: Changement de coordonnées bancaires Marché 2019-23

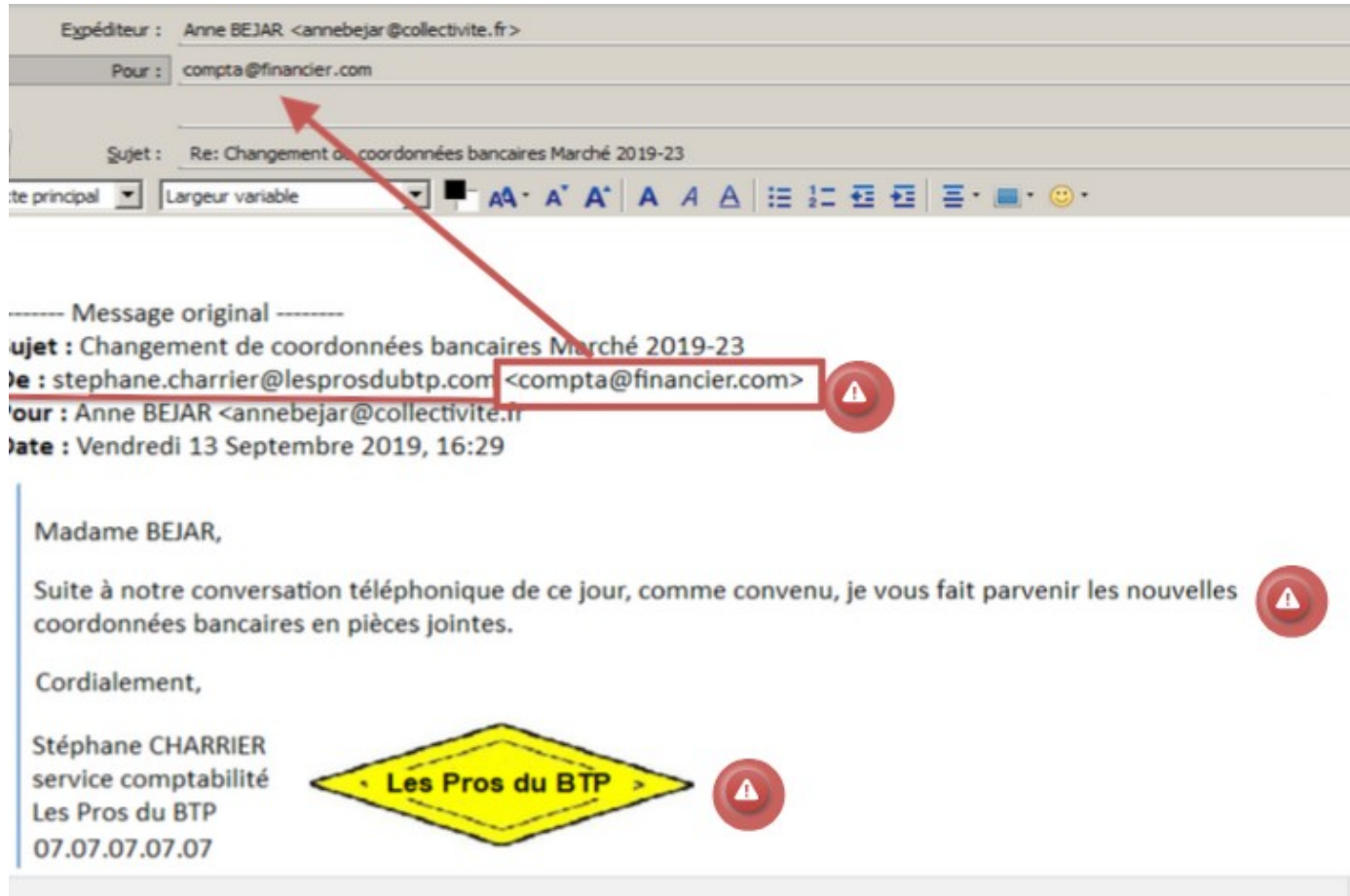
----- Message original -----  
Sujet : Changement de coordonnées bancaires Marché 2019-23  
De : stephane.charrier@lesprosdubtp.com <compta@financier.com>  
Pour : Anne BEJAR <annebejar@collectivite.fr>  
Date : Vendredi 13 Septembre 2019, 16:29

Madame BEJAR,

Suite à notre conversation téléphonique de ce jour, comme convenu, je vous fait parvenir les nouvelles coordonnées bancaires en pièces jointes.

Cordialement,

Stéphane CHARRIER  
service comptabilité  
Les Pros du BTP  
07.07.07.07



# Sommaire

(1) Quelques éléments de contexte

(2) Quels signes doivent alerter ?

**(3) Comment se prémunir des FOVI ?**

(4) Que faire en cas d'escroquerie ?

(5) Les outils disponibles

## (3) Comment se prémunir des FOVI ?

- Effectuer un **contre-appel** au fournisseur à partir de **coordonnées fiabilisées** (dossier de marché, site internet de l'entreprise ou pages jaunes) et pas à partir de coordonnées mentionnées dans un mail ou dans les pièces justificatives jointes au paiement (factures...)
- **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, etc.).
- Accroître la vigilance pendant les **périodes de congés** et de **forte charge de travail**.
- Mentionner les **coordonnées bancaires** sur l'ensemble des **documents contractuels**.

