PRÉFET
DE LA ZONE
DE DÉFENSE
ET DE SÉCURITÉ
EST

Liberté
Égalité
Fraternité

Direction régionale de l'alimentation, de l'agriculture et de la forêt

24 juin 2020

La fraude « au faux fournisseur »
Cela pourrait aussi vous arriver…

Se faire passer pour un fournisseur pour demander à « son » client un changement de coordonnées bancaires est la fraude la plus répandue.

✓ Un exemple tiré d'un cas réel

Un directeur de coopérative agricole de la région Hauts-de-France, désignée ci-après « la coopérative », a récemment signalé avoir fait l'objet d'une tentative d'escroquerie « au faux fournisseur ». L'action s'est déroulée en **quatre temps** :

1/ La coopérative est appelée par un agent se réclamant des impôts, demandant les coordonnées des plus gros clients et les montants en vente Exo et UE au titre des déclarations de TVA de mars et avril 2020. Cette demande n'était pas inhabituelle à cette période, la coopérative rencontre assez régulièrement des difficultés à enregistrer les renseignements sur le site internet dédié ;

2/ La coopérative communique les informations demandées à l'adresse mél qui lui est donnée par l'interlocuteur ; cette adresse a pour domaine « dgfip.impot-ca3.fr » ;

3/ L'agent « des impôts » rappelle la coopérative, il lui indique alors que les douanes demandent à disposer, pour certains de ses clients, dont la société X, des 3 dernières factures émises. La coopérative transmet les informations demandées ;

4/ La société X reçoit un courrier à l'en-tête de la coopérative, l'informant d'un changement de coordonnées bancaires. Toutefois, le client s'étonne de cette situation, il relève en particulier que le compte indiqué est domicilié en Hongrie. Il appelle la coopérative.

Le directeur de la coopérative identifie ainsi la tentative de fraude. Il téléphone à ses clients pour les alerter, puis leur confirme l'alerte par mél. Trois d'entre eux, en Belgique, ont alors recontacté la coopérative en faisant état de l'appel d'une personne se réclamant de l'union des coopératives agricoles dont la coopérative est adhérente, visant à savoir s'il restait encore des factures à payer car le système informatique de l'entreprise serait momentanément indisponible. Ces clients étaient heureusement à jour de leurs factures, sinon ils auraient été invités à opérer leur règlement sur le « nouveau compte ».

✓ Que faire en cas de tentative de fraude ?

En cas de fraude ou tentative de fraude, il convient de **déposer plainte sans délai** auprès de la brigade de gendarmerie territorialement compétente ou du commissariat de police, si l'entreprise est implantée en zone de compétence police.

Le dépôt de plainte est nécessaire afin de lutter efficacement contre ce type d'escroquerie, d'en connaitre les mécanismes et de pouvoir matérialiser les liens entre les différentes affaires de nature analogue.

À l'échelon territorial, plus de 80% des PME et TPE sont implantées en zone de compétence gendarmerie. S'appuyant sur ce maillage territorial, la gendarmerie dispose de **référents sécurité économique et protection des entreprises (SECOPE)** dans chaque région et dans chaque département.

N'hésitez pas à informer directement les référents sécurité économique des tentatives de fraude dont vous seriez victime. Pour les régions Bourgogne-Franche-Comté et Grand Est respectivement, les adresses mél à utiliser sont :

- securite-economique-bourgognefranchecomte@gendarmerie.interieur.gouv.fr
- securite-economique-grandest@gendarmerie.interieur.gouv.fr

✓ Comment prévenir les fraudes ?

Pour prévenir les fraudes de cette nature, diverses précautions doivent être prises.

Il s'agit de mesures de vigilance dont l'appropriation au sein de l'entreprise (cadres, fonctions administratives, comptabilité,…) est essentielle. Notamment :

- de manière générale, veiller à ne communiquer, dans les échanges administratifs avec des interlocuteurs externes, que les éléments strictement nécessaires ; toute information liée à l'environnement de l'entreprise, ses clients, ses fournisseurs,…, pourrait aider un éventuel fraudeur à réunir des éléments préalables d'information qui lui permettront ensuite de « passer à l'attaque » (ces techniques sont dites « d'ingénierie sociale ») ;
- s'assurer de l'identité et de la qualité de la personne qui appelle, en n'hésitant pas à la questionner et à opérer des vérifications, afin d'écarter les doutes éventuels ; rester attentif aux situations inhabituelles, demandes étranges, détails troublants… ; dans le cas présent, le nom de domaine « dgfip.impot-ca3.fr », manifestement atypique pour un service de l'État, aurait dû alerter la coopérative ; la domiciliation du nouveau compte, en Hongrie, a suscité l'étonnement d'un client et a permis de déjouer la tentative ;
- en cas de demande de changement de coordonnées bancaires d'un fournisseur, mettre en place un système de double validation ; il pourra s'agir par exemple de veiller à obtenir confirmation directe de la demande en appelant le fournisseur, à l'aide des numéros de téléphone déjà connus ou identifiables dans les annuaires, sans utiliser les coordonnées présentées dans le mél ou le courrier papier.

Enfin, dans l'éventualité où, en dépit des précautions prises, vous seriez un jour victime de ce type de fraude, n'hésitez pas à contacter d'ores et déjà votre assureur afin de préciser si et dans quelles conditions elle se trouve couverte par votre contrat d'assurance.

Contact DRAAF :
Mission défense et sécurité de zone Est
Mél : jean-francois.laigre@agriculture.gouv.fr
Tél : 03 55 74 10 82