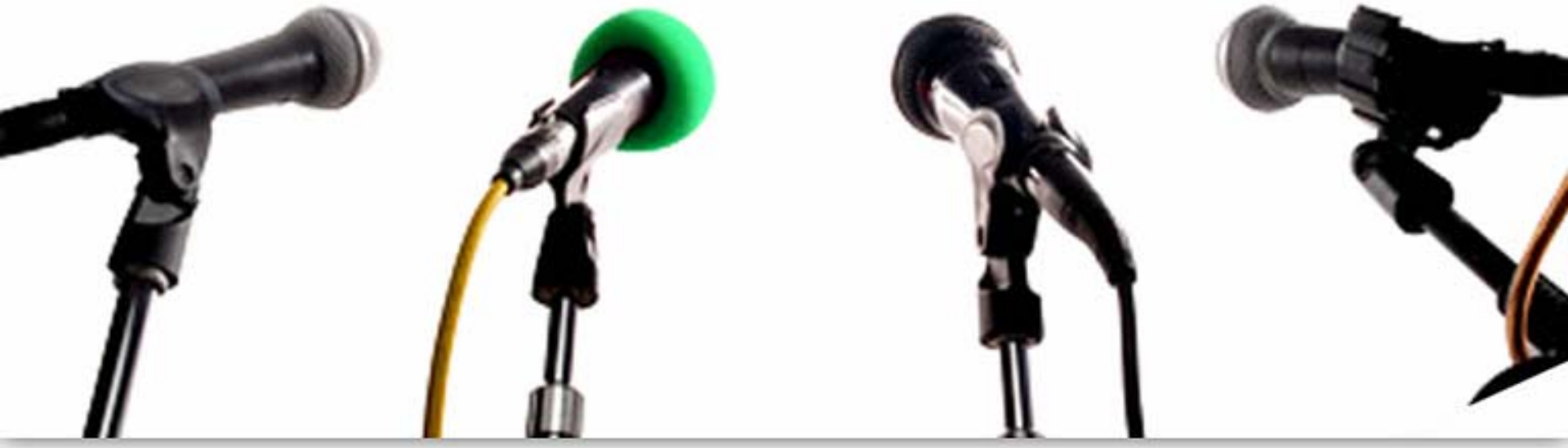
La fraude en entreprise

@ 2015



Prévention de la Fraude

Un contexte favorable à la délinquance financière internationale

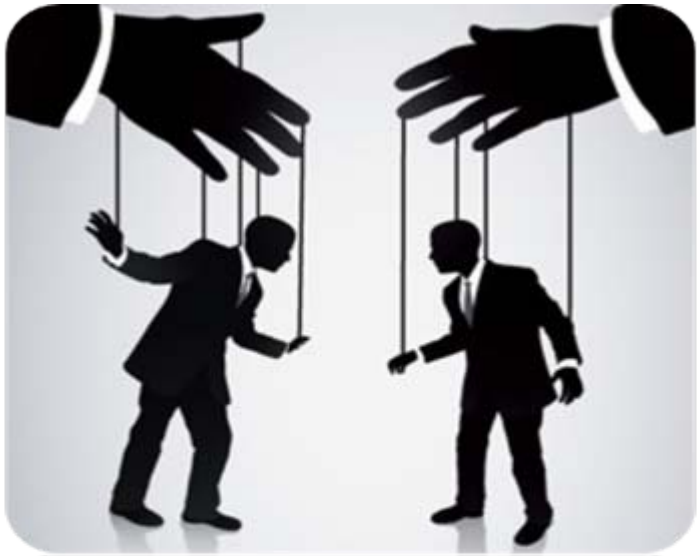
La délinquance financière évolue au rythme où le monde se transforme

- **La mondialisation transforme la délinquance**
  - Des structures d'entreprises de plus en plus complexes qui offrent de beaux terrains de jeu aux fraudeurs
  - La liberté de circulation des capitaux et la fin du contrôle des changes constituent de formidables opportunités
- **Le développement d'Internet et des nouvelles technologies donnent des capacités d'attaques pour :**
  - Scruter les entreprises en pénétrant dans le système d'information et y bâtir des scenarii d'attaques les plus sophistiqués
- **Une volonté de transparence**
  - Qui constitue une arme pour la délinquance financière

Des autorités par nature nationales qui se heurtent à des organisations sans frontières

- **Des états qui n'extradent pas leurs sujets nationaux**

ESCROQUERIE
AUX FAUX ORDRES DE VIREMENT
INGÉNIERIE SOCIALE



Les virements Frauduleux

Définition :

➢**Appropriation par un fraudeur d'informations concernant un client (coordonnées bancaires, logo commercial, signature) dans le but de détourner des fonds à son profit au moyen d'un ordre de virement (ou transfert).**

➢**Le virement frauduleux est l'aboutissement d'un stratagème visant à voler des fonds sur le compte bancaire d'un client. L'attaque se caractérise par intrusion (malware-phishing) ou par usurpation d'identité. Dans le second cas, le fraudeur se fait passer pour le client ou pour la banque.**

