

MEMENTO DDFIP 34 LUTTE CONTRE LA FRAUDE

Version CL 1 (juillet 2020)

COVID-19 : VERIFICATION DE L'HONORABILITE DES FOURNISSEURS DE MASQUES

Réflexe :

- Incitation de la part du fournisseur de passer rapidement des commandes de matériels de protection (masques...).
- Fournisseur n'ayant pas d'antériorité dans la fourniture de matériel médical et paramédical
- Demande de paiement de la commande avant service fait.

Protocole à suivre :

1. En liaison avec votre comptable, collecter les documents qui permettront de procéder au contrôle (RIB, factures proformat/devis, SIREN) pour recouper un maximum d'informations sur le fournisseur.
2. En cas d'incohérences, de doutes ou d'informations insuffisantes pour attester à votre niveau de l'honorabilité du fournisseur, votre comptable saisira son interlocuteur à la direction départementale pour obtenir un avis sur le fournisseur.
Délais de traitement : 3 à 5 jours compte tenu de l'affluence des demandes.

PRÉLÈVEMENTS FRAUDULEUX

Réflexe :

Lors de l'exploitation du relevé dépôt de fonds au trésor (DFT), identification d'un débit au moyen d'un prélèvement non autorisé (en l'absence de mandat SEPA signé par le titulaire du compte ou un de ses délégataires).
Exemple : SNCF, Amazon, Facebook.

Protocole à suivre :

1. Formuler une demande de rejet de prélèvement et une demande d'opposition à prélèvement au service DFT de la DDFIP, (ddfip34.pgp.epargne@dgfip.finances.gouv.fr).
2. En informer par courriel votre comptable.
3. Déposer plainte auprès des services de police ou de gendarmerie : [ici](#).

FALSIFICATION DE CHEQUES

Réflexe :

- lors de l'exploitation du relevé DFT de la régie, identification d'un débit comportant un montant erroné (falsification du montant du chèque).
- l'entreprise demande où en est le paiement de sa facture alors qu'il est déjà payé depuis plusieurs jours (falsification du bénéficiaire).

Protocole à suivre :

1. En cas de préjudice financier (falsification du montant), se rapprocher du service DFT de la DDFIP 34 afin de faire procéder immédiatement au rejet de l'image chèque sans attendre d'avoir la copie du chèque.
Les règles de l'échange image chèques permettent en effet de récupérer les sommes irrégulièrement versées en rejetant l'image chèque jusqu'à 60 jours calendaires après sa présentation (uniquement pour les motifs de rejet n° 33 - falsification - surcharge ou n° 34 - faux chèque).
2. Informer votre comptable en reprenant les éléments en votre possession et les démarches effectuées.
3. Déposer plainte contre X pour tentative d'escroquerie auprès du procureur de la République près le tribunal judiciaire en indiquant l'identité exacte du remettant, lorsqu'elle est connue, et y compris en cas d'absence de perte financière.
4. Communiquer au service DFT de la DDFIP et au comptable une copie de la plainte déposée (ddfip34.pgp.epargne@dgfip.finances.gouv.fr).
5. En cas de préjudice financier, inviter le véritable bénéficiaire du chèque détourné à déposer plainte à titre personnel.

FAUX ORDRES DE VIREMENTS (FOVI)

Réflexe :

La formulation de la demande de changement de coordonnées bancaires :

- un nouveau responsable de l'entreprise (directeur, gérant, comptable, société d'affacturage) a demandé un changement de coordonnées bancaires à l'ordonnateur.

- l'adresse courriel qui diffère de celle de l'entreprise est écrite entre guillemets (« ... ») (c'est donc du texte).
- l'adresse courriel de l'expéditeur est inhabituelle (@protonmail.com, @gmail.com, @financier.com, @pm.me).
- insistance de la personne demandant le changement de coordonnées bancaires (caractère urgent, ton provocant, urgence du paiement).

Le contexte :

- période de vacances scolaires,
- nombreuses absences dans le service,
- période de fermeture annuelle de l'entreprise.
- période de crise sanitaire.

Les pièces justificatives :

- le RIB comporte des mentions inhabituelles : compte à l'étranger, banque en ligne/néobanque, adresse contenant « chez », forme inhabituelle du nom de l'entreprise.
- les autres pièces justificatives comportent des éléments inhabituels : mentions nouvelles, forme nouvelle, mentions déplacées.

L'entreprise demande où en est le paiement de sa facture alors que le mandat (ou la demande de paiement) est déjà payé depuis plusieurs jours.

