



Fraudes bancaires subies par l'Entreprise : prévention et lutte

PMBA

PECH DE LA CLAUSE
MISSOFFE
DE BELOT
& ASSOCIÉS

- Recrudescence des cyberattaques et des arnaques à l'ingénierie sociale : 12% d'augmentation de transactions frauduleuses entre le premier semestre 2023 et le premier semestre 2024
- 584 M au premier semestre 2024 : montant de la fraude aux moyens de paiement (42% fraude CB)
- 66 M premier semestre 2024 : montant de la fraude par manipulation
- 37% des entreprises ciblées au moins une fois par la fraude au faux fournisseur et par la fraude au président en 2023
- Conséquences souvent graves pour les entreprises touchées

**Chiffres issus du rapport de l'Observatoire pour la sécurité des moyens de paiements*

La Fraude au président



Usurpation d'identité

Un fraudeur se fait passer pour un dirigeant, utilisant une adresse email similaire (ex: p.dupont@entreprise-france.com au lieu de lieu de p.dupont@entreprise.fr) ou usurpant l'identité visuelle de l'entreprise



Création d'un climat d'urgence

L'escroc invoque une acquisition confidentielle, un contrôle fiscal urgent ou un litige juridique imminent nécessitant une action immédiate



Demande de virement

Transfert vers des comptes bancaires situés principalement à Hong Kong, Singapour ou dans les pays baltes



Exigence de secret

Menace de compromettre l'opération ou de licenciement en cas de divulgation, avec une pression exercée avant les week-ends ou week-ends ou congés pour limiter les vérifications

Indices d'alerte et prévention

Adresse email trompeuse

Vérifiez attentivement l'adresse de l'expéditeur qui l'expéditeur qui peut ressembler à l'originale avec avec de subtiles différences
(nom.prénom@entreprise-gouv.com)

Caractéristiques du virement

Soyez vigilant face aux demandes de virement à à l'étranger, vers un compte inconnu, d'un montant montant élevé et inhabituel

Ton inhabituel ou menaçant

Méfiez-vous des messages utilisant un langage langage inhabituel ou créant un sentiment d'urgence excessive

Procédures de sécurité

Formez les équipes, instaurez une double signature signature obligatoire et une validation par appel appel téléphonique direct au président, éviter les les publications sur les réseaux qui facilitent l'usurpation

La fraude au faux fournisseur

Usurpation d'identité

Un fraudeur se fait passer pour un fournisseur habituel de l'entreprise

Détournement du paiement

Le paiement est effectué vers le compte du fraudeur plutôt que celui du véritable fournisseur



Demande de changement

Il demande la modification des coordonnées bancaires (IBAN) pour les prochaines factures

Fourniture de faux documents

Il transmet un RIB frauduleux qui semble authentique

La fraude aux moyens de paiement

Phishing

Emails ou appels imitant l'administration ou un tiers de confiance pour obtenir des informations sensibles ou des paiements

Skimming

Copie de carte bancaire lors d'un retrait ou d'un paiement à l'aide de dispositifs frauduleux installés sur les terminaux

Spear-phishing

Usurpation qualité de collègue ou supérieur afin de récupérer les identifiants de membres du personnel en vue d'accéder au système informatique de l'entreprise

Falsification

Modification de chèques ou d'ordres de virement ou de RIB avec usurpation d'identité

Réagir en cas de fraude

Contact immédiat

Contactez sans délai la banque pour tenter un rappel de fonds avant qu'ils ne soient transférés hors du système bancaire



Sécurisation informatique

Bloquer les accès informatiques suspects et isoler les machines potentiellement infectées pour éviter la propagation

Conservation des preuves

Sauvegarder tous les éléments liés à la fraude : emails, pièces jointes, ordres de paiement, communications



Dépôt de plainte

Porter plainte au commissariat ou par courrier au procureur

Après l'incident, une revue organisationnelle s'impose : audit des processus de paiement, revue des délégations de pouvoirs bancaires, sensibilisation renforcée des équipes. Notification à la CNIL si des données personnelles ont été volées.

Voies de recours

Voie pénale

Plainte contre X :

- escroquerie
- usurpation d'identité numérique
- faux et usage de faux
- accès frauduleux à système informatique
- abus de confiance

Objectif : reconnaissance de la qualité de victime, ouverture d'une enquête, appui au volet civil et assurantiel.

Voie civile - CMF

Art. L. 133-18 à L. 133-24 CMF : en cas de **d'opération non autorisée**, remboursement dû obligatoirement par la banque sauf si elle prouve la négligence grave du client ou démontre le bon fonctionnement du système de sécurité.
Obligation d'alerter sa banque dans un délai de **13 mois**.

Voie civile - autres recours

Responsabilité contractuelle de droit commun :
manquement au devoir de vigilance ou de conseil (art. 1231-1 Code civil)
Action en répétition de l'indu en référés contre le bénéficiaire (art. 1302 C. civ.) si le paiement a été réalisé à tort

Saisie conservatoire : par requête

QUESTIONS/RÉPONSES



PMBA

PECH DE LA CLAUSE
MISSOFFE
DE BELOT
& ASSOCIÉS

PMBA Avocats

10, rue de Richelieu

75001 Paris

01.85.09.19.75

pmbassocies.com

cabinet@pmbassocies.com