➢**Les cas les plus souvent rencontrés sont :**

- **Par malware**
- **Par phishing des codes Banque en ligne**
- **Par courrier ou par FAX adressé à l'agence bancaire**
- **Par téléphone en prétextant un test SEPA**
- **Par transfert d'appel ou swap de cartes SIM**

- **Par social Engineering**

Phishings avec pièces jointes

- **Augmentation des phishings dits « avec pièces jointes » :**

  - **Il s'agit de phishing classiques, c'est à dire de mails "se faisant passer pour", à ceci près qu'ils ne contiennent pas de lien vers un faux site de banque en ligne mais sont porteurs d'une pièce jointe html que l'internaute doit ouvrir puis renseigner.**

  - **De très nombreuses informations sont demandées et la finalité de ces attaques (virements frauduleux, ingénierie sociale, fraude carte bancaire ...) n'a pas encore été identifiée.**

Les techniques d'ingénierie sociale les plus courantes

La "Fraude au président ou Directeur Général "

- En usurpant l'identité d'un dirigeant, le fraudeur obtient la collaboration d'une personne de l'entreprise afin d'effectuer un virement à l'étranger, par exemple en prétextant une acquisition de société urgente et très confidentielle
- Les principaux critères d'alerte de cette fraude:
  - Une demande urgente, exceptionnelle et confidentielle
  - Une forte pression exercée sur le collaborateur
  - Une opération inhabituelle vers des comptes et/ou bénéficiaires inconnus

L'usurpation de la banque

- Le fraudeur se fait passer au téléphone pour un interlocuteur de la banque afin d'obtenir des informations confidentielles (codes d'accès, mots de passe), par exemple en demandant à l'entreprise d'effectuer des « virements tests » ou encore des connexions pour mises à jour
- Les principaux critères d'alerte de cette fraude:
  - Une demande de virement avec un montant élevé pour un test
  - L'Utilisation de la norme SEPA pour justifier un tel virement
  - Une demande de prise de contrôle à distance de l'ordinateur du collaborateur

Détournement de lignes téléphoniques

- Les fraudeurs se font passer pour des fournisseurs pour demander des modifications de coordonnées bancaires. Ils confirment ces demandes par de faux courriels ou faux numéros de fax, allant même jusqu'à demander aux opérateurs télécom de re-router les lignes des standards vers leur numéro → Les contre-appels sont dès lors inopérants
- Les principaux critères d'alertes de cette fraude:
  - Un de vos fournisseurs communique de nouvelles coordonnées bancaires par fax ou courriel

Ingénierie sociale
La démarche du fraudeur
5 phases d'attaque

1. La collecte de renseignement : Identification des employés – localisation des documents – copinage – fouille de poubelle – intimidation

- La partie « récolte d'information » est la partie la plus importante de façon à accéder au niveau de privilège le plus élevé possible
- Un fonctionnement des attaques par rebond : chaque information recueillie permet d'accéder au niveau supérieur

2. Recherche du maillon faible : analyse des informations recueillies et sélection d'identités – ciblage – recoupement

Ingénierie sociale
La démarche du fraudeur
5 phases d'attaque (suite)

3. Acquisition d'adresses mail, numéro de fax, de téléphonie :

4. Elaboration de l'objet de la demande : contrôle fiscal, opérations en capital très confidentielles, règlement d'avocats à l'étranger,...

5. Exécution de l'attaque :

- ✓ Muni des informations et utilisant un numéro de téléphone français, l'escrocs se fait passer pour le dirigeant et va persuader le directeur financier ou le comptable d'exécuter un virement.

Les leviers psychologiques : éléments importants

- ✓ Volonté d'endormir la surveillance de sa cible
- ✓ Jouer sur la confiance naturelle et obtenir la soumission sans pression autoritaire
- ✓ Prendre le contrôle : celui qui pose les questions contrôle la conversation
- ✓ Imposer la prise de décisions :
  - ➢ Invoquer un impératif ou un risque de retombées négatives
  - ➢ Oter tout espace de réflexion
  - ➢ Contrainte d'obéir dans l'urgence

Exemple de mail reçu

De : [redacted]
Envoyé : jeudi 3 avril 2014 19:29
À : AUBERT Christine
Cc [redacted]
Objet : Dossier Confidentiel

Bonjour Mme Aubert,

Mon avocat-conseil Maître Desmarais, devrait vous contacter, au sujet d'une opération financière confidentielle, que nous menons conjointement.

Voici l'OPA en cours,

Nous effectuons en ce moment une opération financière confidentielle, concernant un rachat de société.

Cette OPA doit rester strictement confidentielle, personne d'autre ne doit être au courant pour le moment.

L'annonce public de cette OPA aura lieu le 26 Avril 2014 dans nos locaux avec la présence de toute l'administration.

Je vous ai donc choisi pour votre discrétion et votre travail irréprochable au sein du groupe pour le traitement de cette OPA.

Merci de prendre contact immédiatement avec notre cabinet juridique [redacted] pour la remise des coordonnées bancaires afin d'effectuer le virement en date de valeur de ce jour.

