



www.lesclesdelabanque.com

Le site pédagogique sur la banque et l'argent

ORDRES DE VIREMENT DES ENTREPRISES

9 RÉFLEXES SÉCURITÉ



CE GUIDE VOUS EST OFFERT PAR

**Pour toute information complémentaire,
nous contacter : info@lesclesdelabanque.com**

Le présent guide est exclusivement diffusé à des fins d'information du public. Il ne saurait en aucun cas constituer une quelconque interprétation de nature juridique de la part des auteurs et/ou de l'éditeur. Tous droits réservés. La reproduction totale ou partielle des textes de ce guide est soumise à l'autorisation préalable de la Fédération Bancaire Française.

Éditeur : FBF - 18 rue La Fayette 75009 Paris - Association Loi 1901
Directeur de publication : Maya Atig
Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : novembre 2021

SOMMAIRE

1. Respecter une procédure interne pour l'exécution des virements	6
2. Sensibiliser les collaborateurs au risque de fraude lors d'opérations de paiement	8
3. Être en veille sur les escroqueries aux entreprises	10
4. Maîtriser la diffusion des informations concernant l'entreprise	12
5. Faire preuve de bon sens	14
6. Prendre le temps d'effectuer des vérifications	16
7. Veiller à la sécurité des accès aux services de banque à distance	18
8. Sécuriser les installations informatiques	20
9. Contacter immédiatement la banque et la police judiciaire en cas d'escroquerie (ou de tentative)	22
LES RÉFLEXES SÉCURITÉ	25

Introduction

**SI VOUS ÊTES VICTIME
D'UNE FRAUDE
(OU D'UNE TENTATIVE
DE FRAUDE), VOTRE RAPIDITÉ
POUR CONTACTER
VOTRE BANQUE
ET LA POLICE JUDICIAIRE
EST ESSENTIELLE.**

En 2020, près de 900 fraudes aux ordres de virements ont été recensées, avec un préjudice de plus de 120 millions d'euros pour les entreprises et les services publics.

Les conséquences sont souvent désastreuses : perte de tout ou partie de la trésorerie et parfois même liquidation de l'entreprise.

Quelle que soit la taille de votre entreprise, y compris les TPE/PME, vous pouvez être la cible d'escrocs. **Ce guide vous présente quelques réflexes simples pour prévenir ces attaques, déjouer les tentatives de fraude et savoir comment réagir** aux ordres de virement frauduleux.

Une fois un ordre de virement (transfert de compte à compte) émis dans le système bancaire, il ne peut plus être annulé : un virement est en effet irrévocable.

Les tentatives d'escroqueries consistent ainsi à obtenir d'un collaborateur de l'entreprise l'exécution d'un ordre de virement, pour un motif apparemment valable, au bénéfice d'un escroc.

Voici les variantes les plus récentes (cette liste n'est pas exhaustive) :

- **L'escroquerie au « faux président »**

Un escroc se fait passer pour un des dirigeants de l'entreprise auprès d'un collaborateur pour obtenir de lui un virement urgent et confidentiel sur un compte, souvent domicilié à l'étranger. Pour cela, l'escroc se sert d'informations sur la société et ses dirigeants, préalablement recueillies sur Internet ou auprès de services de l'entreprise lors d'appels précédents afin de crédibiliser leur opération d'escroquerie.

- **L'escroquerie à l'usurpation d'identité**

Cette variante de l'escroquerie au « faux président » consiste à usurper l'identité d'une personnalité ou autorité (commissaire aux comptes, banquier, fonctionnaire de police ou du renseignement intérieur voire un ministre...) pour obtenir également l'exécution d'un virement par le dirigeant ou un collaborateur de l'entreprise.

- **L'escroquerie aux coordonnées bancaires**

Un escroc fait croire à un changement de domiciliation bancaire du bailleur (nouveau RIB donc nouvel IBAN), d'un fournisseur/prestataire de services ou de tout autre créancier de l'entreprise pour les prochains règlements de loyers ou de factures. Le motif peut sembler normal dans l'activité d'une entreprise : regroupement de gestion au niveau du groupe, changement de banque. L'escroc envoie alors les nouvelles coordonnées bancaires et une facture par courrier électronique ou postal avec des caractéristiques très proches de celles de l'interlocuteur habituel (adresse de messagerie, en-tête de courrier...).

- **Le piratage de la boîte mail de l'entreprise**

Un pirate peut avoir récupéré vos accès à votre boîte mail. Il peut alors intercepter un message reçu ou envoyé :

- 1^{er} cas : si un créancier vous envoie un nouveau RIB, l'escroc peut le remplacer par le sien en vous renvoyant un autre mail.
- 2^{ème} cas : vous envoyez votre nouveau RIB, l'escroc intercepte le message et remplace le RIB par le sien dans un nouveau mail.

À chaque nouveau RIB reçu ou envoyé par mail, et avant tout virement, appelez votre interlocuteur aux coordonnées habituelles pour vérifier que c'est le bon IBAN.

