Fraude en Entreprise : Perspectives et Stratégies pour 2024

trustpair | SAP

Sommaire

Avec la participation de :

Baptiste Collot, CEO, Trustpair
Slim Trabelsi, Senior Security Architect, SAP

Méthodologie :

- Sondage diffusé par OpinionWay
- Date de sondage : du 06/12/23 au 20/12/23
- Répondants : 151
- Localisation : France
- Ciblage : DAF et responsables trésorerie d’entreprise de plus de 250 salariés

Introduction

2024 marque un tournant dans la lutte contre la fraude pour les entreprises françaises. Avec 64% des sociétés victimes d'au moins une tentative de fraude en 2023 - soit une augmentation de 28% par rapport à 2022 - le phénomène gagne en ampleur, et en dangerosité. Loin de se limiter à des conséquences financières, **la fraude peut avoir des effets en cascade** sur la réputation de l'entreprise et ses relations commerciales. Jusqu'a impacter son activité et chiffre d'affaires.

Ces tendances alarmantes soulignent une réalité inquiétante : la fraude est plus sophistiquée et maintenant bien ancrée dans une "cyber ère". Phishing, hacking, IA, ChatGPT… Les fraudeurs utilisent des technologies de pointe et leurs attaques sont indétectables sans les moyens de prévention adéquats. 55% des entreprises ont d'ailleurs vu une augmentation des cyberfraudes ces 12 derniers mois. Un double enjeu se pose alors pour les entreprises : **protéger leurs systèmes contre les cyberattaques** et prévenir les effets dévastateurs de la fraude.

Face à l'ampleur de la menace, les entreprises ont conscience des risques mais peinent à s'équiper en conséquence. Si elles sont nombreuses (84%) à multiplier les formations dédiées à la cybersécurité, elles sont aussi beaucoup à privilégier des méthodes de prévention manuelles (email, appel téléphonique, etc.). Face à la sophistication des fraudeurs et de leurs techniques, **seules les solutions automatisées peuvent contrer la menace**.

Ce rapport met en lumière le nouveau visage de la fraude, ses principaux enjeux, ainsi que les stratégies à mettre en place pour éradiquer le phénomène en 2024.

> **Les fraudeurs s'adaptent constamment : ils apprenent à contourner les règles de prévention et les barrières antispam. Ils trouvent des failles en s'aidant de l'IA, qui finalement est à double tranchant. Nous nous en servons dans le cadre de notre travail mais eux aussi s'en servent pour infiltrer nos systèmes.**

Slim Trabelsi
Senior Security Architect
SAP

#1 La fraude en 2024, un fléau qui s’intensifie

1

64%

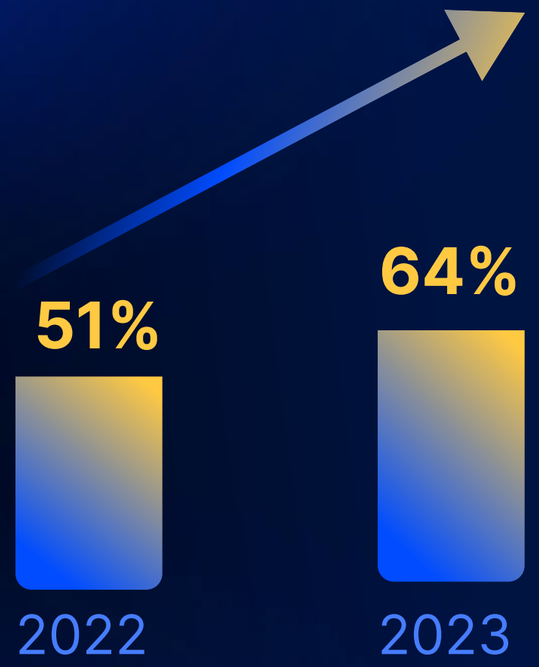
des entreprises françaises ont subi au moins une tentative de fraude en 2023

59%

ont subi plusieurs tentatives

28%

Cela représente une hausse de 28% par rapport à 2022



Questions & répondants :
1,2,3. Par combien de tentatives de fraude au virement votre entreprise a-t-elle été ciblée en 2023 ? Répondants : 151

ANALYSE

En 2023, la fraude a frappé les entreprises françaises comme jamais auparavant. 64% d'entre elles ont été ciblées au moins une fois, 59% plusieurs fois. Cela représente une hausse considérable de 14 points par rapport à 2022. Ce bond significatif des attaques peut s'expliquer par plusieurs facteurs : **des fraudeurs plus sophistiqués et organisés et une hausse conséquente des cyber fraudes**, plus difficiles à détecter que les fraudes "classiques". Les fraudeurs s'appuient par exemple sur l'IA pour générer rapidement des emails de phishing plus convaincants. 52% des tentatives de fraude étaient liées à des cyberattaques.

