

Les BONNES PRATIQUES



Définir et respecter une procédure interne pour l'exécution des virements

Identité des personnes habilitées, montants autorisés, double signature pour les virements internationaux... Cette procédure doit être formalisée dans un document accessible par les seuls collaborateurs concernés.



Prendre le temps d'effectuer des vérifications (ex : contre-appel)

Il est nécessaire de prendre le temps d'effectuer des vérifications, spécialement quand l'opération demandée semble inhabituelle ! Rappeler votre interlocuteur en vérifiant la légitimité du numéro de téléphone dans votre carnet de contact.



Sensibiliser vos collaborateurs au risque d'escroquerie

La sécurité est l'affaire de tous ! Tous les collaborateurs doivent donc être sensibilisés aux risques d'escroquerie, spécialement les services comptables et financiers.



Maîtriser la diffusion des informations concernant l'entreprise

Il faut être vigilant quant aux informations divulguées concernant l'entreprise et ses dirigeants (réseaux sociaux, sites Internet...).



Contactez immédiatement la banque et la police judiciaire en cas d'escroquerie (ou de tentative)

C'est l'action la plus importante en cas de fraude avérée. Les délais pour une possible intervention sont très courts, il faut donc agir rapidement !

POUR PLUS D'INFORMATIONS

consultez le guide de sécurité bancaire
« **Ordres de virement des entreprises** »
élaboré par la Fédération Bancaire Française
et la Police Judiciaire sur
www.lesclesdelabanque.com

POUR TOUT RENSEIGNEMENT **256 990**



Groupe BRED

ENSEMBLE, VOIR PLUS LOIN

Banque Calédonienne d'Investissement • SAEM au capital de 15 milliards F CFP
Siège social : 54, avenue de la Victoire - BP K5 - 98849 Nouméa Cedex • Tél. (+687) 25 65 65 - Fax (+687) 25 65 57
RCS Nouméa 15479 - Ridet n° 0 015 479 001 - RIAS NC170007 voir rias.nc

FRAUDES aux FAUX ORDRES DE VIREMENT

Les bonnes
pratiques pour
s'en prémunir...

+ d'info au **256 990**
coût d'un appel local

► www.bci.nc



Groupe BRED

ENSEMBLE, VOIR PLUS LOIN

FRAUDES aux FAUX ORDRES DE VIREMENT

En 2016, pas moins de **250 millions FCFP** de virements frauduleux ont été recensés en Nouvelle-Calédonie !

L'escroquerie aux faux ordres de virement consiste à obtenir d'un collaborateur de l'entreprise l'exécution d'un ordre de virement, pour un motif apparemment valable, et ce au bénéfice d'un escroc.

Ce type de fraude a souvent des **impacts conséquents** sur l'entreprise, pouvant aller jusqu'à la liquidation judiciaire !

Il en existe plusieurs variantes, dont les plus répandues sont la **fraude au faux président** et la **fraude au faux fournisseur**.

■ ATTENTION

La période de pandémie est propice aux arnaques aux faux ordres de virement.

- Une société pharmaceutique de Rouen a été victime d'une fraude aux faux fournisseurs d'un montant de 6,6 millions d'euros.
- De nombreux faux sites Internet de société produisant du gel hydroalcoolique ou des masques sont apparus sur les toiles au cours des derniers mois.
- De nombreuses campagnes de phishing sont actuellement en cours.

■ LA FRAUDE AU FAUX PRÉSIDENT

Un escroc se fait passer pour un dirigeant de l'entreprise en se servant d'informations recueillies sur la société et sa direction. Il obtient alors d'un collaborateur de l'entreprise d'effectuer un virement important à un tiers, le plus souvent domicilié à l'étranger (dette à régler, provision de contrat...) en insistant sur le caractère urgent et confidentiel de l'opération. Afin d'accentuer la pression sur le salarié, les faux emails peuvent être accompagnés de coups de téléphone de faux avocats pour légitimer l'opération.

■ LA FRAUDE AU FAUX FOURNISSEUR

Un escroc se fait passer pour un fournisseur ou tout autre créancier légitime de l'entreprise, le plus souvent par usurpation d'adresse mail, et prétexte un changement de RIB (ex : changement de banque) pour diriger les virements futurs vers un autre compte bancaire. La demande se fait le plus souvent par email ou courrier en bonne et due forme (en-tête du courrier, adresse de messagerie...).



RESTEZ VIGILANTS !

notamment en télétravail !

- Un contact ou une demande inhabituels doivent **éveiller vos soupçons**.
- Quelle que soit la taille de votre entreprise**, vous pouvez être la cible de ce type de fraude.
- Ces escroqueries se font aussi bien par **téléphone**, par **mail**, que par **courrier**.
- Les **services comptables et financiers** sont les premiers concernés par ce type de fraude.
- Les postes de **secrétaire, standardiste, ou assistant de direction** sont susceptibles d'être contactés au préalable par l'escroc pour recueillir des informations.
- Les fraudeurs sont souvent **très bien renseignés** sur l'entreprise, ce qui accentue d'autant plus leur crédibilité.
- Accentuez la vigilance en veille de **jours fériés**, de **week-ends** ou de **congés scolaires**.
- L'usurpation d'identité d'un dirigeant, de clients ou de fournisseurs importants permet d'**intimider** ou de **mettre en confiance** le collaborateur.