Fraude au virement

Comment s'en protéger ?

— **Digitaliser ses processus de contrôle pour déjouer toute tentative de fraude.**

trustpair

7 entreprises sur 10

ont été victimes de fraude en 2018.[1]

1 Étude Euler Hermes - DFCG 2019

Édito.

Au cours des dix dernières années, le nombre de fraudes a été multiplié par deux. Le sujet concerne toutes les entreprises. Cette dynamique s'explique par l'amélioration des techniques de fraude et le peu d'évolution des processus de contrôle.

Le digital a eu un impact extrêmement positif pour les entreprises (automatisation, meilleur prévisionnel et reporting, optimisation du P2P…). Néanmoins, tout le monde ne s'est pas approprié ces technologies pour les mêmes raisons. Des criminels y ont trouvé **l'opportunité de complexifier et massifier leurs techniques de fraude** afin de surpasser les processus de contrôle des entreprises.

Ces processus de contrôle n'ont que très peu évolué ces dix dernières années. Ils sont restés essentiellement manuels et toujours plus lourds et chronophages. Les publications de ces derniers mois témoignent du **retard pris par les directions financières en matière de digitalisation**. Le numérique représente une formidable opportunité pour réinventer le travail du CFO et de ses équipes. La fraude est l'un des risques où **l'utilisation de la technologie n'est plus une option** pour lutter à armes égales contre les fraudeurs.

Les entreprises doivent impérativement réinventer leur façon de prévenir et détecter les fraudes au virement. Des solutions existent, allant du moteur de règles dans les outils, aux initiatives bancaires. Cependant, ces solutions sont insuffisantes pour adresser le risque dans sa globalité.

Demain, l'intelligence artificielle et le machine learning seront utilisés par les fraudeurs. Les moyens de contrôles actuels, essentiellement manuels, ne sont déjà plus tout à fait efficaces et encore moins efficients.

Comment imaginer la tendance dans un contexte de rationalisation des coûts qui exige de faire mieux avec moins sans amélioration des outils ?

Comment faire évoluer vos processus de contrôle pour vous protéger des fraudes au virement ?

C'est précisément l'objectif de ce guide de vous apporter les réponses à ces questions.

Bonne lecture !

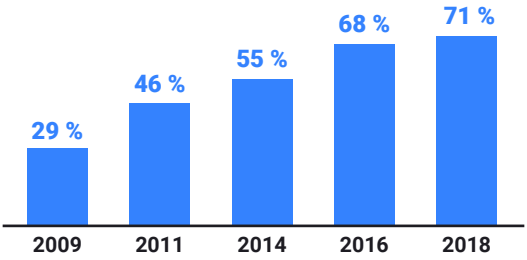
Baptiste Collot
Co-fondateur de Trustpair

1 La fraude évolue

(encore) plus vite que nos entreprises !

La fraude, de quoi parle-t-on ?

Nous ne vous apprenons rien en disant que la fraude ne date pas d'hier. Malgré les mesures de protection prises par l'ensemble des entreprises, les cas de fraude reportés continuent d'augmenter chaque année. Ils sont ainsi passés de 29 % en 2009 à 71 % en 2018 (*PWC Global Economic Crime and Fraud Survey*).



Évolution du taux de fraude reporté au niveau français

La fraude évolue et prend donc de nombreuses formes différentes :

⟶ **Cybercriminalité : piratage informatique**

⟶ **Détournement d'actifs : abus de bien sociaux, fournisseurs fictifs...**

⟶ **Corruption : conflit d'intérêt, délit d'initié...**

⟶ **Fraude aux achats : changement de RIB...**

Et la fraude au virement ?

La fraude au virement est une des conséquences directes de la cybercriminalité, en progression chaque année.
L'intrusion dans les systèmes d'information constitue l'une des 5 grandes attaques subies par les entreprises (28 % selon la dernière étude de la fraude par Euler Hermes). Combinée à d'autres techniques de fraude, le risque peut être critique.

Ces répétitions d'attaques peuvent peser lourd dans le portefeuille des entreprises. En 2018, 13 % des entreprises attaquées ont subi un préjudice supérieur à 100 k€ (contre 10 % en 2017).

Les techniques de fraude évoluent dans le temps.

La fraude a réellement débuté en 2010. À l'époque, la grande majorité des cas étaient liés à la fraude au président.

L'année 2013 marque alors un tournant pour la fraude. Les entreprises ont l'obligation de se mettre à jour pour passer au virement SEPA. Les escrocs s'adaptent alors. La fraude au changement de coordonnées bancaires s'intensifie.

Les changements SEPA sont ainsi une opportunité pour les fraudeurs de se faire passer pour des organismes bancaires et effectuer des virements tests. Sans surprise, l'argent débité ne revient jamais...

Ces évolutions leur ont également permis de récupérer des identifiants (et mots de passe) des comptes bancaires de certaines entreprises. Ils avaient alors la possibilité d'effectuer eux-mêmes des virements, généralement le week-end.

En 2013 et 2014, les escroqueries aux faux ordres de virement atteignent plus de 150 millions d'euros par an (estimation fourchette basse).

— **Thierry Pezennec**
Chef de la section de lutte contre les escroqueries,
à la Direction Centrale de la Police Judiciaire du Ministère de l'Intérieur

Les entreprises ne sont pas équipées pour déjouer les tentatives de fraude.

Une récente étude *(PWC)* souligne l'émergence de nouvelles méthodes de fraude ; la cybercriminalité et les fraudes aux faux fournisseurs gagnent du terrain.

Les cas de cybercriminalité ont plus que doublé au cours des 4 dernières années selon le dernier rapport de PWC - Global Economic Crime Survey 2018. Pour la première fois, ce type de fraude devient le plus signalé devant le détournement d'actifs.

