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 comportant des consignes claires, 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. Il est très important de former vos équipes à détecter et mettre en échec les tentatives de fraudes. Formez spécialement les services comptables et financiers mais sensibilisez tous vos collaborateurs et n'oubliez pas les nouveaux arrivants. Renouvelez vos sessions de sensibilisation régulièrement.

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…).

Contacter immédiatement votre hiérarchie, 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 !

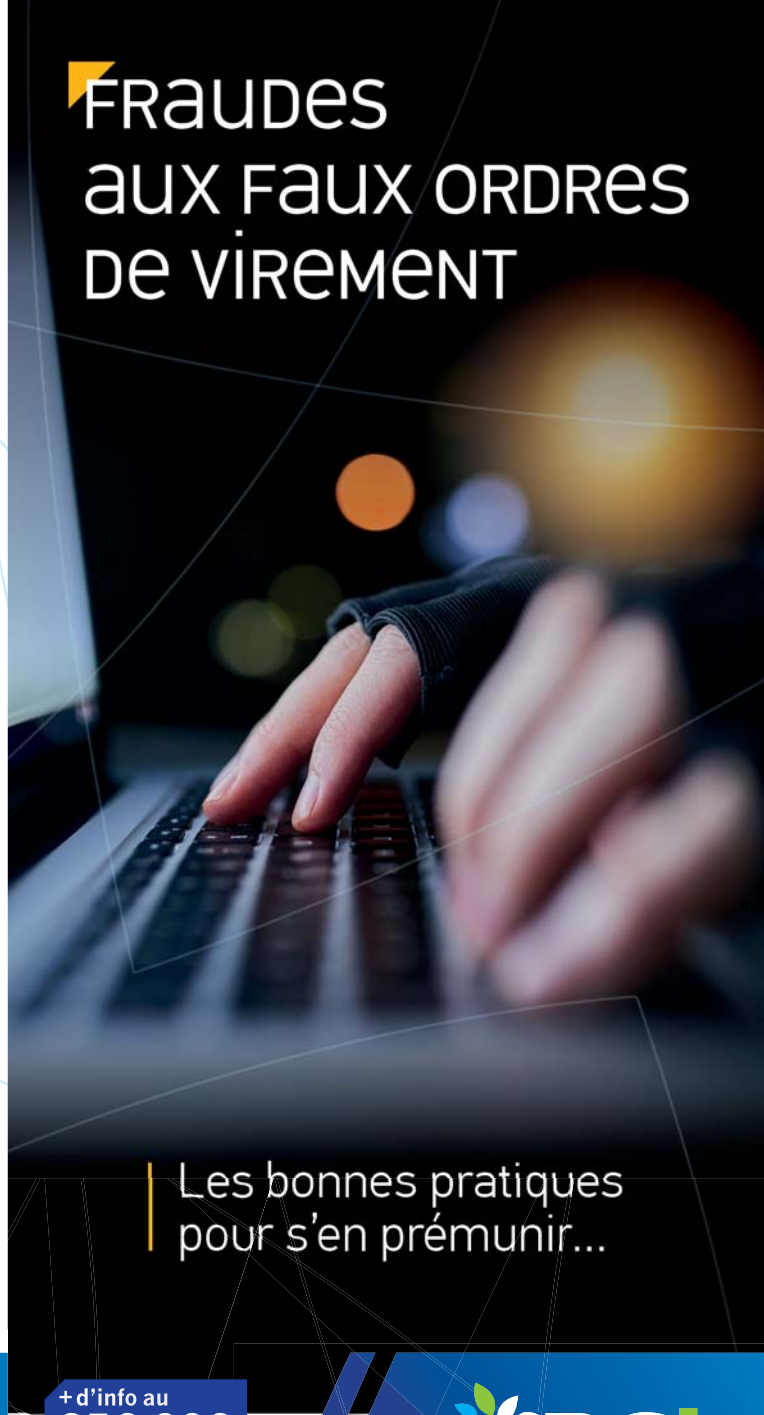
POUR PLUS D'INFORMATIONS

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

+ d'info au 256 990

eudania : 23 74 54 Édition 03/2024

Fraudes aux faux ordres de virement



Les bonnes pratiques pour s'en prémunir…

+ d'info au 256 990

www.bci.nc

BCI Groupe BRED
ENSEMBLE, VOIR PLUS LOIN

Fraudes aux faux ordres de virement

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**.

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, contrat à honorer…) en insistant sur le caractère urgent (contrôle fiscal, etc.) et confidentiel de l'opération (« surtout n'en parlez pas, ce dossier est hautement confidentiel »). 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. Les fraudeurs utilisent la flatterie (« on m'a dit que je peux compter sur vous ») ou l'intimidation pour parvenir à leur fins.

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…).

ATTENTION

Les fraudeurs utilisent des services d'appels dématérialisés et simulent des numéros de téléphone locaux. Ils utilisent des **techniques de « phone spoofing »** pour afficher de faux noms et numéros de téléphone. Ils utilisent également de faux comptes WhatsApp avec les photos de dirigeants.

Les fraudeurs connaissent souvent parfaitement l'entreprise et savent **contrefaire les voix (« deepfake »)**.

Les fraudeurs utilisent souvent des adresses email qui ressemblent à celle de la personne dont ils usurpent l'identité : c'est le **« spoofing » d'email**, dont voici quelques exemples :

Utilisation d'un tiret ('-') : ceo@amazon-corp.com

- Utilisation de caractères holographiques : remplacer '0' par '0', 'l''(L minuscule) par 'i' capital, 'I' ou 'L' par '1', etc.
- Domaine avec une faute : ceo@anazon.com
- Domaine avec une extension peu courante : ceo@amazon.top

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.