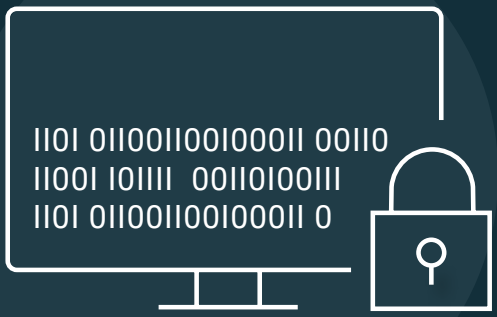
ENTREPRISES

LUTTE CONTRE LA FRAUDE

Prévention de la fraude et sécurisation des transactions

C'EST VOUS L'AVENIR

SOCIETE GENERALE



PRÉVENTION DE LA FRAUDE ET SÉCURISATION DES TRANSACTIONS

Chaque année en France de plus en plus d'entreprises sont victimes de fraude et de cybercriminalité.

En 2018*, ce sont **plus de 7 entreprises sur 10** qui ont subi au moins une tentative de fraude.

Et les conséquences sont souvent dramatiques* : 13 % des entreprises attaquées en 2018 ont subi **un préjudice supérieur à 100 000 €** et pour 5 % d'entre elles, la perte consécutive a dépassé les 500 000 €.

De quoi **fragiliser fortement la trésorerie** des entreprises, **et compromettre leur activité.**

Pourtant, beaucoup d'entreprises ne se sont pas encore dotées d'un budget dédié à la lutte contre la fraude et la cybercriminalité.

C'est la raison pour laquelle, dans ce document, nous vous présentons les cas de fraude les plus fréquents et vous proposons des éléments d'attention pour **mieux sécuriser vos transactions bancaires.**

* Source : baromètre annuel Euler Hermés 2019.

QUELQUES CAS DE FRAUDE CONSTATÉS

FRAUDE AU PRÉSIDENT

Usurper l'identité du dirigeant d'une entreprise pour exiger d'un collaborateur qu'il effectue un virement ne respectant pas les procédures internes, tout en prétextant l'urgence et la confidentialité.

L'escroc dispose de puissants ressorts psychologiques pour manipuler sa victime. Il n'hésite pas à faire intervenir un tiers (faux avocat, faux auditeur...) pour crédibiliser son scénario.

FAUX TESTS DE VIREMENT

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

Pour faciliter l'acte malveillant, l'usurpateur peut suggérer à la victime de lui laisser prendre la main sur son ordinateur. Il utilise alors un site permettant de voir, à distance, tout ce qui se passe sur l'ordinateur ; voire même d'en prendre le contrôle.

FRAUDE AUX CHANGEMENTS DE COORDONNÉES BANCAIRES

Prétendre un changement de coordonnées bancaires afin que la victime effectue un virement sur le compte d'un fraudeur.

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

TROYENS

Envoyer un fichier contaminé contenant « un cheval de Troie » permettant à un pirate d'accéder au poste de travail de la victime.

Une fois le programme installé sur l'ordinateur, le pirate peut voler les mots de passe et/ou identifiants, copier des données sensibles, prendre le contrôle du poste de travail pour exécuter des ordres de paiements, etc.

PHISHING

Soutirer des informations confidentielles en se faisant passer pour un organisme de confiance.

Généralement, l'escroc envoie un courrier électronique à un grand nombre de destinataires les incitant à se connecter sur un faux site web pour y fournir des informations.

QUE FAIRE LORS DE SITUATIONS INHABITUELLES

1. Immédiatement, ne plus valider d'ordres et résister à la pression
2. Fermer temporairement les accès aux outils de saisie et de validation d'ordres
3. Vérifier la légitimité de la demande (contre-appel vers un numéro déjà référencé, toute autre méthode validée par votre entité)
4. Respecter les procédures internes et alerter un responsable

MESURES DE PRÉVENTION À PRENDRE

LIMITER LA DIFFUSION DE L'INFORMATION

- Contrôler la diffusion **d'information sur les sites Internet de l'entreprise**
- N'échanger les documents d'entreprise **que sur des adresses de messagerie professionnelles**
- 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 courrier en-tête 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)

SENSIBILISER LES COLLABORATEURS AUX COMPORTEMENTS APPROPRIÉS

Cela se fait par :

- Le **respect des procédures** opérationnelles et la réalisation des contrôles prévus
- La bonne **compréhension des moyens de sécurité** et de leur utilisation
- La **connaissance des interlocuteurs** (clients, fournisseurs, partenaires)
- L'esprit critique et **l'exercice du droit d'alerte**
- La **valorisation par les managers des tentatives de fraudes stoppées**
- **La vérification de la légitimité des demandes** (par un contre-appel vers un numéro déjà référencé)
- La **remontée d'une demande suspecte** aux collègues et à la hiérarchie

POPULATIONS LES PLUS EXPOSÉES ❯ **Personnes agissant sur les moyens de paiement ou susceptibles de communiquer des informations à l'extérieur (accueil, secrétariat, trésoriers, comptables, etc.).**