Par ailleurs, elle toucherait pas loin de 6 entreprises du 10. Et si la cybercriminalité n'était que la partie émergée de l'iceberg ?

Les données hébergées par votre entreprise sont stratégiques pour les fraudeurs. En piratant vos serveurs, vos interfaces bancaires et vos échanges fournisseurs, les escrocs préparent les prochaines étapes de leur attaque.

La fraude au virement, par exemple, est très souvent la conséquence d'une cyberattaque préalablement subie par l'entreprise.

Pour être mieux armé face à ces combinaisons de fraudes, les processus humains ne suffisent plus. Aujourd'hui, seules 12 à 20 % des fraudes sont détectées par des processus IT.

Pourquoi ce chiffre est-il si bas ?
Simplement parce que les entreprises peinent à combiner processus humains et outils technologiques.

Aucune entreprise n'échappe à la fraude.

Nos grandes entreprises françaises ne font pas exception à la règle, bien au contraire. Le risque est notamment corrélé au volume d'activité de l'entreprise : **plus le nombre de transactions est important, plus il est compliqué d'assurer un contrôle efficace de flux.**

> *La fraude est une réalité que l'on ne peut pas ignorer. Les fraudeurs sont de mieux en mieux équipés technologiquement, avec des méthodes toujours plus performantes.*
>
> *Compte tenu du nombre de fournisseurs enregistrés et du volume de transactions mensuelles, nous sommes une cible pour les fraudeurs.*

Colin Cesana
Responsable Middle Office Trésorerie, Axéréal[1]

Désormais, nous avons affaire à de véritables organisations criminelles pour qui la maximisation du profit est une priorité. Les plus grosses cibles sont aussi les plus intéressantes lorsqu'une opération réussit.

1 Témoignage client Axéréal

Pourquoi les tentatives de fraude **augmentent-elles si rapidement** ?

La fraude est globale. Elle est même devenue internationale. Aujourd'hui, il n'y a plus de limites géographiques pour ces fraudeurs. La plupart d'entre eux n'opèrent d'ailleurs pas en France, mais fréquemment dans des pays sans extradition.

Mais pourquoi donc la fraude est-elle devenue globale au cours de ces dernières années ?

Il y a deux grilles de lecture à avoir sur ce sujet.

#1. LE DIGITAL N'EST PAS QUE POSITIF.

Il a apporté un nombre incalculable d'opportunités pour toutes les entreprises :

⟶ Une automatisation des tâches

⟶ Des gains de temps sur certains sujets

⟶ Des processus avec des économies d'échelle

⟶ Une accélération des flux notamment financiers et d'information

Malheureusement, tout le monde n'utilise pas ces technologies pour les mêmes raisons. Certains individus (et aujourd'hui des organisations criminelles !) y ont vu des failles et donc des opportunités potentielles de fraude. La fraude se structure et devient professionnelle.

Demain, il faudra faire face à **ces fraudeurs aidés par l'intelligence artificielle.** L'automatisation grandissante de leurs attaques leur permettra d'aller encore plus vite et de toucher plus d'entreprises...

#2. DES CONTRÔLES MANUELS QUI PEINENT À DÉTECTER LA FRAUDE.

Soyons optimistes : des processus de contrôle existent. C'est déjà une très bonne nouvelle car la vigilance humaine demeure essentielle dans un dispositif de lutte contre la fraude.

Toutefois, ces processus restent faillibles. Ils ne sont **malheureusement pas suffisants pour éviter tous les cas de fraude** que l'on voit passer régulièrement dans l'actualité.

La technologie permet aujourd'hui à chaque entreprise de réduire au maximum le risque de fraude pour gagner en assurance et en sérénité. Elle permet une systématisation des contrôles fournisseurs et ce, de façon beaucoup plus approfondie.

Un autre avantage de la technologie est **de rendre hyper efficients les processus de contrôle** qui sont souvent aléatoires et hasardeux. La multiplication des sources de contrôle et les progrès de l'intelligence artificielle rendent les technologies de détection de fraude accessibles financièrement. Les équipes métiers peuvent alors **se concentrer sur les 1 % de cas spécifiques qui nécessitent un regard humain.**

Les prochaines évolutions en matière de fraude : à quoi s'attendre ?

Les fraudeurs maîtrisent parfaitement les dernières technologies. **La fraude s'est professionnalisée et beaucoup d'entre eux n'hésitent pas à prendre le temps de mener des enquêtes approfondies sur leurs cibles potentielles.** Organigramme, test des processus, récupération d'informations clés, ils prennent désormais le temps de mettre en place de vraies stratégies de fraude.

Il y a une dizaine d'années, les tentatives de fraudes ressemblaient plus à des attaques massives où l'objectif était de toucher le maximum d'entreprises.

Dans les prochaines années, ils se concentreront sur un nombre plus restreint d'entreprises pour identifier les failles avec un mode opératoire bien défini et adapté à chaque cible.
Nous continuons d'être dans une ère de transformation numérique, et cela n'est pas prêt de s'arrêter. **Ces évolutions remettent perpétuellement en question la gestion des risques en interne, les processus mis en place** et les solutions de prévention et de détection des fraudes actuellement utilisées.

