FICHE N°4 : FAUX ORDRES DE VIREMENT

Depuis 2010, **plus de 3 000 escroqueries ou tentatives d'escroqueries aux faux ordres de virement international** ont visé des sociétés implantées en France et/ou filiales domiciliées à l'étranger.
Le préjudice est d'environ **750 millions d'euros pour les faits commis** et plus de **1,8 milliard d'euros pour les faits tentés.**

Différentes techniques ont été identifiées (par ordre d'importance) :

• **le changement de Relevé d'Identité Bancaire :** de nouvelles coordonnées bancaires sont adressées par courrier électronique avec des caractéristiques de messagerie très proches de celles du fournisseur et/ou de l'interlocuteur habituel ;

• **l'usage d'une fausse identité :** par usurpation de l'identité du dirigeant ou d'un responsable de la société ciblée ou d'une personnalité (de type faux président ou faux ministre) ;

• **via un lien frauduleux :** un lien contenant un logiciel espion invite à se connecter sur le portail de la banque gestionnaire des comptes et à composer les identifiants et codes d'accès. De faux ordres de virement sont alors établis, les mots de passe modifiés, privant les services comptables de toute vérification de leur trésorerie.

En cette période de crise, des groupes criminels organisés en profitent pour usurper l'identité de sociétés produisant et/ou distribuant du matériel de protection et/ou médical. Ils ciblent des établissements et les incitent à réaliser des commandes et des paiements sur des comptes bancaires français ou étrangers.
Les procédures habituelles de lutte contre les fraudes financières, et notamment celles relatives au changement de domiciliation bancaire, sont désorganisés.

De nombreuses escroqueries en lien avec la crise visent des pharmacies, des hôpitaux, des cliniques, des EHPAD et des fournisseurs de matériel de protection médicale.

MESSAGE DE PRÉVENTION

1- Méfiez-vous de toute proposition commerciale prétendument « urgente ».

2- Ne communiquez pas d'informations susceptibles de faciliter le travail des escrocs (noms des différents managers, chefs de division, moyens de règlement, listing fournisseurs¼).

3- Sensibilisez l'ensemble du personnel et les partenaires (exemples : affiches de sensibilisation, E-learning mis à disposition sur le site du Club des directeurs de sûreté et de sécurité des entreprises – CDSE (https://www.cdse.edu/catalog/elearning/index.html)

4- Réalisez une veille régulière sur les évolutions des escroqueries.

5- Prenez le temps de vérifier, même dans l'urgence et sous la pression, les demandes de virement.
Les contre-mesures les plus simples :
• contre-appel avec le numéro habituel connu en interne et non celui fourni par l'escroc,
• vérification auprès du site internet de la société si elle signale avoir été victime d'une escroquerie.

6- Sécurisez les installations informatiques.

7- Veillez à la sécurité des accès aux services de banque à distance.

/!\ Un établissement bancaire ne sollicite jamais les informations de connexion de ses clients.

Les mots de passe doivent être confidentiels, complexes et régulièrement renouvelés.

RECOMMANDATIONS, EN CAS D'ATTAQUE :

→ prendre attache immédiatement avec votre banque pour effectuer un rappel des fonds, la rapidité de la réaction est primordiale ;

→ contacter le service de police ou de gendarmerie le plus proche en apportant un maximum d'éléments (entête de mails et contenus, numéros de téléphone, dates et heures des appels, éléments confidentiels communiqués aux fraudeurs...).