

---

# LA LUTTE CONTRE L'INGÉNIERIE SOCIALE



## La lutte contre l'ingénierie sociale

### Prévention dans les entreprises clientes

#### **Sécuriser les processus et outils internes à l'entreprise :**

- **Définir des processus clairs et formalisés :**
  - si possible, mettre un place un workflow automatisé sur le périmètre Cash Management / trésorerie
- **Sécuriser l'accès aux applications et données sensibles :**
  - limiter les droits des utilisateurs au strict nécessaire ;
  - évaluer l'intérêt des dispositifs d'authentification forte pour les fonctions sensibles ;
- **Mettre en place une ségrégation des rôles :**
  - dissocier saisie et validation des ordres (virements, déclaration de BIC/IBAN) ;
- **Réaliser des contrôles réguliers** (respect des procédures, vérifications des comptes...).



#### **Sécuriser les échanges avec la Banque :**

- **Dématérialiser les flux financiers :**
  - limiter les virements papier / fax (moyen de paiement avec lequel le risque de faux est élevé)
  - privilégier les canaux automatisés (Sogecash Net, Sogecash Web, Ebics, SWIFTNet...) en respectant strictement toutes les consignes de sécurité afférentes à ces outils (clé e-secure, droits des utilisateurs...)
- Communiquer lors d'un rendez-vous avec la banque les noms, signatures, fonctions et coordonnées des personnes habilitées et à joindre en cas de doute sur des opérations bancaires.

## La lutte contre l'ingénierie sociale

### Prévention dans les entreprises clientes

---

#### **Sensibiliser largement le personnel susceptible d'être contacté par les escrocs :**

Cadres, employés des services comptabilité, fournisseurs, trésorerie, informaticiens ...

Ne pas oublier les [secrétaires et standardistes](#) (appelées également lors de la phase d'ingénierie sociale)

Sensibiliser également les [cabinets d'avocats](#) qui représentent l'entreprise dans les pays à risques

But : gagner un temps précieux en cas de transfert frauduleux et actions juridiques à entreprendre à l'étranger.

- Respect des procédures opérationnelles et réalisation des contrôles prévus ;
- Connaissance des interlocuteurs (clients, fournisseurs, partenaires) ;
- Esprit critique ; exercice du droit d'alerte ;
- Valoriser les tentatives de fraudes stoppées.

#### **Ne pas se contenter des informations affichées :**

- Falsification de l'adresse mail apparente de l'expéditeur ;
- Falsification du numéro appelant qui s'affiche sur votre téléphone.

#### **Limiter la diffusion d'informations :**

- Réseaux sociaux professionnels (LinkedIn...), et personnels (Facebook) ;
- Sites internet de l'entreprise ;
- Modèles de fax de l'entreprise ;
- Signatures manuscrites des dirigeants autorisés à valider les opérations (y compris sur les sites internet de l'entreprise).

## La lutte contre l'ingénierie sociale

### Conduite à tenir dans les entreprises clientes

---

1. **Savoir résister à la pression, avoir un sens critique ;**
2. **Respecter les procédures internes ;**
3. **Vérifier la légitimité de la demande :**
  - **Contre-appel vers un numéro déjà référencé, voire vers plusieurs personnes**
  - **Toute autre méthode validée par votre entité**
4. **Ne pas se laisser isoler :**
  - **Ne pas hésiter à faire appel à un collègue ou un responsable.**

**En cas de fraude avérée ou supposée**



**Alerter un responsable interne  
ET la(es) banque(s) et les autorités de police compétentes**

### QUE FAIRE EN CAS DE FRAUDE DETECTEE ?

**La récupération des fonds dépend des actions engagées simultanément par plusieurs acteurs (BANQUE / CLIENT / POLICE)**

#### CLIENT :

- **prévenir la banque** pour qu'elle demande immédiatement le blocage des fonds à la banque destinataire du virement frauduleux
- **déposer plainte en France auprès des autorités compétentes et selon le cas, à l'étranger** auprès de la police locale (indispensable en Chine ou Pologne) pour confirmer la demande de gel des fonds
- **procéder à un contrôle complet du système informatique** (vérification de présence de logiciels malveillants ...)

#### BANQUE :

- appliquer la « procédure de récupération des fonds »
- solliciter le réseau TRACFIN (sans mentionner l'ouverture d'une procédure judiciaire)
- renforcer la sécurité du compte et des contrats Banque à Distance du client (changement codes confidentiels ...)

#### POLICE :

- demande de gel des fonds par l'intermédiaire d'Europol / Interpol et de l'attaché de sécurité intérieure dans le pays destinataire
- officialisation de cette demande par une ordonnance de saisine pénale des fonds, délivrée par un magistrat et collecte de renseignements sur le titulaire du compte à l'étranger et la destination finale des fonds (par Demande d'Entraide Pénale Internationale ou Commission Rogatoire Internationale )

Le temps qui passe joue pour les escrocs ... !



## **Services de police compétents en matière d'ingénierie sociale**

Sur Paris et petite couronne (départements 75, 92,93 et 94) :

### **Brigade des Fraudes aux Moyens de Paiement (BFMP)**

122-126 Rue du Château des Rentiers  
75013 PARIS  
Secrétariat : 01 55 75 22 94

Adjoint au Chef de service : Dominique DUGOIS Commandant Fonctionnel

Ligne Directe : 01 55 75 23 14

Mail : [dominique.dugois@interieur.gouv.fr](mailto:dominique.dugois@interieur.gouv.fr)

Bertrand DUMOUILLA

Ligne Directe : 01 55 75 22 93

Mail : [bertrand.dumouilla@interieur.gouv.fr](mailto:bertrand.dumouilla@interieur.gouv.fr)

Compétence nationale :

### **Office Central pour la Répression de la Grande Délinquance Financière (OCRGDF)**

101 Rue des Trois Fontenot  
92 000 NANTERRE  
Secrétariat : 01 40 97 84 17

En Province :

**SRPJ / DIPJ** ou Brigade de recherche de la Gendarmerie Nationale

**La sécurité est l'affaire de tous.  
Conjuguons nos efforts pour lutter ensemble contre  
la fraude.**

- Les tentatives de fraudes ne peuvent pas être évitées ;
- Les fraudeurs sont de plus en plus inventifs et organisés ;

**Mais**

- Les impacts peuvent être limités grâce à :
  - des processus internes fiables et appliqués avec rigueur ;
  - une vigilance accrue au quotidien ;
  - un partage constant d'informations (mutualisation des bonnes pratiques, informations sur les tentatives déjouées ...).