## (3) Comment se prémunir des FOVI ?

- Accroître la vigilance sur le **risque de piratage des boîtes de messagerie** :
  - changer de mot de passe de connexion régulièrement et en cas de 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).
  
- **Focus paye** : effectuer le dépôt du nouveau RIB papier directement par l'agent public au service RH de l'ordonnateur.

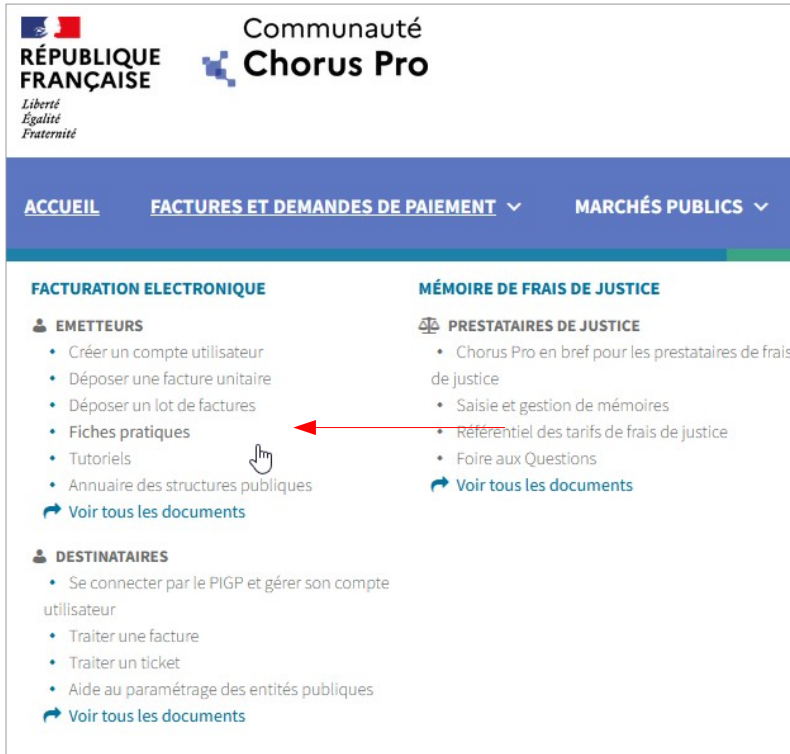


## (3) Comment se prémunir des FOVI ?

### ➤ Adopter les réflexes **CHORUS PRO** :

*Obligation pour les entreprises depuis l'ordonnance du 26 juin 2014 et le décret du 2 novembre 2016*

→ prendre en compte **uniquement les factures transmises par Chorus Pro**, afin de limiter le risque de falsification très présent lors des envois par messagerie ou par voie papier ;



De la documentation est disponible sur la **communauté Chorus pro** accessible sur internet :

→ Fiches pratiques

→ Tutoriels...

# Sommaire

(1) Quelques éléments de contexte

(2) Quels signes doivent alerter ?

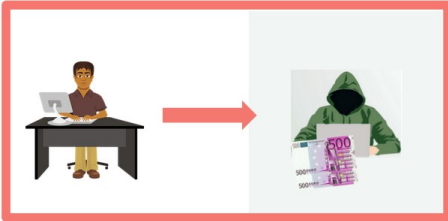
(3) Comment se prémunir des FOVI ?

**(4) Que faire en cas d'escroquerie ?**

(5) Les outils disponibles

## (4) Que faire en cas d'escroquerie ?

Dans le cas d'une **escroquerie avérée** (les sommes ont été payées sur un compte frauduleux)



### Action 1 : informer immédiatement le comptable public

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.

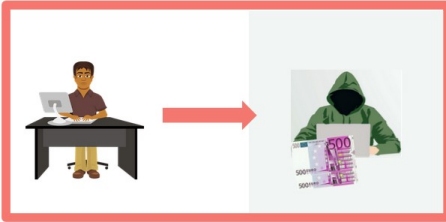
*Le comptable actionnera les procédures bancaires pour tenter de récupérer les fonds versés.*

### Action 2 : identifier l'ensemble des paiements en instance

Vérifier si d'autres paiements ont déjà été réalisés sur le compte bancaire frauduleux ou sont en instance pour en avvertir le comptable.

## (4) Que faire en cas d'escroquerie ?

Dans le cas d'une **escroquerie avérée** (les sommes ont été payées sur un compte frauduleux)



**Action 3 : bloquer les coordonnées bancaires présumées frauduleuses dans les différentes applications de la collectivité et de l'établissement**

**Action 4 : réaliser un dépôt de plainte**

Pour engager des poursuites pénales, le **dépôt de plainte** devra être engagé par l'établissement dans les plus brefs délais.

Les **éléments et pièces de l'escroquerie** (chronologie des faits, RIB frauduleux, identité donnée par l'escroc, adresses de messagerie, n° téléphone, etc.) devront être mentionnés.