Ps : par mesure de sécurité concernant ce type d'opération confidentielle, nous dialoguerons uniquement sur mon mail personnel ([redacted]) pour le moment, ceci afin d'éviter tous risques de divulgation et de respecter les normes de cette OPA.

Merci de ne faire aucune allusion sur ce dossier de vive voix, ni même par téléphone uniquement sur mon mail personnel, selon la procédure imposée par l'AMF (Autorité des Marchés Financiers).

Cordialement,
--
[redacted]

Comment réagir après avoir constaté une fraude

Réactivité, Réactivité, Réactivité, ……..

Le temps est un facteur-clé : réagir sans délai et dans les 24 heures

➢ **Comprendre le mode opératoire : qui à fait quoi et comment**

➢ **<u>Contacter votre banque</u> pour une intervention auprès de la banque bénéficiaire**

❑ **Depuis le 1er janvier 2012, le délai du virement varie selon le type de situation:**

- **Il est de 4 jours ouvrables maximum pour les virements dans l'EEE et dans une devise de ces Etats autres que l'euro (*article L. 133-12 du CMF*)**
- **Il est d'1 jour ouvrable maximum à compter de la réception de l'ordre de virement s'agissant de virements en France et en euros dans la zone SEPA *(Union Européenne + Islande, Norvège, Liechtenstein, Suisse et Monaco)***
- **Il n'y a pas de délai pour les virements émis vers un compte situé hors de l'Espace Economique Européen (« EEE ») ou dans une monnaie qui n'appartient pas à l'un de ces Etats**

➢ **Dépôt de plainte**

➢ **Constituer une « cellule de crise »**

- **L'équipe d'audit (interne dans les grandes entreprises, sinon externe avec des garanties d'indépendance face à la justice et de confidentialité)**
- **L'avocat (pour qualifier le type de fraude, puis définir la stratégie en justice)**
- **<u>Point d'attention</u>** : confidentialité, communication restreinte (attention au complicité interne)

➢ **Prévenir l'assureur**

Les mesures de vigilance
Au niveau de l'entreprise (1/2)

Adopter de bons comportements et des mesures de prévention, car lutter contre la fraude suppose que chaque collaborateur :

- Respecte scrupuleusement les règles de sécurité de l'entreprise
- Alerte de toute demande inhabituelle

Sécuriser les processus et outils internes à l'entreprise:

- Limiter et contrôler l'accès aux applications sensibles
- Dissocier saisie et validation des ordres bancaires
- Définir et respecter les procédures de validation
- Sécuriser l'accès aux applications et données sensibles
- Réaliser des contrôles réguliers

Sécuriser les échanges avec la banque

- Limiter ou supprimer les virements papier ou fax (risque de fraude élevé)
- Privilégier le canal web automatisé et sécurisé
- Alerter au plus vite la banque en cas de doute

Les mesures de vigilance
Au niveau de l'entreprise (2/2)

Sensibiliser régulièrement les collaborateurs

- Inciter les collaborateur à conserver un esprit critique et un exercice du droit d'alerte, à résister à la pression psychologique
- Ne pas se contenter des informations affichées
- Encourager la bonne connaissance des interlocuteurs (clients fournisseurs, partenaires)
- Rappeler aux collaborateurs de ne révéler à quiconque, sous aucun prétexte, mots de passe et identifiants
- Garder un respect absolu des procédures
- Valoriser les managers et collaborateurs ayant déjoué des fraudes grâce à leur vigilance

Maitriser la diffusion d'information

- Limiter les informations publiées sur les sites internet de l'entreprise
- Conserver la confidentialité des signatures manuscrites
- Limiter l'accès aux documents sensibles (modèles de fax etc.), broyer les documents confidentiels obsolètes
- Recommander aux collaborateurs de ne pas publier d'informations relatives à l'entreprise sur internet (réseaux sociaux, blogs, etc.)

Rebondir après la fraude

- **Au-delà de la perte financière et du risque d'image associé, une fraude peut et doit être l'occasion de rebondir.**

- **En renforçant les dispositifs de maîtrise des risques :**
  - Identification des risques
  - Renforcement du dispositif de contrôle (et des moyens associés)
  - Revue de l'organisation et de la gouvernance
  - Changement de culture :
    - Vigilance
    - Rigueur et discipline
    - Responsabilité individuelle

- **L'existence de la fraude doit générer une prise de conscience des failles du dispositif, et permettre de mobiliser des leviers clé ….**
  - Effectuer des analyses post mortem
  - Support et attention du management
  - Sensibilisation des collaborateurs aux risques

- **… qui permettront à l'entreprise de rebondir et de sortir renforcé de l'épreuve**

Liens utiles

- Guide Sécurité Internet du Crédit Agricole , mis à jour régulièrement

- Fédération Bancaire Française : 9 réflexes sécurité

- Reportages :

  Interview FBF Willy Dubost et OCRGDF JM Souvira
  (L'Office Central pour la Répression de la Grande Délinquance Financière)

  http://bigbrowser.blog.lemonde.fr/2013/02/08/larnaqueur-comment-des-voyous-se-font-passer-pour-de-grands-patrons/