



## MESSAGE D'ATTENTION

Merci beaucoup !!!

### **RECRUESCENCE DES ESCROQUERIES AUX FAUX ORDRES DE VIREMENTS INTERNATIONAUX**



### DE QUOI PARLE T-ON ?

Depuis 2005, plusieurs milliers d'entreprises ont été victimes de tentatives ou d'escroqueries avérées aux faux ordres de virement pour un montant total supérieur à 700 millions d'Euros. Ces chiffres ne prennent en compte que les faits suivis d'une plainte, nombre de victimes ne les dénonçant pas de peur d'altérer l'image de leurs sociétés.

En ce début d'année, ce type d'atteinte est en pleine recrudescence ; et les entreprises rhônalpines ne sont pas épargnées.

L'escroquerie au faux ordre de virement bancaire, réalisée par courriel ou par téléphone, est une menace permanente pesant sur toute entreprise et ce, quelle que soit sa taille ou son secteur d'activité.

Opérant souvent depuis l'étranger, bien organisés et informés, jouant sur l'usurpation d'identité, très habiles dans l'art de manier certains ressorts psychologiques, les escrocs abusent leurs victimes sans exercer de violence.

Risques très faibles d'être appréhendés, profits pharaoniques, absence totale de scrupules quant aux conséquences de leurs actes, le tout pour un investissement « temps/moyens » limité, sont autant d'arguments pouvant expliquer leurs motivations.

Souvent très conséquentes, les sommes extorquées peuvent dangereusement fragiliser la santé financière des entreprises.

Dans un contexte économique déjà tendu, les dirigeants ne peuvent se permettre de rester totalement passifs car il en va de la sauvegarde de leurs établissements.

### QUELQUES CONSEILS POUR SE PRÉMUNIR :

- Vérifier l'existence et l'application de procédures internes concernant les virements.
- Sensibiliser régulièrement les équipes financières et comptables ainsi que tout salarié exerçant une fonction « filtre » (*secrétaire, assistante de direction, standardiste,...*). Ces personnels sont susceptibles d'être contactés par l'escroc lors de la phase préparatoire de recueil d'informations.
- Les former au bon usage des moyens informatiques mis à leur disposition, aux dangers des réseaux sociaux ainsi qu'à la protection de l'information. Les responsabiliser par la mise en place de chartes.
- Ne pas rendre public l'organigramme de l'entreprise pour ne pas faciliter la collecte d'informations de l'escroc. Filtrer les renseignements mis en ligne sur votre ou vos sites internet.
- Inviter l'ensemble des salariés à faire rapidement remonter à la hiérarchie tout fait « anormal ».
- Lorsqu'une demande de virement est faite hors du formalisme habituel, exiger une sollicitation écrite provenant d'une adresse mail professionnelle (*et non personnelle*), ainsi qu'un numéro de téléphone fixe (*et non portable*). Vérifier systématiquement les coordonnées recueillies.
- Orienter l'interlocuteur vers la procédure régulière, et ne rien entreprendre sans l'aval de la hiérarchie.
- Veiller à contacter l'établissement bancaire pour vérifier les dires de l'appelant.
- Ne communiquer aucun code confidentiel par téléphone, fax ou courriel.
- Si une tentative de fraude venait à être détectée, tenter de retourner la situation à son avantage en collectant un maximum de renseignements sur l'appelant.
- Bannir toute initiative malheureuse pouvant mettre l'entreprise en péril !!!
- Pour sensibiliser dirigeants, cadres et salariés, la Fédération Bancaire Française (FBF) a publié le guide :

**Ordres de virement : 9 réflexes sécurité**



**En cas de problème avéré ou de simple tentative : Déposer rapidement plainte auprès du service de police ou de gendarmerie territorialement compétent.**