Une **copie de la plainte sera transmise au comptable public.**

## (4) Que faire en cas d'escroquerie ?

Dans le cas d'une tentative de fraude (aucun paiement n'a été réalisé)



**Action 1 : prévenir immédiatement le comptable** et lui transmettre dans les meilleurs délais, les pièces liées à l'escroquerie (échanges de courriels avec l'escroc demandant le changement de RIB, etc.).

Le comptable :

- bloquera immédiatement la demande de paiement ;
- demandera le blocage du compte bancaire dans Hélios.

**Action 2 : invalider les coordonnées bancaires frauduleuses** dans la base tiers du logiciel financier.

**Action 3 : déposer plainte** en tant que victime directe d'escroquerie.

# Sommaire

(1) Quelques éléments de contexte

(2) Quels signes doivent alerter ?

(3) Comment se prémunir des FOVI ?

(4) Que faire en cas d'escroquerie ?

**(5) Les outils disponibles**

## (5) Les outils disponibles

Le site gouvernemental [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

- pour comprendre les menaces et agir ;
- pour adopter les bonnes pratiques ;
- récapitulatif des 10 mesures essentielles pour assurer la cybersécurité.



The screenshot shows the homepage of the French government's cyber security portal. At the top, there is a navigation bar with the French Republic logo and the site name 'CYBER MALVEILLANCE .GOUV.FR'. To the right are links for 'ESPACE PRESTATAIRE', 'MON ESPACE', a search icon, and a language icon. Below this is a main navigation menu with four categories: 'LES MENACES ET BONNES PRATIQUES', 'L'ACTUALITÉ DE LA CYBERMALVEILLANCE', 'NOUS DÉCOUVRIR', and 'VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?'. A breadcrumb trail indicates the current location: 'Accueil → Les bonnes pratiques'. Below the navigation is a secondary menu with three tabs: 'PARTICULIERS', 'PROFESSIONNELS', and 'COLLECTIVITÉS', with 'COLLECTIVITÉS' being the active tab. The main content area features a heading: 'Je suis une collectivité, je voudrais me documenter sur les bonnes pratiques relatives à toutes les menaces'. Below this is a featured article titled 'Que faire en cas de cyberattaque ? (Consignes pour les collaborateurs)'. The article's text states: 'Ce document synthétique vise à fournir aux collaborateurs les consignes d'urgence à appliquer pour réagir en cas de cyberattaque et ainsi aider l'organisation à répondre au plus vite à l'incident pour améliorer ses chances d'y faire face.' At the bottom of the article is a button labeled 'EN SAVOIR PLUS →'. The article image shows a hand pointing to a red key on a keyboard labeled 'Premiers Secours'.

## (5) Les outils disponibles

Le site gouvernemental [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

→ des ressources utiles mises à disposition :

- Kit de sensibilisation aux risques numériques ;

- Méthode de sensibilisation « clé en main » :

- Fiche synthétique des 5 clés
- 4 thématiques (hameçonnage, gestion des mots de passe...) sous plusieurs formats (vidéo,...)
- Outils d'animation
- Témoignages de collectivités victimes de cyberattaques...

- etc.





# (5) Les outils disponibles

## Le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

The screenshot shows the ANSSI website interface. At the top left is the French Republic logo with the motto 'Liberté, Égalité, Fraternité'. Next to it is the ANSSI logo, a circular emblem with a shield and the text 'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI'. A search bar on the right contains the text 'Rechercher...' and a magnifying glass icon. Below the logos is a horizontal menu with seven items: 'Découvrir l'ANSSI', 'Découvrir la cybersécurité', 'Développer des solutions de confiance', 'Sécuriser son organisation', 'Se former à la cybersécurité', 'Connaître et explorer', and 'S'informer sur la réglementation'. The main content area features a dark blue banner with the title 'Bonnes pratiques - Protégez-vous !' and a subtitle 'Assurer sa cybersécurité, c'est beaucoup de bon sens et quelques efforts. Pour autant, rien ne vaut un rappel des fondamentaux !'. Below the banner, on the left, is a sidebar with a 'Se protéger' link and a section titled 'Dix règles d'or préventives' containing a link to 'Bonnes pratiques - Protégez-vous !'. On the right, the main content area shows the publication date 'Publié le 13 Juillet 2022 • Mis à jour le 17 Novembre 2023', the introductory text 'À elles seules, ces dix bonnes pratiques vous protégeront de l'immense majorité des risques numériques qui pèsent sur vos usages personnels ou professionnels.', and a list of two practices: '1. Gérez vos mots de passe avec soin' and '2. Sauvegardez régulièrement vos données', each with a plus sign icon.

# L'essentiel à retenir

Les agents doivent appliquer les règles de vigilance suivantes :

- Faire preuve de **prudence lors des échanges** avec les fournisseurs ;
- Savoir détecter les **signaux d'alerte** ;
- Être particulièrement méfiant face à **toute demande de modification de coordonnées bancaires**, notamment lorsque le nouvel IBAN est un compte étranger ou ouvert sur une néo-banque ;
- Promouvoir utilisation de **Chorus Pro**.

→ au moindre doute effectuer un « contre-appel »