Intelligence artificielle, machine learning et croisement de données

Au-delà d'un simple effet de mode, le potentiel de ce type de technologie est infini. Sans rentrer dans des détails trop techniques sur ces avancées, l'objectif en matière de lutte contre la fraude est très clair :

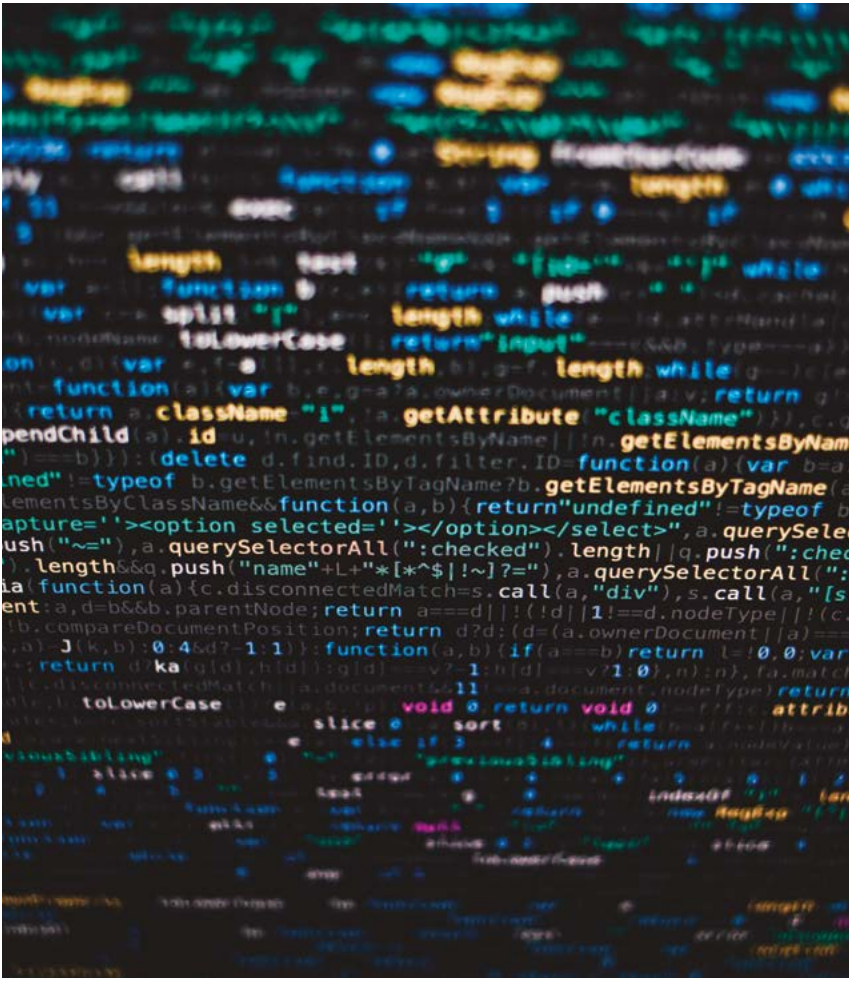
Protéger l'entreprise en déjouant en amont tout risque de fraude.

Le croisement de données est également de plus en plus fréquent dans les solutions technologiques proposées. Encore faut-il que les données récupérées, traitées et analysées soient suffisamment pertinentes.
Quel bénéfice tirer de ces nouvelles méthodes de détection des fraudes ?

Une meilleure maîtrise du risque de fraude est un gain évident de tranquillité pour tout DAF, trésorier ou comptable.

Mais n'oublions pas qu'aujourd'hui, le digital bouleverse le paysage traditionnel que nous avons tous connus ces 20 dernières années à l'échelle de l'entreprise.

En continuant d'appliquer des méthodes d'évaluation des risques et des processus obsolètes qui ne répondent pas aux menaces externes, les entreprises passent à côté de nombreux risques : *confiance interne, réputation externe, perte financière, ralentissement des activités, décrochage du marché…*



La fraude dans l'actualité : il y a des choses à dire.

Facebook et Google se sont fait voler 122 millions de dollars.

Plus une semaine ne passe sans qu'ils ne fassent pas parler d'eux. Cette fois-ci, pour deux cas de fraude.

Entre 2013 et 2015, Evaldas Rimasaukas s'est tranquillement servi dans les comptes de Facebook et Google.

La fraude ? Des fausses factures, envoyées par mail à ces deux géants américains. Sa couverture était une société du nom de Quanta Computer, une entreprise de matériel basée à Taïwan.

Altran : la plus importante cyberattaque de ce début d'année 2019.

L'entreprise de conseil en ingénierie a elle-même reconnu avoir été victime d'une cyberattaque fin janvier. Cet incident grave avait contraint les équipes à déconnecter immédiatement leur système d'information et toutes les applications associées. Dans ce type d'attaque, il est extrêmement difficile d'évaluer l'impact sur les systèmes en place. Les données financières des fournisseurs ont-elles été corrompues ?

Officiellement, aucun vol de données n'a été identifié. Il n'empêche que l'origine de cette nouvelle attaque **serait un simple mail malveillant**, contenant une pièce jointe frauduleuse.

Une cyberattaque de plus contre un géant mondial de l'aluminium.

Il s'agit là de l'entreprise Norsk Hydro. Ce nom ne vous dit peut-être rien et pourtant, c'est l'un des plus gros producteurs d'aluminium au monde.

Comme pour Altran *"cette cyberattaque a considérablement ralenti ses opérations dans plusieurs secteurs d'activité de la société"* a indiqué le groupe.

Cette attaque a touché l'ensemble de son système informatique en cryptant un grand nombre de données. Il s'agit, là encore, du même ransomware qui a touché Altran en janvier dernier.

Une arnaque au faux ordre de virement pour 3 millions d'euros.

L'escroquerie est de taille pour l'entreprise Roxane Nord dans le nord de la France. Cette société produit notamment de l'eau minérale pour Cristaline et Saint-Armand.

Les mails de certains de ses fournisseurs ont été piratés pour demander à l'entreprise d'effectuer les ordres de virement sur un nouveau compte bancaire.

Certaines solutions technologiques auraient pu permettre à Roxane de détecter cette tentative de fraude...

2 Les grands types de fraudes externes en entreprise.

La fraude n'est pas un mythe que l'on se raconte. Elle existe et est de plus en plus difficile à détecter. Les montants sont également loin d'être négligeables : de quelques milliers d'euros, à plusieurs dizaines de millions d'euros !

