

www.lesclesdelabanque.com

Le site pédagogique sur la banque et l'argent

www.aveclespme.fr

Le site pratique pour les PME

ORDRES DE VIREMENT DES ENTREPRISES

9 RÉFLEXES SÉCURITÉ



FEDERATION
BANCAIRE
FRANCAISE

N°1
LES GUIDES
SÉCURITÉ BANCAIRE



les clés
de la banque

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 : Marie-Anne Barbat-Layani
Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : janvier 2015

SOMMAIRE

Introduction	3
1. Respecter une procédure interne pour l'exécution des virements	6
2. Sensibiliser spécifiquement les collaborateurs au risque d'escroquerie	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 rapidement la banque et la police en cas d'escroquerie (ou de tentative)	22
9 RÉFLEXES SÉCURITÉ	25

Introduction

SELON
LA POLICE JUDICIAIRE,
LES ESCROQUERIES AUX ORDRES
DE VIREMENT AURAIENT TOUCHÉ,
**EN 5 ANS, PLUSIEURS CENTAINES
D'ENTREPRISES** DE TOUTES TAILLES,
IMPLANTÉES EN FRANCE OU DES FILIALES
DANS L'UNION EUROPÉENNE,
**AVEC PLUS DE 300 MILLIONS D'EUROS
DE PRÉJUDICES.**

CERTAINES PME PEUVENT AINSI
SE RETROUVER AVEC UNE TRÉSORERIE
DÉFICITAIRE ET RISQUER DE
METTRE EN PÉRIL LA CONTINUITÉ
DE LEUR ACTIVITÉ.

Parce que vous effectuez régulièrement des ordres de virement, depuis votre système d'information (SI) ou par une plateforme de banque à distance, **ce guide vous présente quelques principes simples pour déjouer les tentatives de fraudes aux ordres de virement.**

Un virement est une opération de transfert financier de compte à compte. Une fois un ordre de virement émis dans le système bancaire, il ne peut plus être annulé : il est irrévocable.

Les tentatives d'escroqueries peuvent concerner une entreprise quelle que soit sa taille : groupe international, PME ou TPE. Elles **consistent à obtenir d'un collaborateur** de cette dernière **l'exécution d'un ordre de virement au bénéfice d'un escroc.**

La Fédération Bancaire Française (FBF) a réalisé avec la Police Judiciaire une vidéo explicative disponible sur :
www.fbf.fr, www.aveclespme.fr,
www.lesclesdelabanque.com



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

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

Un escroc se fait passer pour un des dirigeants auprès d'un collaborateur pour obtenir de lui un virement urgent et confidentiel sur un compte domicilié à l'étranger. Pour cela, l'escroc se sert d'informations recueillies sur la PME et ses dirigeants sur Internet ou auprès de services de l'entreprise.

- **L'escroquerie aux coordonnées bancaires**

Un escroc fait croire à un changement de domiciliation bancaire du bailleur, d'un fournisseur ou de tout autre créancier légitime de l'entreprise pour les prochains règlements de loyers ou de factures. Il envoie les nouvelles coordonnées bancaires par courrier électronique, avec des caractéristiques de messagerie très proches de celles de l'interlocuteur habituel.

- **L'escroquerie à l'informatique**

L'escroc se fait passer pour un technicien prestataire de l'entreprise visée et tente d'obtenir par le collaborateur l'exécution de « virements tests ». Il peut aussi 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 de réussite en utilisant d'autres méthodes.

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, pour la France et pour l'international, par personne habilitée,
- les plafonds périodiques d'opérations,
- le circuit de validation des opérations (au moins 2 personnes).

Les personnes habilitées à effectuer un virement doivent recevoir une formation sur la procédure à respecter. La bonne mise en œuvre de cette procédure doit être contrôlée régulièrement.



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

Sensibiliser spécifiquement les collaborateurs au risque d'escroquerie

Les collaborateurs doivent être conscients que l'entreprise peut à tout moment être la cible de tentatives d'escroquerie. Comment aborder le sujet et que dire exactement ?