Protocole à suivre :

1. Au moindre doute, effectuer un contre-appel à l'entreprise à partir des pièces d'origine dans le dossier et vérifier par tous moyens (internet, site de l'entreprise, annuaire pages jaunes...) les coordonnées. Ne jamais utiliser le numéro de téléphone indiqué dans la demande. Vérifier l'identité de l'interlocuteur en cas de demandes sur des factures.
2. Signaler immédiatement ses doutes à votre comptable, être rapide et discret.
3. Rassembler les éléments suivants :
 - coordonnées de l'escroc potentiel
 - coordonnées bancaires nouvelles dont RIB,
 - recenser les montants en jeu (mandats/demandes de paiement concernés),
 - collecter les pièces justificatives associées et les contacts avec l'ordonnateur/le comptable,
 - décrire succinctement le mode opératoire.
4. Envoyer un courriel à votre comptable avec l'ensemble des éléments du point précédent.

SUSPICION DE DÉTOURNEMENT

Réflexe :

- inadéquation entre l'activité du service ou de la régie et les écritures budgétaires et comptables,
- discordance entre les mouvements financiers et la comptabilité / opacité du processus de production des informations budgétaires et comptables.
- pratique de la structure non conforme à son objet,
- actions de l'agent non conformes à ses fonctions,
- usagers signalant de manière répétée la réception d'une relance à tort alors qu'ils ont déjà payé la dette en question.

Protocole à suivre :

1. Collecter discrètement le plus de données possibles,
2. Alerter votre comptable et lui transmettre une première analyse de la situation et les données et informations collectées pour déterminer les suites à donner.

AUTRES TYPES DE FRAUDES

COURRIELS FRAUDULEUX – HAMEÇONNAGE

Réflexe :

- message semblant provenir d'une autorité de confiance,
- message à caractère urgent ou lucratif,
- imitation des signatures, entêtes et sites des autorités de confiance, voire de documents de procédure (droit de communication, par exemple).
- adresse courriel d'envoi avec terminaison « suspecte » (@protonmail.com, @gmail.com, @financier.com, par exemple). Vigilance : l'adresse qui s'affiche peut cacher une autre adresse courriel non visible.
- volonté d'obtenir des données personnelles ou confidentielles,
- indication [phishing] présente devant le sujet du message.

Protocole à suivre :

1. Ne jamais cliquer sur les liens ni ouvrir les pièces jointes.
2. En cas de courriel imitant l'identité visuelle et usurpant les missions de la DGFIP, enregistrer le courriel frauduleux au format « .eml » et le joindre à un courriel destiné à votre comptable en indiquant en objet de votre message « courriel frauduleux ». Le comptable transférera ensuite au service dédié le courriel douteux pour analyse.

RANÇONGIELS

Réflexe :

- un logiciel malveillant bloque l'accès à un ordinateur ou à des fichiers et réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès,
- ouverture d'une pièce jointe douteuse ou clic sur un lien malveillant reçu dans des courriels ou encore navigation sur des sites compromis dont un cybercriminel a pris le contrôle.

Protocole à suivre :

1. Débrancher le poste de travail infecté et fermer toutes les connexions à ce poste de travail (serveur, clé USB etc).
2. Alerter immédiatement vos services informatiques, l'éditeur du logiciel de gestion financière et votre comptable.
3. Ne pas payer la rançon réclamée (ne garantit pas un déblocage total et l'absence de réitération du procédé frauduleux).
4. Avertir votre comptable et la Préfecture ou l'ARS.
5. Déposer plainte auprès des services de police ou de gendarmerie.
6. S'informer sur <https://www.cybermalveillance.gouv.fr>

FRAUDES DIVERSES (ex. usurpation d'identité d'agents de la DGFIP)

Réflexe :

- l'adresse courriel ne respecte pas la forme classique des contacts de la DGFIP : @dgfip.finances.gouv.fr,
- la demande ne respecte pas les circuits d'information habituels : voie hiérarchique, circuit entreprise/ordonnateur/comptable, direction/services du réseau.
- la demande porte sur des informations habituellement confidentielles ou soumises au secret professionnel,
- la demande comprend des inexactitudes sur les grades, les fonctions habituels de vos contacts de la DGFIP.

Protocole à suivre :

1. Vérifier les coordonnées indiquées par l'interlocuteur auprès de votre comptable ou de son équipe, à partir des coordonnées officielles de vos contacts DGFIP.
2. Collecter le plus de données possibles,
3. En faire une restitution à votre comptable (première analyse de la situation et données et informations collectées), pour déterminer les suites à donner.

Direction départementale des Finances publiques de l'Hérault -

Trésorerie/Service de gestion comptable de ...

Comptable : M ou Mme XXXX xxxxx tél. : 04 xx xx xx xx / 06 xx xx xx xx / BALF du SGC/trésorerie