Ces attaques pèsent sur l'entreprise. Dans une étude publiée par Euler Hermes, les DAF interrogés comprennent que leur trésorerie n'est désormais plus le seul actif mis en danger par les tentatives de fraude.

Si 85 % d'entre eux mentionnent les risques financiers comme principale fraude, la corruption et la fuite des données arrivent en seconde place (45 %), suivi du risque d'interruption de l'activité (30 %) et du risque de réputation (20 %).

Les directeurs financiers et leurs équipes sont aujourd'hui en position de force pour traiter ces sujets stratégiques. Ils sont à même d'apprécier les impacts organisationnels et financiers de ces risques. Leur rôle est aujourd'hui d'arbitrer les investissements en sécurité IT et en couverture des risques.

Quels sont les trois principaux cas de fraude ? Comment les détecter ?
Nous y sommes !

Fraude aux
(faux) fournisseurs.

Une fraude aux fournisseurs commence, dans la plupart des cas, par des échanges de mails (voire de courriers papier). Elle est devenue, ces dernières années, **l'une des fraudes les plus courantes** lorsque l'on parle d'usurpation d'identité.

Un exemple pour comprendre…

Le Directeur Achat de votre entreprise reçoit un email de l'un de vos sous-traitants asiatiques. Suite à des migrations techniques de "comptes", les prochains paiements devront être effectués sur un compte bancaire différent : en Italie.

Votre Responsable Comptable reçoit alors un mail de votre Directeur Achat pour modifier le compte bancaire dudit fournisseur. La demande ayant été transmise par les équipes Achat, vous ne jugez pas nécessaire de faire les contrôles habituels car ils prennent du temps à vos équipes. Dans un cas comme celui-ci, il ne doit pas y avoir de risques. Il n'y a jamais eu aucun problème du côté des Achats.
Plusieurs paiements sont ensuite réglés sur ce nouveau compte sans problème particulier. Quelques mois plus tard, le Directeur Achat prend connaissance d'un mail de son véritable fournisseur lui demandant de bien vouloir régler les 5 dernières factures impayées.

En regardant de plus près, l'email reçu il y a quelques mois pour un changement de compte ne correspond pas tout à fait à son véritable sous-traitant.

C'est trop tard.

Certains indices doivent vous alerter

⟶ Un changement de compte bénéficiaire doit toujours être considéré comme potentiellement suspect

⟶ Un changement de coordonnées d'un fournisseur est à risque, d'autant plus lorsqu'il s'agit de compte à l'étranger.

⟶ L'adresse email : elle peut ressembler, à quelques lettres près, à l'adresse email de votre véritable fournisseur.

⟶ Le contenu du mail et le ton employé sont-ils différents de d'habitude ?

Les questions à se poser

⟶ L'adresse mail et la signature correspondent-elles aux informations à votre disposition ? Comparez-les avec de précédents échanges.

⟶ Avez-vous pris le temps de déclencher la procédure habituelle ? Contre-appel ou vérification des nouvelles coordonnées grâce à un outil dédié ?

La cyberfraude
(ou ransomware).

On parle généralement de fraude au virement par **malware ou phishing bancaire**. **Moins répandue que les autres,** cette fraude efficace et dangereuse est amenée à progresser dans les années à venir : **il est nécessaire de se préparer à contrer ce type d'attaques dès maintenant. Les techniques utilisées sont généralement très sophistiquées.**

Un exemple pour comprendre…

Un de vos collaborateurs du service comptabilité reçoit un email de l'un de ses fournisseurs avec pour objet "Facture" ou "Invoice". Sans surprise, le mail contient en pièce jointe un document "Facture".

Le comptable ouvre la pièce jointe. Sans le savoir, il vient de déclencher l'installation d'un logiciel malveillant (*malware*). L'ordinateur peut désormais être contrôlé à distance.

La liste des contacts clients, fournisseurs, ainsi que l'ensemble des adresses mails et données sensibles sont ainsi récupérées. Les fraudeurs peuvent également en profiter pour envoyer de nouveaux mails frauduleux sous couvert du nom de votre entreprise.

Certains vont encore plus loin en créant de fausses pages de site de paiement. Les codes de validation renseignés sont ensuite enregistrés pour effectuer des virements frauduleux dans les jours ou les semaines à venir.

Certains indices doivent vous alerter

⟶ Un email inhabituel, même d'un de vos fournisseurs connus.

⟶ L'adresse mail de votre fournisseur n'est pas la même que d'habitude.

⟶ Incohérence du contenu du mail : le ton, le vocabulaire et la nature de vos échanges vous surprennent.

⟶ Des lenteurs sur votre site de paiement bancaire.

⟶ Une page de validation de paiement bancaire inhabituelle. Par exemple, une page vous demande de confirmer votre code, alors qu'aucune action de votre part ne vous y contraint.

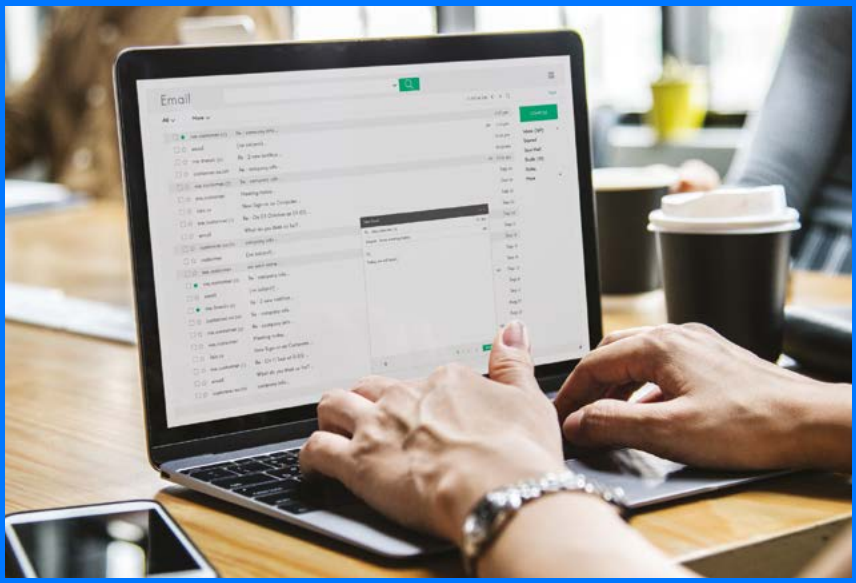
Les questions à se poser

⟶ Connaissez-vous l'expéditeur ? Vous attendiez-vous à recevoir une nouvelle facture à ce moment-là ?

