ESCROQUERIE AUX FAUX ORDRES DE VIREMENT (HORS DÉPENSES FISCALES)

Mode opératoire

L'escroquerie aux faux ordres de virement vise à **pousser un salarié ou un agent public à effectuer un virement sur un compte bancaire frauduleux**, en **usurpant l'identité** du véritable créancier ou d'un autre acteur habilité à intervenir dans la chaîne du règlement.

Trois modes opératoires sont actuellement identifiés : l'escroquerie au changement de coordonnées bancaires, la fraude au président, l'escroquerie à l'informatique.

Dans la sphère publique, les **demandes frauduleuses de changement de coordonnées bancaires** constituent le mode opératoire le plus répandu.

Comment s'en prémunir ?

Tous les agents intervenant dans la chaîne de la dépense doivent :

- faire preuve de **prudence lors des échanges** avec les fournisseurs et les ordonnateurs ;
- savoir **détecter les signaux d'alerte** (fautes d'orthographe, erreurs de syntaxe, logo et/ou adresse de messagerie légèrement modifiés, adresse comportant une terminaison « suspecte ») ;
- être particulièrement **méfiants face à tout changement de coordonnées bancaires ou affacturage** ;
- consulter **FICOBA** et effectuer un **contre-appel**, en cas de doute.

Le contre-appel doit être réalisé à partir des coordonnées téléphoniques figurant sur le marché, le site internet de l'entreprise ou un annuaire. **Il ne faut jamais contacter le fournisseur à partir des coordonnées mentionnées dans un mail ou dans les pièces justificatives transmises pour le paiement**, puisque celles-ci peuvent avoir été falsifiées.

Pour en savoir plus :

Espace FOVI sur Ulysse > Gestion publique > Contrôle interne comptable et bancaire > Escroquerie aux faux ordres de virement

E-formation FCE210ET relative à « la lutte contre les escroqueries aux faux ordres de virement »

Fiche relative aux actions à réaliser en cas d'escroquerie aux FOVI

Actions à réaliser en cas de fraude :

Il convient de **vérifier immédiatement si des paiements ont été réalisés**.

CAS 1. Il s'agit d'une escroquerie avérée :

Une fraude est suspectée et un ou plusieurs paiements ont été réalisés vers le compte bancaire présumé frauduleux.

4 actions cumulatives doivent être réalisées rapidement :

1. adresser immédiatement à la **Banque de France une demande de blocage des fonds**, à partir du mail de signalement disponible sur Ulysse ;
2. engager une procédure de **SCT Recall** auprès de l'ESI PSAR compétent (Rouen pour les virements émis à partir de CHORUS ou Hélios / Châlons pour les virements émis par les clients DFT ;
3. adresser un **signalement urgent à la Mission RDCIC**, accompagné des pièces frauduleuses transmises par l'escroc. La Mission saisira le bureau RH2B ;
4. **réaliser un dépôt de plainte** après expertise du bureau RH-2B puis transmettre la copie à la Banque de France, la Mission RDCIC et au bureau RH2B.

NOTA : La réalisation de ces actions ne garantit pas la récupération systématique des fonds escroqués.

CAS 2. Il s'agit d'une tentative d'escroquerie :

Une fraude est suspectée mais aucun paiement n'a été réalisé vers le compte bancaire présumé frauduleux.

Un **signalement urgent** doit être adressé **à la Mission RDCIC,** accompagné des pièces frauduleuses transmises par l'escroc.

La Mission RDCIC est à la disposition des comptables pour les assister dans toutes leurs démarches. A cet effet, une boite aux lettres électronique dédiée a été créée :

mission.rdcic-escroquerie@dgfip.finances.gouv.fr

PRÉLÈVEMENT FRAUDULEUX

Mode opératoire

Le prélèvement frauduleux est le **détournement, par un tiers, des coordonnées bancaires d'un poste comptable, d'une agence comptable ou d'une régie, pour y domicilier des prélèvements**.

Lors de l'exploitation du relevé de compte Banque de France (BDF) ou Dépôt de fonds au Trésor (DFT), un prélèvement non autorisé est constaté en débit (en l'absence de mandat SEPA signé par le titulaire du compte ou un de ses délégataires).

Exemple : SNCF, SFR, Amazon, etc.

Comment s'en prémunir ?

Le recours au prélèvement SEPA est conditionné à la signature d'un mandat de prélèvement par le comptable public (titulaire d'un compte Banque de France ou Dépôts de Fonds au Trésor sur lequel seront domiciliés les prélèvements), conformément à la réglementation SEPA.

