EN RÉSUMÉ

En matière d'escroquerie, il n'existe pas de fatalité. La prévention de ce type d'atteinte passe essentiellement par le *bon sens des personnes ciblées* et *l'application stricte des procédures édictées en interne*.

La confiance a ses *limites*. Dès lors que d'importantes sommes d'argent sont en jeu, on ne pourra jamais reprocher à quiconque d'avoir pris des précautions en procédant aux vérifications d'usage.

***A retenir* :**

les notions de « *discrétion* » et « *d'urgence* » demandées doivent *immédiatement* éveiller vos soupçons !!!

EN CAS DE PROBLÈME

- **Déposez *rapidement* plainte à la gendarmerie ou au commissariat dont vous dépendez.**
- **Munissez-vous de tous les renseignements en votre possession :**
  - **Références du ou des transferts d'argent effectués,**
  - **Références de la ou des personnes contactées (adresse de messagerie ou postale, pseudos utilisés, numéros de téléphone, fax, copie de courriels) ;**
  - **Tout autre renseignement pouvant permettre d'identifier l'escroc.**

Ne pas déposer plainte de peur d'altérer l'image de l'entreprise, permet aux escrocs de poursuivre leurs activités délictuelles en toute impunité !!!

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFECTURE DE LA RÉGION RHONE-ALPES

DIRECTION CENTRALE DU RENSEIGNEMENT INTERIEUR
DCRI

Gendarmerie nationale

dpso

DIRECCTE Rhône-Alpes
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

Plaquette rédigée par le Comité Régional de Sécurité Économique de la Région Rhône-Alpes.
Document édité à 100 000 exemplaires par le service de diffusion de la Gendarmerie de Limoges

Sécurité économique territoriale
Rhône-Alpes

€scroquerie au faux ordre de virement : Comment s'en prémunir ?

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 professionnels de l'escroquerie financière abusent leurs victimes sans exercer de violence.

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

Toutefois, 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.

Les quelques recommandations ci-après ont pour but de limiter les risques.

Avec un rapport risques/profits toujours à leur avantage, les escrocs vous observent, testent votre niveau de sécurité et s'engouffrent dans toute faille identifiée.

CE QUE DIT LA LOI ?

Délit puni de *5 ans d'emprisonnement* et de *375 000 € d'amende*, l'escroquerie est le fait de tromper une personne physique ou morale afin de l'inciter à remettre des fonds, des valeurs, des services ou un bien quelconque. (*article 313-1 du Code pénal*)

Elle est fréquemment réalisée par un ou des individus faisant état d'un faux nom ou d'une fausse qualité (*identités connues des victimes ou professions inspirant la confiance telles que celles de dirigeant d'entreprise, de client, de fournisseur, ...*) ;

Cette infraction est prescrite dans le délai de *3 ans* à compter de la date de la remise de la chose ou du dernier versement d'argent. *La tentative d'escroquerie est sanctionnée des mêmes peines.*

QUELS SIGNES DOIVENT VOUS ALERTER ?

Pour mieux ferrer sa proie, l'escroc prend toutes sortes de renseignements sur elle, ainsi que sur l'entreprise et son fonctionnement (organigramme, activité, partenaires...), notamment par le biais des réseaux sociaux et des différentes parutions publiées en sources ouvertes (*ingénierie sociale*).

Toutefois, nombre d'escroqueries financières ont dans bien des cas des *dénominateurs communs* permettant de les détecter :

Fréquemment commises les veilles de week-ends, surtout lorsqu'ils sont suivis ou précédés de jours fériés (délai permettant d'éviter la découverte rapide du méfait).

Usurpation d'identité d'un responsable de l'entreprise, de clients importants ou de personnels ayant un poste clé de façon à intimider ou mettre en confiance.

Caractère d'urgence signalé et totale discrétion demandée sous un quelconque prétexte pour que la « *victime* » n'ait le temps de vérifier le bien-fondé de la sollicitation.

Aucune coordonnée vérifiable communiquée par l'escroc, celui-ci prétextant dans bien des cas être en déplacement et ne pouvoir être contacté autrement que par téléphone portable.

Demande de virement souvent faite au profit de banques situées hors Union Européenne de manière à compliquer au maximum la tâche des enquêteurs.

COMMENT S'EN PRÉMUNIR ?

En amont :

- *Vérifier* l'existence de procédures internes concernant les virements et surtout qu'elles sont connues et appliquées.
- *Sensibiliser* régulièrement les équipes financières et comptables ainsi que tout salarié exerçant une fonction de «*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* ».

Rehausser le niveau de vigilance, sans toutefois verser dans la paranoïa !!!

Durant la phase « *contact* » :

- 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.*
- *Ne communiquer aucun code confidentiel* par téléphone ou par courriel.
- Si une tentative de fraude venait à être détectée durant la phase « *contact* », tenter de retourner la situation à son avantage en collectant un maximum de renseignements sur l'appelant.

Bannir toute initiative malheureuse pour ne pas mettre l'entreprise en péril !!!