QUI CONTACTER ?

SERVICES DE POLICE COMPÉTENTS EN MATIÈRE D'INGÉNIERIE SOCIALE

- **Paris et petite couronne (départements 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**

- **Compétence nationale**

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

  101, rue des Trois Fontanot
  92000 NANTERRE

  Secrétariat **01 40 97 84 17**

- **Autres**

  SRPJ ou Brigade de recherches de la Gendarmerie Nationale (en province)

En cas de doute, n'hésitez pas à prendre contact avec votre interlocuteur Société Générale habituel

LA PRÉVENTION DES FRAUDES BANCAIRES par ingénierie sociale

SOCIETE GENERALE

Banque & Assurances

Société Générale - BDDF/DCM/CCM Tour Granite 75886 PARIS CEDEX 18 - S.A. au capital de 998 320 373,75 EUR - 552 120 222 RCS PARIS. Siège social : 29, bd Haussmann 75009 PARIS - Crédit photos : Samuel Melo - GettyImages - SG - 10/2013

DEVELOPPONS ENSEMBLE

L'ESPRIT D'EQUIPE SOCIETE GENERALE

Toujours se rappeler que

LA SÉCURITÉ EST L'AFFAIRE DE TOUS !

Les fraudeurs exploitent les faiblesses des organisations qu'ils ciblent, en particulier l'absence éventuelle de coordination entre les différents acteurs d'un processus.

En cas de doute, n'hésitez pas à contacter votre correspondant habituel au sein de Société Générale.

L'ingénierie sociale

se définit comme « l'art » de manipuler son interlocuteur pour qu'il réalise une action ou divulgue une information.

Les comportements frauduleux ne constituent pas un phénomène nouveau. En effet, les escroqueries, abus de confiance ou détournements d'actifs ont toujours accompagné l'activité économique.

Cependant, les moyens techniques et de communication actuels (messageries et réseaux sociaux), accessibles à un public large, ouvrent des opportunités nouvelles aux fraudeurs, tant en termes de variété que de complexité des attaques.

En outre, les risques pénaux encourus par les cybercriminels restent aujourd'hui limités par rapport à d'autres délits plus « classiques ».

Enfin, le caractère international des malversations complexifie le travail d'enquête des forces de l'ordre et l'arrestation des fraudeurs.

Les banques ont été les premières entreprises ciblées par ces fraudes. Cependant, on constate aujourd'hui un report assez massif de ces attaques vers les entreprises françaises, leurs filiales à l'étranger et les implantations françaises de groupes étrangers (Directions Financières en particulier). Les banques font face à ce problème depuis de nombreuses années et Société Générale souhaite sensibiliser ses clients sur ce sujet.

Les mesures de prévention

Les bonnes pratiques de lutte contre l'ingénierie sociale rappelées ici sont appliquées par Société Générale et font l'objet de révisions constantes. Pour une efficacité maximale, nous vous proposons de les déployer également au sein de votre organisation.

1 SÉCURISER LES PROCESSUS ET OUTILS INTERNES À L'ENTREPRISE

- Définir des processus clairs et formalisés
  - *Si possible, automatiser les processus 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, déclarations de BIC/IBAN)*
- Réaliser des contrôles réguliers
  - *Respect des procédures, vérification des comptes...*

2 SÉCURISER LES ÉCHANGES AVEC LA BANQUE

- Limiter les virements papier ou fax (moyens de paiement avec lesquels 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 à joindre en cas de doute sur des opérations bancaires

3 SENSIBILISER LES COLLABORATEURS AUX COMPORTEMENTS APPROPRIÉS

- Respect des procédures opérationnelles et réalisation des contrôles prévus
- Connaissance des interlocuteurs (clients, fournisseurs, partenaires)
- Esprit critique et exercice du droit d'alerte
- Ne pas se contenter des informations affichées : les fraudeurs peuvent facilement modifier l'adresse mail apparente de l'expéditeur ou le numéro de téléphone appelant qui s'affiche sur le téléphone de leur cible
- Valorisation par les managers des tentatives de fraudes stoppées grâce à la vigilance des collaborateurs

POPULATIONS LES PLUS EXPOSÉES
Trésoriers - Comptables - Personnes agissant sur les moyens de paiement

4 LIMITER LA DIFFUSION DE L'INFORMATION

- Contrôler la diffusion d'informations sur les sites Internet de l'entreprise
- Recommander aux collaborateurs de ne pas diffuser d'informations sensibles sur les réseaux sociaux professionnels (LinkedIn…) et personnels (Facebook…)
- Veiller à limiter l'accès aux documents sensibles, comme le modèle de fax de l'entreprise
- Conserver la confidentialité des signatures manuscrites des dirigeants autorisés à valider des opérations (y compris sur les sites Internet de l'entreprise)

QUELQUES CAS D'INGÉNIERIE SOCIALE : critères d'alerte et conduite à tenir

L'imagination des fraudeurs est sans limite et les cas d'ingénierie sociale sont plus fréquents depuis quelques mois. Certains signaux peuvent vous alerter…

CRITÈRES D'ALERTE

FRAUDE AU PRÉSIDENT

- Demande urgente et confidentielle
- Virement inhabituel (montant important, vers un compte inconnu ou un pays avec lequel l'entreprise n'a aucune activité)
- Demande exceptionnelle, ne respectant pas les procédures internes

FAUX VIREMENTS SEPA

Société Générale ne sollicite jamais un client afin de :

- réaliser des virements tests d'un montant supérieur à quelques euros
- communiquer des informations confidentielles par téléphone ou e-mail (en particulier : identifiant et mot de passe)
- prendre le contrôle de son ordinateur

DÉTOURNEMENT DES LIGNES TÉLÉPHONIQUES

- Un site ou un service ne reçoit plus aucun appel téléphonique pendant une période anormalement longue
- Une de vos connaissances vous contacte sur votre portable et vous indique qu'un inconnu répond aux appels sur votre ligne fixe

EN CAS DE DEMANDE INHABITUELLE

1. **Savoir résister à la pression et avoir un sens critique**
2. **Respecter les procédures internes**
3. **Vérifier la légitimité de la demande**
   - *Contre-appel vers un numéro déjà référencé*
   - *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)

N'OUBLIEZ PAS !

- Les tentatives de fraude ne peuvent être évitées dans le cadre d'une activité industrielle ou commerciale classique
- Les fraudeurs font preuve d'inventivité, sont parfois bien organisés, démontrent souvent une expertise technique importante

MAIS…

- Outre les contre-mesures techniques bien connues des Directions des Systèmes d'Information, les impacts peuvent être limités grâce à :
  - **des processus internes fiables et appliqués avec rigueur**
  - **une vigilance au quotidien des salariés dans le cadre de leur fonction**
  - **un partage constant d'informations** : mutualisation des bonnes pratiques, informations sur les tentatives déjouées…