# Prévention des escroqueries aux faux ordres de virements internationaux (FOVI)

Depuis ces trois dernières années, plusieurs centaines d'escroqueries ou tentatives d'escroqueries aux faux ordres de virements internationaux visent des sociétés implantées en France et/ou filiales domiciliées sur l'Union Européenne. Ces escroqueries ont généré un préjudice global d'environ 300 millions d'Euros pour les faits commis et 500 millions pour les faits tentés.

Réalisée par téléphone et/ou par mail, l'escroquerie concerne les sociétés quelles que soient leurs tailles. Souvent situés à l'étranger, les escrocs collectent un maximum de renseignements sur l'entreprise (ingénierie sociale sur internet) avant de lancer leur opération sur les personnes capables d'opérer ces virements. Les auteurs prétextent une opération d'importance capitale et confidentielle, afin d'abuser l'interlocuteur et obtenir un ou plusieurs virements internationaux.

**Les variantes d'escroqueries** : ces modes opératoires ne sont pas exhaustifs. Les escrocs les renouvellent régulièrement.

**L'escroquerie « au faux président »** :
L'escroc se fait passer pour un des dirigeants de la société, avec la complicité d'un soit disant cabinet d'avocats ou de notaires, dans le but d'effectuer un virement confidentiel vers l'étranger.

**L'escroquerie « au changement de Relevé d'Identité Bancaire »** : **Fausses factures – Au bail locatif**
L'escroc, prétextant être un représentant du bailleur, ou l'un des fournisseurs, indique un changement de coordonnées bancaires et demande la réalisation du virement vers un autre pays. Dans le cadre des loyers (souvent trimestriel), l'escroc prétexte une délocalisation de la comptabilité à l'étranger.

**L'escroquerie « au virement SEPA, à l'informatique »** :
L'escroc, se faisant passer pour un technicien, demande une communication d'informations confidentielles (identifiant et mot de passe) afin d'effectuer des virements tests. L'escroc peut également adresser par mail un message comportant une pièce jointe, en donnant comme instructions l'installation du logiciel lui permettant alors de prendre le contrôle de l'ordinateur et récupérer des informations à l'insu de son correspondant.

Pour s'en prémunir, il suffit de mettre en œuvre des mesures simples de sécurité pour décourager les escrocs.

## A) La prévention :

1°) Ne pas communiquer d'informations susceptibles de faciliter le travail des escrocs :
- Noms des différents managers, chefs de division, des personnes en charge des paiements fournisseurs,
- Les techniques de règlement (chèques, virements, prélèvements,etc...), les noms des applications employées dans les processus de règlement, les codes d'exécution des virements !
- Le listing des fournisseurs.

2°) Sensibiliser le personnel susceptible d'être contacté par les escrocs :
Le service comptabilité, les fournisseurs, la trésorerie, les secrétaires et standardistes.

3°) Sensibiliser les partenaires :
La banque, le cabinet d'avocats de la société, les fournisseurs.

4°) Effectuer une veille sur les évolutions des escroqueries par la presse, les communications des pouvoirs publics, les fédérations, les associations professionnelles.

5°) Faire preuve de bon sens :
Demande inhabituelle, illogique, différente des procédures définies par la société.

**B) Les signes d'une attaque :**

Un virement à l'international non planifié est demandé par un membre du conseil d'administration, le dirigeant, l'un de ses adjoints, avec l'aide d'un cabinet d'avocats, sous la surveillance de l'Autorité des Marchés Financiers, par l'un « des fournisseurs » prétextant un changement de coordonnées bancaires.
Cette demande peut revêtir un caractère urgent et confidentiel. L'escroc fera usage de flatterie ou de menace dans le but de manipuler son interlocuteur.
Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise et son environnement : données personnelles concernant le chef de l'entreprise, ses collaborateurs, les banques, etc...

**C) Se prémunir de cette attaque :**

Résister aux tentatives d'intimidation et à la pression psychologique.
En cas de doute, prendre attache directement avec la personne au sein de la société soit physiquement soit avec les coordonnées connues de l'entreprise.
Se méfier de tout changement de coordonnées téléphoniques ou mails : la communication d'un nouveau numéro à l'indicatif français n'est pas une garantie, tout comme une adresse mail hébergée par un opérateur généraliste. Dans ce dernier cas, l'affichage complet de l'entête du mail permettra d'identifier le réel émetteur.
Dans ce cas, il faut contacter son interlocuteur habituel avec les coordonnées connues de la société.

**D) Exécution du virement :**
Effectuer en urgence un compte rendu de l'événement à la hiérarchie.
Demander immédiatement à la banque le retour des fonds.
Déposer plainte en apportant un maximum d'éléments (entête de mails et leurs contenus, numéros de téléphone utilisés par les escrocs, dates et heures des appels, les éléments confidentiels communiqués aux escroc, etc...)