Ordres de virement

9 RÉFLEXES SÉCURITÉ

les clés de la banque

LES GUIDES BANCAIRES
N°1 / Sécurité

CE GUIDE VOUS EST OFFERT PAR :

les clés de la banque

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

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 : mai 2024

SOMMAIRE

9 RÉFLEXES SÉCURITÉ

En cas de fraude avérée ou de tentative, votre rapidité à contacter votre banque et la Police Judiciaire est essentielle.

Introduction

Les fraudes aux ordres de virement ont des conséquences graves : perte de tout ou partie de la trésorerie ou même liquidation de l'entreprise. En 2022, les préjudices recensés s'élevaient à 313 millions d'euros pour les entreprises, les services publics et les particuliers, soit 3 fois plus qu'il y a 5 ans !
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 réagir efficacement.

Fraudes types les plus fréquentes (liste non exhaustive)

Les tentatives d'escroqueries consistent à obtenir d'un collaborateur **de l'entreprise l'exécution d'un ordre de virement non planifié, pour un motif apparemment valable, au bénéfice d'un escroc**. Une fois émis dans le système bancaire, le virement est irrévocable : impossible de l'annuler.

L'escroquerie à l'usurpation d'identité

L'escroc se fait passer pour une personne de l'entreprise (y compris de la direction, ex : « fraude au président ») ou pour une autorité extérieure (commissaire aux comptes, banquier, fonctionnaire de police ou du renseignement intérieur voire un ministre…) auprès d'un collaborateur ou du président de l'entreprise, pour lui faire réaliser un virement.

Pour le convaincre, il prétexte que c'est urgent et confidentiel. Il 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 (ingénierie sociale). Souvent, le compte bénéficiaire est domicilié à l'étranger.

ATTENTION Avec le développement de l'intelligence artificielle, les escrocs peuvent modifier des vidéos ou des enregistrements sonores, de sorte qu'on croit véritablement qu'il s'agit de la personne dont ils usurpent l'identité. On appelle ça un « deepfake ».

L'escroquerie aux coordonnées bancaires
(fraude au RIB)

L'escroc fait croire à un changement de domiciliation bancaire du bailleur, d'un fournisseur/prestataire de services ou de tout autre créancier de l'entreprise.

L'escroc envoie de nouvelles coordonnées bancaires et une facture par courrier électronique ou postal avec des caractéristiques très proches de celles de l'interlocuteur habituel (adresse e-mail, en-tête de courrier…).

L’escroquerie à l’informatique

L’escroc se fait passer pour un personnel du service technique de la banque de l’entreprise visée. Il 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 permettant de récupérer des informations de sécurité ou de pirater le système informatique de l’entreprise.

ATTENTION Les escrocs renouvellent leurs modes opératoires régulièrement. Ils persévèrent en cas d’échec comme en cas de succès, en utilisant d’autres méthodes si nécessaire.

Le piratage de la messagerie électronique

Un pirate peut avoir récupéré vos accès à votre boîte mail.

Il peut alors intercepter un message et modifier une pièce jointe. Il pourrait ainsi remplacer le RIB envoyé ou reçu par le sien pour récupérer l'argent.

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 a été piratée et suspendez tout paiement le temps de cette vérification.

Sécurisez votre boîte mail pour éviter qu'un pirate n'y accède. À chaque nouveau RIB reçu ou envoyé par mail, et avant tout virement, appelez votre interlocuteur aux coordonnées habituelles pour vérification.

Cybermalveillance.gouv.fr, propose des modules d'e-sensibilisation (« SensCyber »), accessibles à tous, pour comprendre, agir, partager les bonnes pratiques et tester vos connaissances en matière de cybersécurité.

1. Respecter une procédure interne pour l'exécution des virements

Vous devez établir une procédure écrite et claire au sein de votre entreprise **pour l'exécution des virements**. Elle doit préciser notamment :

- l'identité des personnes habilitées à effectuer des virements ;
- les montants autorisés, par personne habilitée, en France et à l'international ;
- les plafonds périodiques d'opérations et les zones géographiques autorisées ;
- le circuit de validation des opérations (au moins 2 personnes) ;
- la procédure spécifique en cas d'urgence ou d'opérations inhabituelles.

Pour être efficace, cette procédure nécessite :

- la **formation** régulière **des personnes habilitées** à effectuer un virement ;
- un **contrôle** régulier de sa pertinence pour une éventuelle mise à jour ;
- une communication interne sur son existence, à destination du personnel non habilité.

