QUI CONTACTER ?

SERVICES DE POLICE COMPÉTENTS EN MATIÈRE DE FRAUDE BANCAIRE

- **Paris et petite couronne (départements 92, 93 et 94)**

  Brigade des Fraudes aux Moyens de Paiement (BFMP)
  36 rue du Bastion
  75017 PARIS

  Secrétariat **01 87 27 72 00**

- **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 d'alerte ou si vous pensez être victime de fraude, contactez vos interlocuteurs habituels et, en dehors des horaires d'ouverture, écrivez à l'adresse suivante : securite@societegenerale.fr

SOCIETE GENERALE

Banque & Assurances

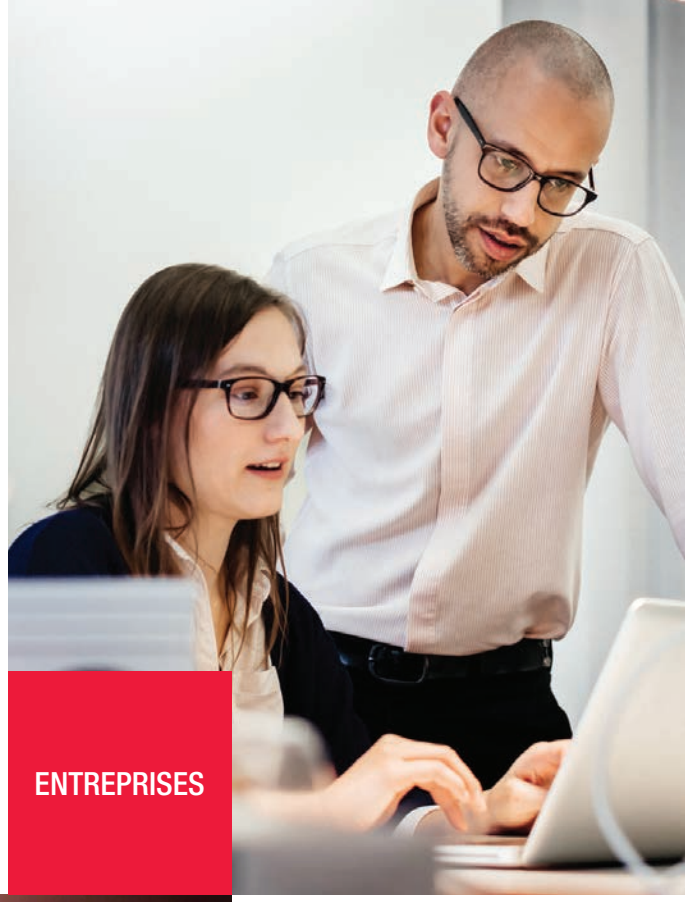
Société Générale - BDDF/DCM/MCO Tour Granite 75886 PARIS CEDEX 18 - S.A. au capital de 1 009 641 917,50 EUR - 552 120 222 RCS PARIS. Siège social : 29, bd Haussmann 75009 PARIS - Crédit photos : GettyImages - SG - Réf : 144057 - 07/2017

papiers Avec Ecofolio tous les papiers se recyclent.

Société Générale, membre fondateur d'Ecofolio, participe au recyclage du papier et a conçu ce document dans le souci d'une incidence minimale sur l'environnement.

LA PRÉVENTION DES FRAUDES BANCAIRES

ENTREPRISES



SOCIETE GENERALE

DEVELOPPONS ENSEMBLE
L'ESPRIT D'EQUIPE

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.

La fraude bancaire

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.

Le caractère souvent international des fraudes bancaires 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. Aujourd'hui, ces attaques se reportent vers les entreprises quelles que soient leur taille et leur activité. Société Générale souhaite sensibiliser ses clients sur ce sujet.

Les mesures de prévention

Les bonnes pratiques de lutte contre la fraude 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 ordres de virement papier ou fax (modalités de transmission des ordres avec lesquelles le risque de fraude est élevé)
- Privilégier les canaux automatisés (Sogecash Net, Sogecash Web, Sogecash SFTP, Sogestel*, Sogestel TS, SWIFTNet,...) en respectant strictement toutes les consignes de sécurité afférentes à ces outils, notamment l'utilisation d'un certificat ou d'un logiciel de sécurité (3Skey, Secure Access...)
- Communiquer, lors d'un rendez-vous avec la banque, les noms, signatures, fonctions et coordonnées des personnes à contacter en cas de doute sur des opérations bancaires

*Assorti du service "Ordre d'Exécution Disjoint" d'une de nos Offres de Banque à Distance.

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, partage constant d'informations

POPULATIONS LES PLUS EXPOSÉES

Trésoriers - Comptables - Personnes agissant sur les moyens de paiement ou susceptibles de communiquer des informations à l'extérieur

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 de fraude bancaire :

FRAUDE AU PRÉSIDENT

Principe

Usurper l'identité du dirigeant d'une entreprise pour exiger d'un collaborateur ayant pouvoir sur les comptes bancaires qu'il effectue un virement frauduleux, en prétextant l'urgence et la confidentialité.

En se faisant passer pour un haut responsable de l'entreprise, l'escroc place le collaborateur en situation de subordination hiérarchique et dispose de puissants ressorts pour manipuler sa victime.

CRITÈRES D'ALERTE

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 TESTS DE VIREMENT

Principe

Se faire passer pour le service télématique d'une banque et prétexter des tests de compatibilité avec l'entreprise cliente pour demander à la victime d'effectuer un virement bancaire.

Pour faciliter la fraude, l'escroc peut suggérer à la victime de lui laisser prendre la main sur son ordinateur. Il utilise alors un site de support informatique permettant de voir tout ce qui se passe sur l'ordinateur distant, voire même d'en prendre le contrôle.

BON À SAVOIR

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.

FRAUDE AU CHANGEMENT DE COORDONNÉES BANCAIRES

Principe

Prétendre un changement de coordonnées bancaires pour diverses raisons (délocalisation, problème de compte, etc.) afin d'obtenir de sa victime qu'elle effectue un virement à l'étranger sur le compte d'un fraudeur.

Via un e-mail à caractère officiel, l'escroc usurpant l'identité d'un fournisseur ou d'un prestataire prétend un changement de coordonnées bancaires pour ordonner un virement frauduleux.

Le fraudeur peut joindre à son mail une facture appuyant sa demande et faisant figurer le nouvel IBAN.
Ce mode opératoire peut également toucher les entreprises locataires de société de gestion immobilière (escroquerie au bail locatif).

TROYENS

Principe

Envoyer un fichier contaminé contenant un cheval de Troie permettant à un pirate d'accéder à votre poste de travail.

Une fois le programme installé sur l'ordinateur, le pirate peut, par exemple, voler vos mots de passe et/ou identifiants, copier des données sensibles, prendre le contrôle du poste de travail pour se connecter à vos outils de banque à distance et exécuter des ordres de paiements, etc.

PHISHING

Principe

Soutirer des informations confidentielles en se faisant passer pour un organisme de confiance : banque, administration, opérateur téléphonique, etc.

Le plus souvent, l'escroc envoie un courrier électronique à un très grand nombre d'internautes incitant à se connecter sur un faux site web pour y fournir des informations.

EN CAS DE DEMANDE INHABITUELLE

1 — **Savoir résister à la pression**

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