Cette escalade s'accompagne d'une intensification des attaques contre les grandes entreprises de plus de 1 000 salariés. Celles-ci sont 69% à avoir été victimes d'au moins une tentative de fraude et 63% victimes de plusieurs tentatives. Il n'y a rien d'étonnant à cet écart. Les grands groupes manipulent plus de fonds et ont souvent des systèmes et process plus complexes et internationaux qui ouvrent la voie aux fraudeurs.

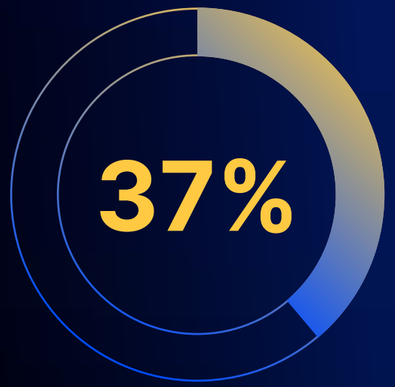
> **Il y a un vrai changement d'échelle de la fraude : une industrialisation et une spécialisation des attaques. Aujourd'hui, la fraude est presque devenue un service. Sur le Dark Web, elle est proposée comme un outil clé en main à des fraudeurs professionnalisés et organisés.**

Slim Trabelsi
Senior Security Architect
SAP

trustpair

#2 Un phénomène plus dangereux aux séquelles nombreuses

1



des entreprises ont subi au moins une fraude aboutie

2

55%

des entreprises ont perdu en moyenne plus de

50.000€

par fraude aboutie

3

28%

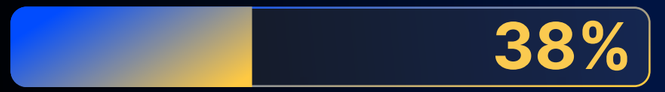
des entreprises se disent prêtes à mettre fin à une collaboration si le partenaire ou prestataire était victime de fraude

4

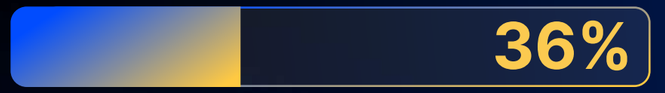
En plus des pertes financières, les entreprises craignent :

une discontinuité de l'activité

des conséquences réglementaires



et une réputation ternie auprès des clients



Questions & répondants :

- 1. Combien de ces tentatives de fraudes ont abouti (que les fonds aient été récupérés ou non) ? Répondants : 151
- 2. Quelle était la perte financière moyenne par fraude aboutie ? Répondants : 61
- 3. Continueriez-vous de collaborer avec une entreprise si elle était victime d'une fraude aboutie et perdait votre paiement ? Répondants : 151
- 4. Au-delà des pertes financières, quels sont les impacts de la fraude qui vous inquiètent le plus ? Répondants : 151

ANALYSE

Si elle gagne en fréquence, la fraude gagne aussi en dangerosité : elle aboutit plus fréquemment et a des conséquences variées. 37% des entreprises ont subi au moins une fraude aboutie en 2023, ce qui représente un bond de 14 points par rapport à 2022. Pour 57% des entreprises ciblées en 2023, au moins une tentative de fraude a abouti. En cause ? **Une fraude plus digitale et complexe à détecter.** Les pertes financières aussi, augmentent, avec une perte moyenne de plus de 50.000€ par fraude pour plus de 50% des entreprises.

Mais les conséquences financières sont loin d'être le seul impact redouté par les organisations. Près de la moitié d'entre elles (45%) craint une discontinuité dans l'activité suite à une fraude, suivie de près par des conséquences réglementaires et de conformité (38%) et une réputation ternie auprès des clients (36%).