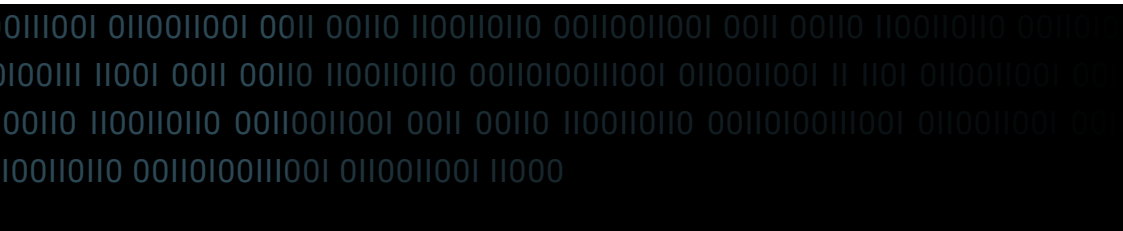
SÉCURISER

LES PROCESSUS ET LES 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
  - s'assurer de l'existence de dispositifs d'**authentification forte** pour les fonctions sensibles
  - ventiler les **actions sur différents canaux** (ordinateur, téléphone mobile...)
- **Mettre en place une répartition des rôles :**
  - **dissocier saisie et validation** des ordres
  - mettre en place une **double signature** en fonction de seuils de montants adaptés à chaque compte
- **Réaliser des contrôles réguliers** (respect des procédures, vérification des comptes…)

LES ÉCHANGES AVEC LA BANQUE

- **Supprimer les virements papier ou fax**
- Privilégier les canaux automatisés en **respectant les consignes de sécurité** relatives à ces outils, notamment l'utilisation d'un certificat ou d'un logiciel de sécurité et la définition des droits des utilisateurs
- Définir des **plafonds de paiements** adaptés
- **Communiquer à la banque les noms, signatures,** fonctions et coordonnées des personnes à joindre en cas de doute sur des opérations bancaires



SÉCURISATION DE VOS VIREMENTS ET PRÉLEVEMENTS

Société Générale vous propose des solutions pour :

1

PRÉSERVER
LA CONFIDENTIALITÉ DE VOS ORDRES DE PAIEMENT

Virement Confidentialité Haute vous garantit la confidentialité de vos ordres de virements SEPA (tels que les salaires, les primes ou toute autre transaction) jusqu'aux relevés de compte et d'opérations. Cette solution innovante **protège vos informations sensibles.**

2

VÉRIFIER
LES DONNÉES BANCAIRES DE VOS PARTENAIRES

Vérification des IBAN via SEPAmail vous permet de vérifier, en des temps de réponse très courts, la concordance entre un IBAN et son titulaire et ainsi de limiter les fraudes aux fausses coordonnées bancaires (usurpation d'IBAN, client indélicat, fraude au faux fournisseur...).
Ce service, développé en collaboration avec les principaux établissements bancaires, couvre 95 % des IBAN des particuliers et entreprises installés en France.

3

VOUS PROTÉGER
CONTRE LES PAIEMENTS INDÉSIRABLES

Payment Protection Solutions sécurise vos virements par des critères que vous définissez (pays destinataires, IBAN bénéficiaires, devise…). Vous vous protégez ainsi contre la perte financière, d'image, de temps dans les démarches, notamment dans celle relative à la récupération des fonds avec un risque d'échec pour cette dernière.

4

CONTRÔLER
LES MANDATS AUTORISÉS

Liste de Mandats Autorisés vous permet de choisir seulement ceux à débiter de votre compte. Vous êtes ainsi protégés contre les prélèvements de petites sommes sous forme d'abonnements débités à tort (téléphonie, décoration florale, cinéma…) qui, une fois cumulées, peuvent représenter des montants plus importants.

POUR ACTIVER CES SERVICES, PRENEZ CONTACT AVEC VOTRE CHARGÉ D'AFFAIRES ENTREPRISES.

QUI CONTACTER EN CAS DE FRAUDE ?

IMMÉDIATEMENT :

- **CONTACTEZ VOTRE CHARGÉ D'AFFAIRES ENTREPRISES.**
- **ENVOYEZ UN MAIL** également à **securite@societegenerale.fr**

DANS LES HEURES QUI SUIVENT, DÉPOSEZ PLAINTE AUPRÈS DES SERVICES SUIVANTS :

- **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)

  36, rue du Bastion
  75017 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)

COMMUNIQUEZ LE DÉPÔT DE PLAINTE À VOTRE AGENCE

À TRÈS BIENTÔT

DANS VOTRE CENTRE D'AFFAIRES
750 Chargés d'Affaires Entreprises

SUR INTERNET
entreprises.societegenerale.fr

SUR LES RÉSEAUX SOCIAUX

@SG_etvous @SocieteGenerale

Société Générale

#AuprèsDesEntrepreneurs

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

SOCIETE GENERALE

Société Générale. S.A. au capital de 1 066 714 367,50 EUR. Siège social : 29, bd Haussmann - 75009 Paris - 552 120 222 RCS Paris - Crédits photos : Getty Image.
Réf. : 144057 - Octobre 2020.