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

2. Sensibiliser les collaborateurs aux risques de fraude

La sécurité est l'affaire de tous au sein de l'entreprise. Chaque collaborateur, quelle que soit sa fonction, doit être conscient que leur entreprise peut à tout moment être la cible de tentatives d'escroquerie.

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 de tentatives (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, des fautes, ou une adresse électronique avec un nom de domaine inhabituel, etc. ;
- **entraîner vos équipes** à détecter les mails frauduleux à l'aide de prestataires spécialisés.

3. Être en veille sur les escroqueries aux entreprises

Les **fraudes évoluent régulièrement** : les escrocs adaptent constamment leurs méthodes en fonction de leurs expériences et profitent de l'actualité, économique, financière… pour tromper la vigilance des entreprises.

Pour maintenir une veille efficace et informer vos collaborateurs des dernières escroqueries, suivez les informations récentes sur les fraudes grâce à la **presse**, aux communications des **pouvoirs publics** et des **associations professionnelles**.

De nombreuses occasions ou événements permettent de sensibiliser et former votre entreprise : Forum InCyber (ex Forum International de la Cybersécurité), événements organisés par les Chambres de Commerce, par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI), le cybermoi/s…

4. Maîtriser la diffusion des informations concernant l'entreprise

Un certain nombre d'informations peuvent circuler sur votre entreprise… extraits du Registre national des entreprises, organigramme, procès-verbaux d'assemblée générale, dans la presse… et bien sûr sur votre propre site Internet.

Tous ces éléments sont utilisés par les escrocs pour gagner la confiance d'interlocuteurs au sein de l'entreprise pour leur soutirer davantage d'informations, notamment confidentielles. Ils peuvent passer des appels téléphoniques, a priori anodins, pour vérifier la fonction de certains collaborateurs. Ayant rassemblé un maximum d'informations, ils peuvent alors facilement se faire passer pour un dirigeant ou un partenaire de l'entreprise.

ATTENTION Ne diffusez jamais d'informations qui risqueraient de compromettre la confidentialité de vos activités et procédures. Ne divulguez ni le nom ni la fonction des personnes habilitées à réaliser des virements.

5. Faire preuve de bon sens

Les escrocs veulent 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 est minutieusement préparée et annoncée 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 aussi 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. Ils privilégient d'ailleurs les veilles de weekends ou de jours fériés pour éviter au maximum les contrôles.

Prenez donc le temps d'effectuer des vérifications, surtout quand l'opération demandée est inhabituelle. Cette vérification doit **par exemple** prendre la forme de :

- **contre-appel** auprès du partenaire commercial ou financier en utilisant les coordonnées « connues » figurant dans vos fichiers internes ;
- **consultation de factures antérieures** en cas de « rappel pour impayé » ;
- **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 notés sur un document ni communiqués à qui que ce soit. Ils permettent une traçabilité des connexions et transactions effectuées par chaque personne.

Les mots de passe doivent être suffisamment complexes et souvent 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) via notamment des recherches sur Internet.

ATTENTION Codes, identifiants, mots de passe, ne donnez jamais ces données. Même votre établissement bancaire ne vous les demandera jamais.

8. Sécuriser les installations informatiques

Afin de limiter le risque d'infection et de piratage informatique (par des programmes espions ou malveillants), **l'installation de logiciels doit être strictement encadrée. 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 de fraude

La **banque** examinera la possibilité de procéder à un « **retour de fonds** » dans le cadre des relations interbancaires. Les délais sont cependant extrêmement courts. Une réaction rapide est donc essentielle. Pensez à modifier vos codes d'accès aux services de banque à distance.

Au sein de la police judiciaire, la division de lutte contre la criminalité financière mènera au plus tôt les actions nécessaires (enquêtes, relations avec les services d'autres pays…).

Déposez plainte en fournissant un maximum d'éléments constitutifs de l'escroquerie en appui : courriels, fax, enregistrements de conversation, numéros de téléphone des correspondants…

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

LES RÉFLEXES CLÉS

Ordres de virement

1. Respecter une procédure interne pour l'exécution des virements
2. Sensibiliser les collaborateurs aux risques de fraude
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 immédiatement la banque et la police judiciaire en cas de fraude

lesclesdelabanque.com

FÉDÉRATION
BANCAIRE
FRANÇAISE