Ces craintes sont loin d'être infondées : une fraude réussie a généralement des effets en cascade pour l'entreprise. **L'impact réputationnel peut aisément se répercuter sur les fournisseurs et investisseurs**, menaçant la relation de confiance, voire l'activité commerciale. D'ailleurs, près d'une entreprise sur trois se dit prête à envisager de mettre fin à une collaboration si son partenaire ou prestataire était victime de fraude.

trustpair

> **La cyberfraude est plus complexe à identifier et reste plus longtemps non détectée. Les montants perdus sont donc généralement plus importants.**

Baptiste Collot
Co-fondateur et CEO
Trustpair

#3 La fraude au RIB, point d'orgue de la menace

1

49%

des entreprises ciblées ont été victimes de **fraude au RIB**

37%

de fraude au **faux fournisseur**

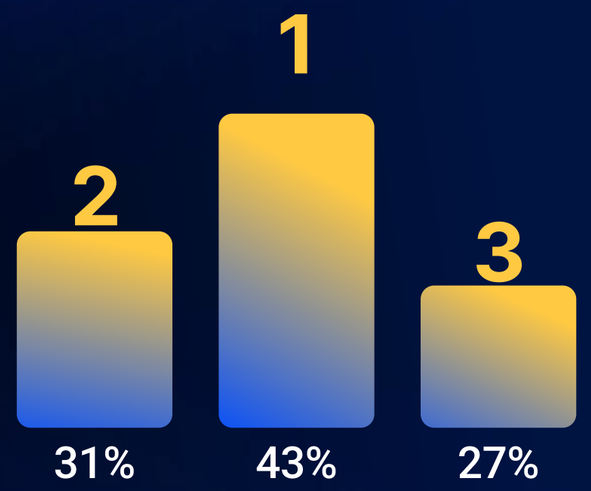
37%

de **fraude au président**

2

Les méthodes de paiements utilisées par les entreprises victimes de fraude :

1 virement classique
2 prélèvement SEPA
3 paiement par carte



Questions & répondants :

- 1. De quel(s) type(s) de tentative(s) de fraude votre entreprise a-t-elle été victime ? Répondants : 100
- 2. Concernant les fraudes abouties, quelle(s) étai(en)t la(les) méthode(s) de paiement utilisée(s) ? Répondants : 61

ANALYSE

En 2023, la fraude au RIB a pris son envol, surpassant les autres types de fraudes. 49% des entreprises ciblées l'ont été par une fraude au RIB, versus 37% par une fraude au faux fournisseur et au président. D'ailleurs, le virement classique a été utilisé comme méthode de paiement pour 43% des entreprises ciblées, surpassant de loin le prélèvement SEPA (31%) et le paiement par carte (27%).

L'intensification des cyberattaques explique la propagation de la fraude au RIB. Des fraudeurs de plus en plus sophistiqués infiltrent les systèmes informatiques des fournisseurs, envoient un email de demande de changement de RIB et reçoivent les paiements à la place des fournisseurs. Une fois les systèmes infiltrés, **il est impossible de détecter la fraude sans un outil de détection automatisé** comme Trustpair. Une double défense est dés lors nécessaire : un premier rempart contre les risques cyber et un deuxième contre les effets financiers de la cyberfraude.

> **L'email d'un des fournisseurs de notre client a été piraté. Les fraudeurs ont envoyé une demande de modification de RIB par email et notre client a payé le fraudeur deux fois. La fraude a été longue à détecter : le fournisseur pensait simplement que les paiements étaient en retard. Cet exemple de fraude au virement illustre la complexité que le cyber-risque vient ajouter à ce type de fraude : dans le cas d'une fraude au RIB par cyberattaque - comme ici - il est impossible de la détecter**

Baptiste Collot
Co-fondateur et CEO
Trustpair

trustpair

#4 A l’heure de la cyber menace, l’adaptation **nécessaire** des entreprises

1

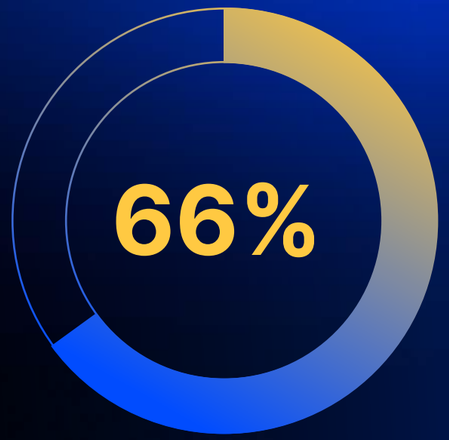
52%

des tentatives de fraude étaient liées à des cyberattaques

55%

des entreprises constatent une augmentation des cyberfraudes ces 12 derniers mois

2



des entreprises désignent le risque de cyberattaques comme leur principal facteur de vulnérabilité à la fraude

3

61%

des entreprises ciblées l’ont été par le biais d’un email de phishing

35%

par appel téléphonique

34%

par des faux sites internet

Questions & répondants :