⟶ Le titre de la pièce jointe est-il habituel ?

⟶ Votre système d'exploitation et votre navigateur internet sont-ils à jour ?

⟶ Votre base clients et fournisseurs est-elle protégée par un accès sécurisé ?



La fraude au **président.**

L'arnaque au faux président fait partie des FOVI, ces **escroqueries aux Faux Ordres de Virement Internationaux**.

Cette fraude est bien connue, et pourtant, peu d'entreprises s'en protègent réellement. Avec 2 300 plaintes déposées en moins de 5 ans, elle représente à elle seule près de 23 % des tentatives de fraudes. Cette menace ne concerne désormais plus seulement les grands groupes.

Un exemple pour comprendre…

Le principe est très simple : le fraudeur appelle un salarié en se faisant passer pour l'assistant ou le bras droit du Directeur de l'entreprise.

Il lui explique qu'il doit envoyer un virement urgent et confidentiel de 550 000 € pour finaliser l'acquisition d'une nouvelle entité à l'étranger. Cette opération est stratégique et le timing est très serré.

Le fraudeur demande ensuite des informations sur les procédures de paiement de l'entreprise en expliquant que les virements depuis l'étranger ont déjà été validés par le Directeur *(actuellement en vacances, cela tombe mal…)*. Le bordereau de virement sera signé par le fraudeur qui reproduira la signature du PDG *(facilement accessible dans votre dernier rapport annuel)*.

Le virement de plusieurs centaines de milliers d'euros vient maintenant de partir.

Certains indices doivent vous alerter

⟶ Un interlocuteur que vous ne connaissez pas et qui ne devrait pas vous appeler.

⟶ L'urgence de la situation et son caractère extrêmement confidentiel.

⟶ La flatterie : *"Monsieur Dupont, notre Directeur m'a demandé de vous appeler directement car nous pouvons vous faire entièrement confiance"*.

⟶ L'intimidation : *"C'est extrêmement urgent. Je ne veux pas perdre de temps. Charles, notre Directeur, ne serait pas content que l'opération échoue pour une question de délai"*.

Les questions à se poser

⟶ Avez-vous l'habitude de traiter ce genre de sujets ?

⟶ Avez-vous l'autorisation d'effectuer des virements à l'étranger ?

⟶ Quelle genre de communication entretenez-vous avec vos supérieurs ?

⟶ Les procédures spécifiques pour les virements internationaux sont-elles respectées ?

⟶ Votre interlocuteur est-il au fait de ces informations ?

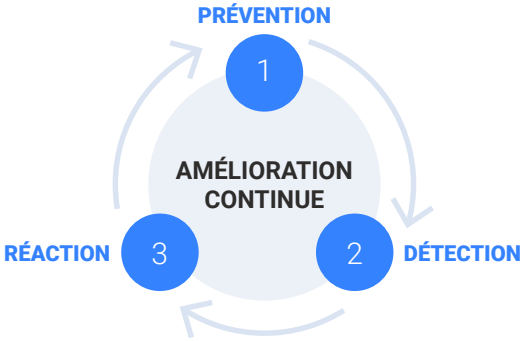
3 Des méthodes simples

pour déjouer
tout risque de fraude.

Nous préférons insister de nouveau : la fraude n'arrive (*malheureusement*) pas qu'aux autres. **Les pirates tentent moins d'attaques, mais avec un meilleur taux de réussite** et donc une augmentation des fraudes du côté des entreprises.

Il n'y a **pas de recette miracle pour lutter contre la fraude**. Les efforts des entreprises pour déjouer ces risques doivent être permanents et se perfectionner à mesure que la fraude se complexifie.

Chez Trustpair, nous avons identifié **trois phases clés dans la lutte contre la fraude** :



Prévention :
entre éducation et dimension technologique.

La dimension éducative est extrêmement importante ici.

Dans l'exemple d'une fraude au président, un aspect psychologique entre en jeu. Sans une prévention des risques liés à ce type de fraudes, il est très facile de ne pas la détecter. C'est humain.

Un supérieur hiérarchique vous demande de ne pas appliquer les procédures habituelles *"pour le bien de l'entreprise"*. Lorsque des instructions viennent du top-management, il n'est pas évident d'aller contre sa demande sous prétexte des procédures déjà en place.

Il y a donc un **véritable travail d'éducation de tous les collaborateurs**, et pas seulement du top-management. Ces aspects doivent être abordés le plus simplement possible :

- ⟶ Les types de fraudes
- ⟶ Leurs risques
- ⟶ Les différentes manières de les détecter
- ⟶ Les procédures à mettre en place

Vous pourriez même commencer par partager ce livre blanc à l'ensemble de l'entreprise (*merci !*).

La fraude n'est pas une honte. C'est important de le dire. Les entreprises doivent apprendre à libérer la parole en interne, et ce n'est malheureusement pas toujours le cas.

Une pratique que l'on recommande à nos clients est de communiquer sur d'éventuels retours d'expérience (*fraudes ou tentatives*).