Vous pouvez :

- **communiquer sur l'importance de la procédure** d'exécution des virements en place dans l'entreprise, les points de contrôle à effectuer (par exemple savoir distinguer l'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 tentatives d'escroquerie et **appeler à une plus grande vigilance** (en cas de demande extérieure notamment sur les procédures et l'organigramme de l'entreprise, demande de virement vers des coordonnées bancaires nouvelles, orthographe fantaisiste, adresse électronique avec un nom de domaine inhabituel...), etc.



Vous pouvez utiliser la vidéo réalisée par la FBF avec la PJ pour la sensibilisation des équipes des PME.



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 tenter de tromper la vigilance des entreprises.

Pour maintenir une vigilance efficace, il est utile d'effectuer une veille active sur ce sujet grâce à la presse, aux communications des pouvoirs publics ou des associations professionnelles.



N'hésitez pas à communiquer à vos collaborateurs les récentes escroqueries dévoilées.

4

Maîtriser la diffusion des informations concernant l'entreprise

La plupart du temps, les escrocs utilisent des informations extraites du Registre du Commerce et des Sociétés, des procès-verbaux d'assemblée générale mais aussi 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 doit faire particulièrement attention à ne pas diffuser d'informations qui risqueraient de mettre en péril la confidentialité de vos activités et procédures.



EXEMPLE

La publication d'un organigramme détaillé de votre entreprise peut être une source d'information intéressante pour des escrocs. Des appels téléphoniques peuvent être également effectués par un escroc pour vérifier les fonctions de certaines personnes.

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 mais elle devra avoir été minutieusement préparée et le changement de coordonnées bancaires annoncé en amont du règlement,
- nouvelle domiciliation bancaire **à l'étranger** d'un fournisseur/bailleur/client, même en zone SEPA. Des vérifications s'imposent,
- **demande** d'un prétendu dirigeant **de déroger aux procédures définies** et exigeant la plus grande discrétion. La hiérarchie doit être informée.



Il est important de déceler les tentatives d'intimidation, de pression psychologique ou encore l'empathie et la flatterie 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 le plus souvent la veille de week-ends ou de jours fériés pour réduire la possibilité de contrôle. Il est d'autant plus nécessaire de prendre le temps d'effectuer des vérifications, a fortiori si l'opération demandée est inhabituelle.

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

- d'un **contre-appel** auprès du partenaire commercial ou financier au moyen de coordonnées figurant dans les fichiers internes de l'entreprise (ligne de téléphone fixe par exemple),
- d'une **consultation de factures antérieures** en cas de « rappel »,
- ou d'une **demande de renseignement auprès de sa hiérarchie et de ses collègues**.



ATTENTION

Toute opération prétendument urgente doit être systématiquement présentée au responsable hiérarchique désigné, particulièrement celle qui exigerait la discrétion.

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 quelconque document ou communiqués à qui que ce soit.

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.

Sécuriser les installations informatiques

Afin de limiter le risque d'infection et de piratage informatique (par des logiciels espions ou des programmes malveillants), **la possibilité d'installation de logiciels doit être strictement encadrée et vos postes** informatiques doivent **posséder un 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

Les pièces jointes attachées à des messages en provenance d'expéditeurs inconnus ou dont l'adresse présente des différences par rapport à l'adresse habituelle sont également un risque potentiel. Il ne faut ni les ouvrir ni les conserver.

9

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

La **banque** doit être contactée le plus rapidement possible. Elle **pourra** alors **examiner** avec vous **les possibilités pour éventuellement 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 très courts.
Une réaction rapide est
donc essentielle.

En cas de tentative d'escroquerie, il sera sans doute prudent de demander un changement de vos codes d'accès pour vos services de banque à distance.

La division économique et financière du Service Régional de **Police Judiciaire** (SRPJ) **doit** également **être saisie et une plainte doit être déposée.**

Un maximum d'éléments constitutifs de l'escroquerie doivent être apportés en appui : courriers électroniques, fax, enregistrements de conversation, numéros de téléphone des correspondants... pour être transmis aux enquêteurs.



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

9 RÉFLEXES SÉCURITÉ

1. Respecter une procédure interne pour l'exécution des virements
2. Sensibiliser spécifiquement les collaborateurs au risque d'escroquerie
3. Être en veille sur les escroqueries aux entreprises
4. Maîtriser la diffusion des informations concernant l'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 rapidement la banque et la police en cas d'escroquerie (ou de tentative)



Retrouvez la
vidéo dédiée