- 1. Les tentatives de fraudes dont vous avez été victimes étaient-elles liées à des cyberattaques (c’est à dire pour laquelle le fraudeur a recours à internet ou la technologie) ? Répondants : 100
- 2. Quels sont, selon vous, les facteurs qui rendent votre entreprise plus vulnérable au risque de fraude? Répondants : 151
- 3. Quels ont été les canaux utilisés pour perpétrer ces fraudes (tentatives et fraudes abouties) ? Répondants : 100

ANALYSE

La fraude a changé de visage ces dernières années et est aujourd'hui bel et bien entrée dans une "cyber ère". En 2023, 52% des tentatives de fraude étaient liées à des cyberattaques. Plus d'une entreprise sur deux a constaté une augmentation des cyberattaques ces 12 derniers mois. Les entreprises en ont conscience : 66% d'entre elles désignent en effet le risque de cyberattaques comme leur principal facteur de vulnérabilité à la fraude.

D'une fraude manuelle gérée par des fraudeurs isolés et parfois "amateurs", nous sommes passés à **une fraude industrielle et personnalisée avec des fraudeurs hautement spécialisés**. Ils utilisent des outils de pointe - souvent basés sur l'IA et le machine-learning - et des techniques indétectables sans les protections adéquates. Les fraudeurs utilisent par exemple Chat GPT pour rédiger massivement et rapidement des emails de phishing personnalisés. 61% des entreprises ciblées par la fraude en 2023 l'ont d'ailleurs été par le biais d'un email de phishing.

Ces évolutions exigent des entreprises des réponses adaptées : **celle d'un équipement automatisé de pointe** pour faire armes égales avec les fraudeurs et d'une implication transverse des dirigeants. Certaines grandes entreprises l'ont bien compris et adoptent maintenant une approche "décentralisée" avec des responsables de sécurité informatique dans chaque unité business.

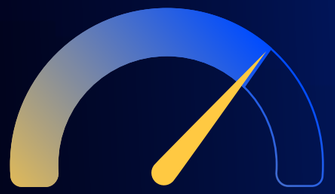
trustpair

> **Le phishing, ce n'est plus un fraudeur seul qui fait des fautes d'orthographe, utilise des anciens logos ou des designs douteux. Finalement aujourd'hui, c'est presque du "Phishing-as-a-service". Des cybercriminels très organisés proposent des solutions clés en main - souvent basées sur l'IA et le machine learning - pour commettre des fraudes et générer des emails de phishing très personnalisés et "performants". Ils prennent un pourcentage des revenus.**

Slim Trabelsi
Senior Security Architect
SAP

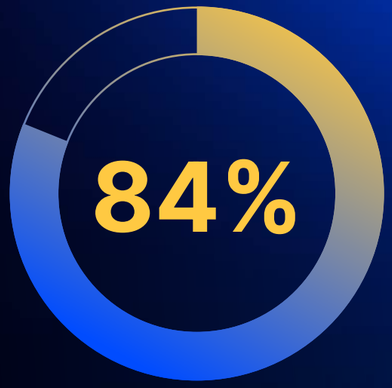
#5 **Risques cyber :** les entreprises à l'heure de la **prise de conscience**

1



Les entreprises évaluent leur maturité en matière de cybersécurité à 7,1/10

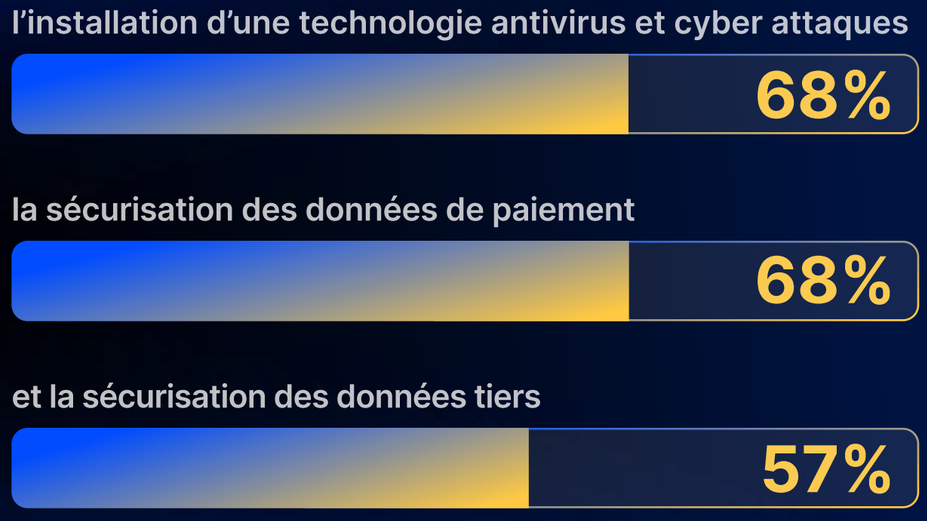
2



des entreprises ont déjà reçu ou vont recevoir une ou plusieurs formations pour détecter et prévenir les cyberfraudes