> ***Nous avons eu au cours du dernier trimestre 3 tentatives de fraudes et une fraude avérée. Les types de fraudes étaient les suivants. [...] Nous les avons déjouées de cette façon [...], grâce à des procédures internes [...]. Soyez vigilants au quotidien dans vos communications en externe, comme en interne.***

La sensibilisation par l'exemple concret aura beaucoup plus d'impact sur vos collaborateurs. Ces cas d'usage peuvent prendre différentes formes :

- Dossier de quelques pages
- Newsletter interne
- Infographie
- Interview

Vos collaborateurs doivent aussi se former à ces sujets. **La répétition de l'information est clé.**

Le sujet de **la fraude n'est pas toujours sexy** lorsque l'on s'adresse à d'autres départements : marketing, commercial, service client... Et pourtant, vous connaissez l'importance de sensibiliser l'ensemble de l'entreprise.

Utilisez des supports ou des outils ludiques :

- bandes dessinées
- dispositif de e-learning
- études de cas interactives
- mises en situation
- vidéos

Au-delà de la formation et de l'éducation de vos équipes, il est important **d'accompagner la prévention du risque avec des outils technologiques.**

L'essor du digital doit permettre d'améliorer la détection des risques. Il y a une dizaine d'années, aucune vérification ne pouvait être automatisée. Aujourd'hui, les technologies permettent d'automatiser facilement les contrôles et la détection de cas de fraude.

Des solutions existent pour ramener de la technologie et de l'automatisation dans des processus de contrôles traditionnellement humains. **Ces outils sont généralement connectés à vos solutions déjà en place.** Ils scannent toutes les informations liées à vos fichiers de paiement et à votre référentiel fournisseurs pour **remonter automatiquement les anomalies éventuelles.**

Vous souhaitez lutter à armes égales avec les fraudeurs ?

Équipez-vous enfin d'outils technologiques pour prévenir tout risque. C'est la seule solution pour lutter efficacement contre ces tentatives de fraude. Ils utilisent eux-mêmes les dernières technologies, pourquoi pas vous ?

En résumé : **Éducation de vos équipes et processus de contrôle automatisé**

La détection,
plus que jamais stratégique.

La détection du risque de fraude commence par **deux bonnes pratiques essentielles et simples à mettre en place :**

UNE SÉPARATION DES TÂCHES EST INDISPENSABLE.

C'est le cas dans la quasi-totalité des grands groupes, mais ce n'est toujours pas la norme dans les entreprises de plus petite taille (*parfois jusqu'aux ETI*).

Dans la mesure du possible, **les tâches de saisie et de paiement doivent être effectuées par deux personnes différentes**, ou au minimum validées par un tiers.

LA VALIDATION DES FICHIERS DE PAIEMENT

Chaque entreprise porte la responsabilité de ses instructions de paiement. Vos partenaires bancaires peuvent mettre en place des outils de contrôle et porter une attention particulière à certains flux exceptionnels. Ils n'ont toutefois aucune obligation de résultat, la responsabilité de vérifier les paiements repose sur l'entreprise émettrice.

Il est donc primordial de systématiser ces contrôles en interne pour limiter tout risque sur vos paiements. Des solutions dédiées peuvent vous aider à gagner en sérénité sur ce sujet-là.

Les processus humains ne sont pas infaillibles.

Nous en avons parlé dans les premières pages de ce livre blanc : les tentatives de fraude se sont complexifiées. Nous n'avions pas encore abordé la question des processus de contrôle. Ces derniers n'ont pas (*ou très peu*) évolué au cours de ces dernières années.

Très peu de processus ont été digitalisés pour faire face à ces menaces.

La principale cause de la fraude est généralement liée au référentiel fournisseurs de votre entreprise.

Lorsque nous démarrons un premier audit fournisseur chez nos clients, le constat est sensiblement le même à chaque nouvelle intervention :

30 à 50 % des données présentes dans les bases fournisseurs sont erronées.

Ces erreurs peuvent être liées à des doublons, des comptes fournisseurs mal associés ou fermés, ou encore des sociétés en liquidation judiciaire.

Mais au-delà des erreurs bien présentes, ce chiffre témoigne d'une chose : **les entreprises, quelles qu'elles soient, ne maîtrisent pas leurs données fournisseurs.**

Et c'est probablement votre cas. Heureusement, tout se corrige et s'améliore !

Comment expliquer cette perte de contrôle de la donnée en interne ?

La première raison est la multiplication des données. La data n'a jamais été aussi présente, à tous les niveaux de l'entreprise.

> *La volumétrie de données n'a jamais été aussi importante qu'aujourd'hui. Les processus manuels actuellement en place ne permettent pas d'adresser efficacement le problème avec un risque de perte très important. En parallèle, les équipes en charge de ces contrôles se réduisent...*

— **Baptiste Collot**
CEO, Trustpair

Des lenteurs dans le processus

La vérification manuelle des fournisseurs est chronophage et faillible.

Prenons un exemple.

Vous souhaitez ajouter un nouveau fournisseur dans votre référentiel. Aujourd'hui, des contrôles manuels existent dans votre entreprise : contrôle des données juridico-légales, contre-appels, échange d'emails avec vos contacts de référence pour garantir l'exactitude de ses informations bancaires, demande de RIB certifiés...

En moyenne, ce **type de procédure prend 15 minutes**, pour chaque fournisseur.

15 minutes pour vérifier l'exactitude des informations d'un fournisseur. En 2019.

Pourquoi ? Parce qu'aucune solution digitale n'est déployée pour automatiser ce travail sans plus-value particulière.

Des solutions existent pour vous accompagner dans cette problématique. Trustpair en fait partie.

Chez Trustpair nous permettons à nos clients la validation instantanée d'un fournisseur en vérifiant l'identifiant de l'entreprise (SIREN, TVA...) et ses coordonnées bancaires associées (IBAN notamment).