Il est rappelé que l'exploitation des relevés est quotidienne :

- le relevé BDF du jour J doit être téléchargé depuis CADRAN en J+1 et comptabilisé / exploité systématiquement en date comptable de J+1 ;

- le relevé de compte DFT est mis à la disposition du titulaire du compte de manière quotidienne. Ce dernier doit s'assurer au jour le jour de son exploitation.

Pour en savoir plus :

Page n°8 du *bulletin d'informations "Les moyens de paiement" n°4* de décembre 2017

L'espace Ulysse > Gestion Publique > Activités bancaires et moyens de paiement > Foire aux questions MDP (Moyens de paiement)

Actions à réaliser en cas de fraude :

CAS 1. il s'agit d'un prélèvement frauduleux sur un compte BDF :

1. demander le **rejet de l'opération** au moyen de *ce bordereau ;*

2. formuler une opposition au moyen de *cet imprimé ;*

3. saisir le bureau RH2B « Déontologie, protection juridique et contentieux » (*bureau.rh2b@dgfip.finances.gouv.fr)* ;

4. réaliser un dépôt de plainte après expertise du bureau RH-2B **p**uis transmettre une copie de la plainte à ce même bureau.

CAS 2. Il s'agit d'un prélèvement frauduleux sur un compte DFT :

1. demander dans les plus brefs délais **le rejet de l'opération** en s'adressant au teneur de compte ;

2. formuler une opposition en s'adressant au teneur de compte (mention des RUM et ICS concernés) ;

Le mandataire a le droit de contester tout prélèvement SEPA ordinaire (autorisé ou non) jusqu'à 8 semaines maximum après le débit du compte de dépôts de fonds de l'organisme. Passé ce délai, et dans un délai maximum de 13 mois à compter de la date de débit du compte, le mandataire peut contester un prélèvement uniquement si celui-ci n'a pas été autorisé par ses soins.

3. saisir le bureau RH2B « Déontologie, protection juridique et contentieux » (*bureau.rh2b@dgfip.finances.gouv.fr)* ;

4. réaliser un dépôt de plainte après expertise du bureau RH-2B puis transmettre une copie de la plainte à ce même bureau.

FALSIFICATION DE CHÈQUES SUR LE TRÉSOR

Mode opératoire

Ce type d'escroquerie vise à falsifier un chèque sur le Trésor pour en modifier le montant et/ou le bénéficiaire :

- lorsque **le montant du chèque sur le Trésor a été falsifié** et que la **fraude est détectée par le contrôle automatique** réalisé par l'application KHQ (par corroboration entre le numéro du chèque et le montant de celui-ci), il n'y a **pas de préjudice financier**.

- lorsque **le bénéficiaire du chèque a été modifié sans modification du montant** et que le paiement emprunte le circuit interbancaire, il y a **préjudice financier**.

Comment s'en prémunir ?

- **limiter l'usage des chèques sur le Trésor** ;

Compte tenu des risques de fraudes ou de falsification et des coûts inhérents au chèque sur le Trésor, son usage doit rester limité.

Le recours au chèque sur le Trésor doit répondre à des situations d'urgence rendant impossible l'exécution de virement, mode normal de règlement des dépenses (ex: dispositifs d'urgence, aide et secours, catastrophe naturelle,...).

- **procéder à des contrôles lors du paiement en numéraire ;**

Dans le cas d'un paiement en numéraire, le caissier doit interroger KHQ pour vérifier le montant et l'identité du bénéficiaire.

- **faire opposition au moindre doute.**

Qu'il s'agisse d'une présomption de fraude, de falsification ou de vol, avec ou sans préjudice financier, le comptable assignataire doit, sous peine de voir sa responsabilité engagée, enregistrer le jour même les oppositions des chèques sur le Trésor dans l'application KHQ. Si le paiement est demandé ultérieurement, celui-ci est obligatoirement réalisé par virement.

Pour en savoir plus :

Instruction du 22 juillet 2013 relative aux modalités de gestion des moyens de paiement et des activités bancaires du secteur public

Mémento des actions à réaliser par le comptable en cas de falsification ou d'utilisation frauduleuse d'un chèque sur le Trésor

Actions à réaliser en cas de fraude :

S'il y a préjudice financier, procéder immédiatement au **rejet de l'image chèque** sans attendre d'avoir la copie du chèque.

Par ailleurs, qu'il y ait ou non préjudice financier :

1. saisir le bureau RH2B « Déontologie, protection juridique et contentieux » (*bureau.rh2b@dgfip.finances.gouv.fr)* ;

2. déposer plainte après expertise du bureau RH-2B contre personne non dénommée (contre X) pour tentative d'escroquerie auprès du procureur de la République près le tribunal judiciaire.