D'une manière générale, sécurisez votre boîte mail pour éviter qu'un pirate n'intercepte un message reçu ou envoyé.

Vous avez effectué un virement qui n'est pas parvenu à son destinataire ? Vous constatez qu'un paiement qui vous a été envoyé ne vous parvient pas ? Vérifiez si votre messagerie professionnelle n'a pas été piratée et suspendez tout paiement le temps de cette vérification.

- **L'escroquerie à l'informatique**

L'escroc se fait passer pour un personnel du service technique de la banque de l'entreprise visée et tente d'obtenir l'exécution de « virements tests » par le collaborateur. Il peut aussi se faire passer pour un technicien prestataire informatique de l'entreprise et demander l'installation de logiciels qui permettront de récupérer des informations de sécurité ou de pirater le système informatique de l'entreprise.



ATTENTION

Les escrocs renouvellent leurs modes opératoires régulièrement. Ils continuent leurs tentatives en cas d'échec comme en cas de succès, en utilisant d'autres méthodes si nécessaire.

1

Respecter une procédure interne pour l'exécution des virements

Une procédure écrite d'exécution des virements au sein de votre entreprise **doit être clairement définie**.

Elle précise notamment :

- l'identité des personnes habilitées à effectuer des virements,
- les montants autorisés, par personne habilitée, pour la France ou pour l'international,
- les plafonds périodiques d'opérations et les zones géographiques d'habilitation,
- le circuit de validation des opérations (prévoir au moins 2 personnes),
- les procédures applicables en cas d'urgence ou d'opérations « inhabituelles ».

Les personnes habilitées à effectuer un virement doivent être formées sur la procédure définie.

Le respect de cette procédure doit être contrôlé régulièrement.



Cette procédure doit être formalisée dans un document auquel les collaborateurs concernés, et eux seuls, pourront se référer.

2

Sensibiliser les collaborateurs au risque de fraude lors d'opérations de paiement

La sécurité est l'affaire de chacun au sein de l'entreprise. Tous les collaborateurs, quelles que soient leurs fonctions, doivent être conscients que leur entreprise peut à tout moment être la cible de tentatives d'escroquerie. Comment aborder le sujet ?

Vous pouvez :

- **communiquer sur l'importance du respect de la procédure** d'exécution des virements, **les points de contrôle à effectuer** (par exemple distinguer le BIC/IBAN d'un compte domicilié en France de celui d'un compte domicilié à l'étranger), **les opérations que chacun est habilité à effectuer**,
- **présenter des exemples** d'escroquerie ou des tentatives d'escroquerie (communiqués par vos réseaux : fédérations professionnelles... ou recherchés dans les médias),
- **appeler à une plus grande vigilance** face aux demandes extérieures notamment sur l'organigramme de l'entreprise, le nom des responsables, les procédures de paiement et face aux courriers reçus avec une orthographe fantaisiste ou une adresse électronique avec un nom de domaine inhabituel, etc.

3

Être en veille sur les escroqueries aux entreprises

Les formes d'escroqueries évoluent régulièrement.

Les escrocs adaptent leurs méthodes en fonction de leurs expériences et profitent de l'actualité économique et financière pour tromper la vigilance des entreprises.



N'hésitez pas à informer vos collaborateurs des récentes escroqueries dévoilées.

Pour maintenir une vigilance efficace, suivez les informations récentes sur les fraudes grâce à la presse, aux communications des pouvoirs publics et des associations professionnelles.



À SAVOIR

Les événements tels que le FIC (Forum International de la Cybersécurité), ceux organisés par les Chambres de Commerce ou le site de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) ainsi que le mois européen de la Cybercriminalité (octobre) sont autant d'occasions pour sensibiliser et former toute l'entreprise.

4

Maîtriser la diffusion des informations concernant l'entreprise

Les escrocs utilisent des informations extraites du Registre du Commerce et des Sociétés, des procès-verbaux d'assemblée générale ou celles qui figurent sur votre site Internet, dans la presse... pour se faire passer pour un dirigeant ou un partenaire de l'entreprise.

Votre entreprise ne doit pas diffuser des informations qui risqueraient de mettre en péril la confidentialité de ses activités et procédures. Attention notamment à ne pas divulguer les noms et fonctions des personnes habilitées à réaliser des virements.



EXEMPLE

La publication d'un organigramme trop détaillé, notamment sur votre site ou dans des annuaires locaux ou professionnels, est une source d'informations pour des escrocs. Ces derniers peuvent également effectuer des appels téléphoniques, a priori anodins, pour vérifier les fonctions de certains collaborateurs.