Parenthèses refermées, avec cet exemple, nous avons voulu vous montrer **les limites des contrôles manuels**, mises en perspective avec des outils digitaux développés ces dernières années.

Des processus à digitaliser d'urgence

Les processus de contrôle doivent donc être revus, améliorés et digitalisés.

Plus simple à dire qu'à faire.

La première réponse que nous pouvons vous apporter se trouve du côté des éditeurs de logiciels.

Les processus manuels ne suffisent plus à déjouer les tentatives de fraude. À ce propos, la majorité des fraudes a lieu sur des périodes creuses pour l'entreprise :

- → Pause déjeuner
- → Week-end
- → Période de vacances

Les collaborateurs sont généralement moins vigilants ou simplement absents.

Une solution technologique doit donc faire partie de vos processus, côté fournisseurs. **Trois étapes sont particulièrement stratégiques :**

- → Le contrôle des nouveaux RIB
- → La maintien à jour des informations (bancaires) de vos fournisseurs
- → Le paiement de vos fournisseurs

Ces solutions doivent permettre de s'adapter à votre contexte, à vos habitudes. C'est pourquoi certains éditeurs associent machine learning, data mining ou encore intelligence artificielle. Ils sont tendances, mais ne résoudront pas tous vos challenges autour de la fraude.

Beaucoup d'éditeurs de logiciels proposent aujourd'hui des solutions plus ou moins performantes. Mais il existe encore trop peu de solutions faciles à prendre en main, intuitives et rapides à déployer.

La technologie au service de vos collaborateurs. Et non l'inverse.

Parler d'intelligence artificielle et de machine learning à certains de vos collaborateurs n'améliorera pas vos contrôles pour autant. Vos équipes n'ont pas à se préoccuper de ces sujets, il leur faut avant tout des outils faciles à prendre en main pour qu'ils puissent être adoptés (et utilisés !) le plus rapidement possible.

3 questions pour Thierry Pezennec,

Chef de la section de lutte contre les escroqueries, à la Direction Centrale de la Police Judiciaire du Ministère de l'Intérieur

#1. Comment fait-on alors pour diminuer ces attaques et tentatives de fraude ?

La répression est une chose, mais elle est difficile. Les auteurs anonymisent leurs attaques.

L'accent a été porté (*et continue de l'être*) sur la prévention auprès des banques et des entreprises. Lorsqu'un nouveau modus operandi apparaît, c'est notre rôle à tous de communiquer et de partager l'information auprès des associations et des fédérations du secteur (*CDSE, AFTE, MEDEF…*).

La fraude peut avoir de graves conséquences d'un point de vue financier, mais aussi humain. J'ai par exemple constaté de nombreuses entreprises, bailleurs sociaux ou associations en grande difficulté de trésorerie après ce type d'escroquerie.

Un des cas marquants fut celui d'une entreprise, victime d'une fraude au changement de RIB d'environ 1,6 millions d'euros, en 2016. Les conséquences furent dramatiques : une liquidation judiciaire et 44 personnes au chômage.

D'un point de vue humain, certains comptables ou responsables financiers sont traumatisés d'avoir pu se faire berner de la sorte. J'ai en mémoire le cas d'un comptable qui n'avait pu supporter les faits commis sous l'emprise d'un escroc et avait mis fin à ses jours.

Les actions de sensibilisation existent. Elles ont permis de réduire les cas de fraude avérée, mais ce n'est pas encore suffisant. Il faut aller plus loin.

#2. Comment les fraudeurs sont-ils organisés aujourd'hui ?

Il existe deux principaux groupes criminels.

Le premier, situé en Israël, composé principalement de quelques dizaines de personnes d'origine franco-israélienne, agit par téléphone et mail. La coopération avec les autorités judiciaires israéliennes est primordiale et intense, permettant ainsi de démanteler des groupes organisés.

Le second est basé au Nigéria. Ces personnes réussissent à s'immiscer dans les échanges de mails (toujours en anglais) entre le client et le fournisseur par l'utilisation de malwares. La difficulté principale réside dans l'identification précise de l'origine des attaques.

Plus de 80 % des cas de fraudes abouties en 2018 concernaient des changements de coordonnées bancaires fournisseurs. Les escrocs récupèrent ainsi les factures côté fournisseur en se faisant passer pour le client. Puis, par une démarche inverse, ils prennent attache avec le client en se faisant passer pour le fournisseur, factures à l'appui. Ils indiquent alors une modification des coordonnées bancaires et fournissent à l'appui un nouvel IBAN de la société fantôme précédemment créée à l'étranger.

Depuis maintenant un an, **les virements se font aussi sur des comptes bénéficiaires français avant d'être transférés à l'étranger.** Derrière certains de ces comptes bancaires français, la société est bien réelle, l'escroc propose une commission sur un virement qui va arriver sur le compte de l'entreprise. Sur d'autres comptes bancaires français, notamment ceux détenus par les néobanques, la société (une coquille vide) est gérée par un homme de paille qui, contre une rémunération, accepte de fournir des documents administratifs pour faciliter l'ouverture de ces derniers. À l'issue, il transmet les identifiants et mots de passe à un tiers, complice des escrocs.

#3. Un dernier mot sur la prévention et la lutte contre la fraude ?

La prévention est au cœur de la lutte contre la fraude. Des actions doivent être répétées régulièrement. Les méthodes utilisées par les fraudeurs changent au gré de l'évolution des processus de contrôle mis en place au sein des entreprises.

La technologie, je pense notamment à l'intelligence artificielle, doit aussi être au service de la prévention. C'est cette **combinaison gagnante de technologie et de processus humain qui permettra de diminuer drastiquement les cas de fraude avérée.**

Réaction :
que faire en cas de fraude ?