Remarque :

- indiquer l'identité exacte du remettant, lorsqu'elle est connue ;

- si le bénéficiaire a été falsifié, inviter également le véritable bénéficiaire du chèque détourné à déposer plainte à titre personnel.

3. transmettre la copie du dépôt de plainte :

- systématiquement au bureau RH2B et à la Mission RDCIC (*mission.rdcic-escroquerie@dgfip.finances.gouv.fr*) ;

- au bureau CL1C, quel que soit le montant s'il y a préjudice financier, et uniquement dans les cas où le montant falsifié du chèque sur le Trésor est supérieur à 10 000 euros s'il n'y a pas de préjudice financier (*bureau.cl1c-moyens-de-paiement@dgfip.finances.gouv.fr*) ;

L'objet du courriel sera formalisé comme suit « Fraude chèque sur le Trésor_DDFiP (compléter le n° du département) ».

USURPATION D'IDENTITÉ, DE TITRE, OU DE FONCTION D'UN AGENT

Mode opératoire

CAS 1. Des personnes usurpent l'identité d'un d'agent de la DGFiP :

- par téléphone ou par courriel afin d'**obtenir des informations sensibles ou confidentielles** de la part de son interlocuteur ;
- afin d'**établir de faux documents.**

CAS 2. Des personnes **usurpent le titre et la qualité d'agent des finances publiques** et demandent à des **usagers**, de manière insistante et avec un caractère d'urgence et/ou de menace, des versements d'argent, fréquemment sur des comptes situés à l'étranger.

Comment s'en prémunir ?

La plus grande vigilance est requise quant aux éléments suivants :

- l'**adresse courriel** ne respecte pas la forme ;
- la demande ne respecte pas les **circuits d'information habituels** (voie hiérarchique, circuit entreprise / ordonnateur / comptable, etc.) ;
- la demande porte sur des **informations soumises au secret professionnel et/ou fiscal** ;
- la demande comprend des **inexactitudes sur les grades, les fonctions** (par ex. « contrôleur fiscal ») ;
- l'appel téléphonique reçu ne permet pas d'**identifier sans ambiguïté l'interlocuteur** (appel masqué notamment).

En cas de doute, il convient :

- de **ne donner aucun renseignement,** ni indication, sur l'organisation, les procédures mises en œuvre, l'état d'avancement d'un dossier ;
- de n'**initier aucun acte administratif, comptable ou financier** ;
- de **procéder à un contre-appel** vers un numéro de téléphone issu des annuaires officiels de la DGFiP.

Actions à réaliser en cas de fraude :

CAS 1 : les **tentatives d'usurpation d'identité d'un agent de la DGFIP doivent faire l'objet d'un signalement par la voie hiérarchique au référent protection juridique.**

Ce dernier transmettra le signalement au **bureau RH-2B** en charge de la déontologie, de la protection juridique et du contentieux.

CAS 2 : l'usurpation de la qualité d'agent des finances publiques (ou «des impôts ») constitue le moyen de l'escroquerie, dont l'objectif est de porter préjudice aux usagers.

Il appartient aux directions locales de rappeler aux usagers qui se manifestent que la DGFiP est étrangère à de telles manœuvres et qu'ils sont fondés, en tant que principales victimes de cette tentative d'escroquerie, à déposer plainte.

Pour en savoir plus :

Guide de saisine de la direction générale en cas d'incident contre les agents ou l'administration

Circulaire du bureau RH-2B du 08/04/2013 relative à la création de la fonction de référent protection juridique des agents

RANÇONGICIEL

Mode opératoire

Un rançongiciel (« ransomware » en anglais) est un logiciel malveillant qui bloque l'accès à un ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

Le poste informatique peut être infecté suite à une intrusion dans le système, après avoir ouvert une pièce jointe ou cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis dont un cybercriminel a pris le contrôle.

Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes qui peuvent ainsi perdre définitivement toutes leurs données et leurs historiques sur plusieurs années.

Comment s'en prémunir ?

