MAI 2016

Ce guide a été élaboré
avec la Police Judiciaire

ORDRES DE VIREMENT
DES ENTREPRISES

9 RÉFLEXES SÉCURITÉ

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**

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 : mai 2016

SOMMAIRE

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

Introduction

Avec plus de 500 millions d'euros de préjudices depuis 2010, ce sont au moins 1 600 entreprises victimes d'escroqueries aux ordres de virement qui en subissent les conséquences souvent désastreuses. Certaines ont perdu toute ou partie de leur trésorerie et quelques-unes ont dû aller jusqu'à la liquidation.

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

Un virement est un 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 consistent 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**.

La Fédération bancaire française (FBF) a réalisé, avec la Police judiciaire, une vidéo explicative disponible sur :
www.fbf.fr, www.aveclespme.fr,
www.lesclesdelabanque.fr

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 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 recueillies sur la société et ses dirigeants sur internet ou auprès de services de l'entreprise lors d'appels précédents.

- **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 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 par courrier électronique ou avec un courrier en bonne et due forme, avec des caractéristiques très proches de celles de l'interlocuteur habituel (adresse de messagerie, en-tête de courrier...).

- **L'escroquerie à l'informatique**

  L'escroc se fait passer pour un technicien du service connectique 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.

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 spécifiquement les collaborateurs au risque d'escroqueries

La sécurité est l'affaire de tous 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'escroqueries ou des tentatives d'escroqueries (communiqués par vos réseaux : fédérations professionnelles… ou recherchés dans les médias),
- **appeler à une plus grande vigilance** face aux demandes extérieures notamment sur les procédures, l'organigramme de l'entreprise, face aux courriers reçus avec une orthographe fantaisiste ou une adresse électronique avec un nom de domaine inhabituel, etc.

Vous pouvez utiliser la vidéo réalisée par la FBF (4 minutes) avec la Police Judiciaire pour sensibiliser vos équipes.

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 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 informer vos collaborateurs des récentes escroqueries dévoilées.

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 est une source d'information 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 mais elle doit normalement 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 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 à 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 (ligne de téléphone fixe par exemple),
- d'**une consultation de factures antérieures** en cas de « rappel pour impayé »,
- ou d'**une demande de renseignement auprès de sa hiérarchie et de ses collègues**.

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 connus uniquement des personnes habilitées** à s'y connecter. Ils doivent rester strictement confidentiels et ne pas être reportés sur un document ni communiqués à qui que ce soit. Ils doivent toujours permettre 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), **la possibilité d'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 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)

C'est certainement l'action la plus importante à engager 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.

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

Le Service Régional de Police Judiciaire (SRPJ) doit être contacté 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
9 RÉFLEXES SÉCURITÉ

1. Respecter une procédure interne pour l'exécution des virements
2. Sensibiliser spécifiquement les collaborateurs au risque d'escroqueries
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 judiciaire en cas d'escroquerie (ou de tentative)

Retrouvez la vidéo dédiée

les clés de la banque

www.lesclesdelabanque.com
Le site pédagogique sur la banque et l'argent

www.aveclespme.fr
Le site pratique pour les PME

FÉDÉRATION
BANCAIRE
FRANÇAISE