Il y a deux situations à prendre en compte :

⟶ une fraude avérée

⟶ une tentative de fraude

Cas n°1 : Fraude avérée

L'enjeu ici est d'agir vite pour éventuellement éviter le transfert de fonds de votre banque vers celle du fraudeur. Vous pouvez ainsi recourir au recall, pour obtenir un retour des fonds.

Qu'est-ce que le recall d'un virement ?

Cette procédure vous permet de demander à votre banque d'annuler un virement bancaire pour obtenir la restitution des montants versés. Elle est **possible en cas de fraude**.

Si l'ordre de virement n'a pas encore été exécuté par la banque, vous devez la contacter au plus vite afin d'annuler un virement SEPA. C'est une course contre la montre. C'est d'ailleurs pour cela que les cas de fraude ont lieu en fin de semaine. Les délais d'action sont généralement de 48h avant que les fraudeurs ne transfèrent l'argent sur une multitude d'autres comptes bancaires.

Une fois l'ordre exécuté, il est toujours possible pour vous de récupérer les sommes indûment payées, mais les procédures sont bien plus complexes :

⟶ **Législation différente** en fonction du pays de la banque du bénéficiaire

⟶ **Provision nécessaire** sur le compte bancaire du fraudeur. Les sommes transitent très rapidement.

⟶ **Virement dans la zone SEPA** exclusivement (*espace économique européen*)

La phase *"réaction"* doit très vite être bouclée par de nouvelles actions de prévention. Partager l'information en interne - le scénario et les conditions dans lesquelles s'est déroulée cette fraude - est une première étape vers une nouvelle campagne de prévention.

Cas n°2 : Tentative de fraude

Dans le cadre d'une tentative de fraude, lorsque l'un de vos collaborateurs a un doute, il se doit de faire remonter l'information. Mieux vaut parfois perdre quelques heures plutôt que plusieurs centaines de milliers d'euros, non ?

Une fois de plus, partagez l'information entre les équipes. Une bonne pratique que nous avons observée chez nos clients est de prévenir vos collègues dans d'autres entreprises. **Certaines campagnes de fraudes sont *"simplement"* répliquées** dans plusieurs entreprises.

En partageant les techniques utilisées, les templates de mails et le mode opératoire, vous pouvez prévenir d'autres DAF, trésoriers ou collaborateurs des équipes Trésorerie et Comptable.

Gouvernance des données et gestion des processus : le rôle du DAF et de ses équipes.

Cette boucle *prévention - détection - réaction* doit être pilotée par le DAF avec le relais du Directeur Trésorerie et du Directeur Comptable.

Notre analyse du rôle du DAF aujourd'hui et de ce qu'il devra être demain est aussi applicable (*dans une moindre mesure*) à toutes les personnes que l'on vient de citer.

Les fonctions du Directeur Financier ont bien évolué, à commencer par sa place dans l'entreprise. Longtemps tenu à son rôle de financier, sa fonction s'est largement étendue ces dernières années.

Les données se multiplient, les demandes de reporting par la même occasion. **Le DAF occupe désormais une place plus centrale**, en partageant de l'information à tous les niveaux, pour toutes les équipes.

Un rapport d'Accenture synthétise le rôle du DAF comme suit :

> ***Le Directeur Financier se rapproche fortement de celui d'architecte de la valeur de l'entreprise. Il lui faut désormais piloter la croissance et gérer la complexité, tout en maîtrisant les coûts.***

Mais qu'attend-on, concrètement, du DAF aujourd'hui, sur des sujets de fraudes ?

Le DAF : garde-fou et early adopter de nouvelles solutions technologiques

Tout investissement ou achat de nouveaux outils logiciels passent à un moment ou à un autre dans les mains du Directeur Financier. Il joue donc **un rôle moteur de conseiller stratégique** lorsqu'il s'agit de tester une nouvelle solution logicielle dans le cadre de la lutte contre la fraude (*par exemple… !*).

Le DAF prend de la hauteur.

Le Big Data, tendance il y a quelques années, a permis d'apporter une nouvelle dimension au reporting. Cette analyse plus fine des projets doit lui permettre de prendre de meilleures décisions sur la meilleure manière d'**améliorer les processus** (*financiers*), d'allouer les bonnes ressources au bon endroit selon les points de faiblesse de l'entreprise.

Pour finir.

La fraude se complexifie et devient de plus en plus technologique. Les fraudeurs ont compris comment bénéficier des technologies pour réaliser des escroqueries de plus en plus sophistiquées et ciblées. Les processus de contrôle en place ne sont plus adaptés pour déjouer les tentatives de fraude.

La réponse des entreprises se doit d'être technologique ! La perte liée à la fraude ne devrait pas faire partie du quotidien des entreprises. N'attendez pas qu'il soit trop tard pour agir.

Assurer un contrôle exhaustif et manuel des données fournisseurs et de paiement est impossible compte tenu du volume de données et de l'ensemble des missions des directions financières. **Une nouvelle collaboration s'ouvre alors entre les directions financières, les DSI et des partenaires externes.**

Et maintenant ?

Trustpair accompagne les ETI et grands groupes dans le contrôle des coordonnées bancaires de leurs fournisseurs pour les protéger des fraudes au virement.

La solution a été imaginée par un ancien trésorier confronté au manque d'efficacité des solutions existantes. Trustpair couvre l'ensemble de la chaîne de paiement avec le contrôle automatique des RIB fournisseurs, l'audit en continu de la base tiers et la vérification des paiements.

Grâce à Trustpair, les directions financières peuvent digitaliser leurs contrôles avec un gain de temps et de sécurité significatif.

Visitez www.trustpair.fr pour en apprendre plus sur la solution et découvrir des témoignages clients.

trustpair

Grande Arche de la Défense
1 Parvis de la Défense
92800 Puteaux

+33 1 84 88 87 23
contact@trustpair.fr
www.trustpair.fr