5

Faire preuve de bon sens

Le but des escrocs est généralement de convaincre leur cible d'effectuer une opération de virement, souvent en urgence et en secret, et ce malgré les habitudes ou la logique. **Il faut s'interroger notamment en cas de :**

- **changement de domiciliation bancaire** d'un bailleur ou d'un fournisseur. Cette opération est évidemment possible et normale dans l'activité d'une entreprise, mais habituellement elle doit avoir été minutieusement préparée et le changement de coordonnées bancaires est souvent annoncé en amont du règlement,
- nouvelle domiciliation bancaire **en France, comme à l'étranger** d'un fournisseur/bailleur/client, même en zone SEPA. Des vérifications s'imposent,
- **demande** d'un dirigeant de l'entreprise **de déroger aux procédures définies** dans la plus grande discrétion. La hiérarchie doit être informée.



Il est important de déceler les tentatives d'intimidation, de pression psychologique... L'empathie et la flatterie sont souvent utilisées par les escrocs.

6

Prendre le temps d'effectuer des vérifications

Les escrocs invoquent souvent un caractère d'urgence à leur demande de virement qu'ils présentent d'ailleurs régulièrement la veille de week-ends ou de jours fériés pour réduire les contrôles possibles. Il est nécessaire de prendre le temps d'effectuer des vérifications, surtout quand l'opération demandée est inhabituelle.

Cette vérification doit **par exemple** prendre la forme :

- d'**un contre-appel** auprès du partenaire commercial ou financier en évitant le numéro indiqué dans le message ou le courrier reçu et en utilisant les coordonnées « connues » figurant dans vos fichiers internes,
- d'**une consultation de factures antérieures** en cas de « rappel pour impayé »,
- d'**une demande de renseignement auprès de sa hiérarchie et de ses collègues.**



ATTENTION

Toute opération prétendument urgente et/ou confidentielle doit être systématiquement présentée au responsable hiérarchique désigné dans la procédure.

7

Veiller à la sécurité des accès aux services de banque à distance

Les codes d'accès au service de banque à distance de l'entreprise **doivent être uniquement connus des personnes habilitées** à s'y connecter. Ils doivent rester strictement confidentiels et ne pas être reportés sur un document ou communiqués à qui que ce soit. Ils permettent une traçabilité des consultations et transactions effectuées.

Les mots de passe doivent être suffisamment complexes et régulièrement modifiés. Par exemple, une date de naissance ne constitue pas un code efficace car elle peut être obtenue au moyen de documents facilement accessibles (ex : k-bis) ou via des recherches sur Internet.



À NOTER

Votre établissement bancaire ne vous demandera jamais de lui communiquer les informations permettant la connexion à votre espace de banque à distance.

8

Sécuriser les installations informatiques

Afin de limiter le risque d'infection et de piratage informatique (par des logiciels espions ou des programmes malveillants), **l'installation de logiciels doit être strictement encadrée et vos postes informatiques doivent posséder un système antivirus régulièrement mis à jour.**

Une charte informatique est recommandée. Elle précise les conditions d'utilisation du matériel informatique de l'entreprise et s'applique à l'ensemble des collaborateurs.



EXEMPLE

Ne pas ouvrir ni conserver les pièces jointes des messages d'expéditeurs inconnus ou dont l'adresse email est différente de l'adresse habituelle car elles représentent un risque potentiel.

9

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

Contacter la banque et la police est l'action la plus importante en cas de fraude avérée.

La banque doit être contactée le plus rapidement possible. Elle **examinera** avec vous **les possibilités de récupérer les fonds** dans le cadre de relations interbancaires, en sachant qu'un ordre de virement est irrévocable.



ATTENTION

Les délais pour une possible intervention sont extrêmement courts. Une réaction rapide est donc essentielle.

En cas de tentative d'escroquerie, vous demanderez à modifier vos codes d'accès aux services de banque à distance.

La direction zonale ou territoriale de la police judiciaire et, en son sein la division de lutte contre la criminalité financière, **doivent être contactés en parallèle** afin de mener les actions de police (enquêtes, relations avec les services d'autres pays...) possibles dans un délai très court.

Une plainte doit être déposée avec un maximum d'éléments constitutifs de l'escroquerie apportés en appui : courriers électroniques, fax, enregistrements de conversation, numéros de téléphone des correspondants....



Au sein de la Police Judiciaire, l'Office Central pour la Répression de la Grande Délinquance Financière (OCRGDF) est notamment en charge de la lutte contre les escroqueries nationales ou internationales.



ORDRES DE VIREMENT DES ENTREPRISES **LES RÉFLEXES SÉCURITÉ**

1. Respecter une procédure interne pour l'exécution des virements
2. Sensibiliser les collaborateurs au risque de fraude lors d'opérations de paiement
3. Être en veille sur les escroqueries aux entreprises
4. Maîtriser la diffusion des informations concernant votre entreprise
5. Faire preuve de bon sens
6. Prendre le temps d'effectuer des vérifications
7. Veiller à la sécurité des accès aux services de banque à distance
8. Sécuriser les installations informatiques
9. Contacter immédiatement la banque et la police judiciaire en cas d'escroquerie (ou de tentative)