Il convient d'appliquer les règles de vigilance suivantes :

- **utiliser des mots de passe** suffisamment complexes et les changer régulièrement ;
- appliquer de manière régulière et systématique les **mises à jour de sécurité** du système et des aplications/programmes installés sur les postes informatiques ;
- **tenir à jour l'antivirus et configurer le pare-feu** ;
- **faire des sauvegardes régulières des données** pour pouvoir les réinstaller dans leur état d'origine au besoin et **stocker ces sauvegardes** sur un équipement totalement déconnecté du réseau informatique ;
- **désinstaller les applications ou programmes dont l'éditeur n'assure plus de support** (absence de mise à jour de sécurité) ;
- **n'utiliser un poste de travail en session "administrateur"** que très ponctuellement et uniquement pour des opérations d'administration du poste ;
- **ne pas ouvrir les courriels provenant d'expéditeurs inconnus** ou d'un expéditeur connu mais dont la structure, la syntaxe, l'orthographe et/ou la teneur du message sont inhabituelles ou vides. **Ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens provenant de ces messages** ;
- **ne pas installer d'applications ou de programmes « piratés »,** dont l'origine ou la réputation sont douteuses ;
- **éviter les sites non sûrs ou illicites**.

Actions à réaliser en cas de fraude :

Il est recommandé à la victime de :

- **débrancher** le poste de travail infecté ;
- **éteindre les serveurs** et couper leur accès internet ;
- **ne pas connecter les serveurs de sauvegarde** aux ordinateurs, ni même aucun autre équipement périphérique (clé USB, ...) ;
- **alerter immédiatement** les services informatiques de la structure, et le cas échéant l'éditeur du logiciel de gestion financière ;
- **ne pas payer la rançon** réclamée (le paiement ne garantit pas un déblocage total et définitif du système d'information et pourrait inciter le cybercriminel à réitérer son action) ;
- **saisir les services juridiques** de la structure compétents pour l'engagement éventuel de poursuites pénales ;
- **identifier, si possible, la source et le périmètre** de l'infection et **prendre les mesures nécessaires** pour qu'elle ne puisse pas se reproduire.

Pour en savoir plus :

Fiche de vigilance sur les rançongiciels (dédiée au Secteur Public Local)

HAMEÇONNAGE

Mode opératoire

Le hameçonnage (« phishing » en anglais) est une pratique consistant à envoyer un message électronique à de nombreux destinataires pour récupérer sous un motif fallacieux des informations personnelles et/ou confidentielles.

Ces courriels se présentent comme des messages provenant d'une autorité de confiance (administration fiscale, banque,...), et mentionnent souvent un caractère urgent (compte personnel expirant, ...) ou lucratif (remboursement d'impôt, dossier administratif incomplet, gain de loterie, ...).

Après avoir cliqué sur un lien inclus dans le message, le destinataire tombe ainsi souvent sur un **site piraté imitant le site officiel.**

Il peut également s'agir de courriels contenant une pièce jointe ou un lien piégé, dans le but d'obtenir des informations (personnelles ou confidentielles) depuis le poste du destinataire.

Comment s'en prémunir ?

Certains éléments doivent éveiller la vigilance :

- **émetteur inconnu** ;
- **imitation** des signatures, en-têtes et sites des autorités de confiance ;
- message rédigé **en anglais**, ou, lorsqu'il est rédigé en français, comportant des **fautes d'orthographe** et des **erreurs de syntaxe** ;
- adresse comportant une **terminaison « suspecte »** (@dgfip-finances-gouv.cloud, @dgfip-impots.info, par exemple) ;
- message à **caractère urgent ou lucratif** ;
- message ayant pour but d'obtenir des **données personnelles ou confidentielles** ;
- **indication [phishing]** présente devant l'objet du message.

Pour en savoir plus :

Ulysse > Assistance informatique > Signalement de courriels frauduleux ou indésirables

Actions à réaliser en cas de fraude :

Lorsqu'un message présente ces caractéristiques ou en cas de doute, il convient de :

1. ne pas cliquer sur les liens ni ouvrir les pièces jointes ;

2. signaler le courriel frauduleux :

- en cas d'usurpation de l'identité de la DGFiP : transférer le courriel au bureau SI2B, sur la balf dédiée à cet effet :

phishing@dgfip.finances.gouv.fr

Le bureau SI-2B expertisera les courriels signalés afin de faire interdire les sites internet concernés en recherchant l'origine du lien et appréciera l'opportunité de suites judiciaires.

Pour permettre une meilleure exploitation, les services devront s'assurer que le message frauduleux qu'ils signalent s'accompagne d'un lien encore actif.

Attention, cette BALF ne doit en aucun cas être communiquée aux personnes n'appartenant pas à la DGFiP.

Remarque : Si le signalement est fait par l'usager via e-contact, l'agent doit transmettre le signalement sur la BALF dédiée (cf.supra) et répondre à l'usager que le courriel est un faux et que l'administration fiscale n'est pas à l'origine de ce type d'envois.

- en l'absence d'usurpation de l'identité de la DGFiP, un signalement peut-être effectué à l'adresse suivante :

https://www.internet-signalement.gouv.fr

3. Supprimer le courriel.