3

Dans les 12 derniers mois, les entreprises ont investi dans :



Questions & répondants :

- 1. Sur une échelle de 1 à 10, comment évaluez-vous la maturité de votre entreprise en matière de cybersécurité ? Répondants : 151
- 2. Est-ce que votre entreprise a reçu une ou plusieurs formations pour détecter et prévenir les cyber fraudes ? Répondants : 151
- 3. Au cours des 12 derniers mois, dans quels domaines votre entreprise a-t-elle investi en matière de cybersécurité et de processus financiers ? Répondants : 151

ANALYSE

Les entreprises sont de plus en plus sensibles aux risques cyber. Elles évaluent d'ailleurs leur maturité en matière de cybersécurité à 7,1/10. Rien d'étonnant quand on voit que 84% d'entre elles ont déjà reçu ou vont recevoir une ou plusieurs formations pour détecter et prévenir les cyber fraudes.

Mais si des formations régulières sont nécessaires pour comprendre les dernières méthodes et techniques, **elles ne sont pas suffisantes pour contrer la sophistication des cyber fraudeurs**. Les entreprises semblent l'avoir compris puisque 68% d'entre elles ont investi dans une technologie anti virus et cyberattaques dans les 12 mois. L'objectif ? Combattre à armes égales et s'équiper d'une technologie plus avancée que les fraudeurs.

> Il est maintenant possible de générer des visuels et des voix via l'IA. Avec l'échantillon de voix de quelqu'un on est capable de leur faire dire tout ce qu'ils veulent. Cela permet de faire des attaques de phishing vocales comme la fraude au président par exemple. Le fraudeur manipule la voix du dirigeant puis laisse un message sur WhatsApp en demandant à un employé aux accès suffisant de faire certaines actions. La détection sans outil est quasiment impossible.

Slim Trabelsi
Senior Security Architect
SAP

trustpair

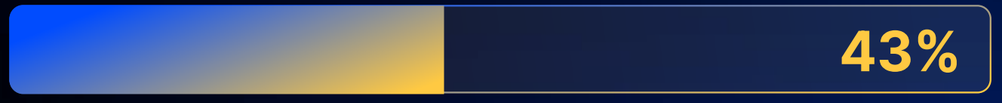
#6 Face à ces défis, les lacunes de la lutte anti-fraude

1

Parmi les mesures de protection contre la fraude, les entreprises privilégient :

la formation des équipes à la fraude

devant la vérification systématique des données tiers



et une bonne collaboration entre les équipes procurement, finance, trésorerie et IT

2

47%

des entreprises (47%) réalisent un contrôle continu tout au long de la chaîne de paiement

3

Les moyens de contrôle privilégiés par les entreprises en cas de modification de données tiers sont les emails de vérification (51%) et les appels téléphoniques (49%)

Questions & répondants :

- 1. Dans votre entreprise, quelles sont les mesures de protection déjà mises en place contre la fraude ? Répondants : 151
- 2. A quel moment dans le processus de paiement des factures fournisseurs vérifiez-vous les informations bancaires de vos fournisseurs ? Répondants : 151
- 3. Quelles méthodes utilisez-vous pour contrôler les coordonnées bancaires de vos tiers ? Répondants : 151
- 4. Combien de temps les contrôles vous prennent-ils par RIB ? Répondants : 151

ANALYSE

Si les entreprises ont conscience du risque cyber, elles restent **insuffisamment équipées contre la fraude**, privilégiant des méthodes de lutte traditionnelles. 55% d'entre elles privilégient en effet la formation des équipes comme mesure de protection contre la fraude, devant la vérification systématique des données tiers (48%). Une vérification continue est pourtant nécessaire pour s'assurer que les paiements sont envoyés aux bénéficiaires légitimes et pas à des fraudeurs.

Face à l'envol de la fraude au RIB et des cyberattaques, il est essentiel de **contrôler en continu les données fournisseurs** et pas uniquement lors d'évènements spécifiques (demande de modification, entrée en base, etc.). Pourtant, moins d'une entreprise sur deux réalise un contrôle tout au long de la chaîne de paiement. En cause ? Le manque de ressources, de temps et d'outil dédié qui rendraient la tâche plus efficace.

De plus, les contrôles s'effectuent encore de manière très manuelle : les moyens privilégies sont les emails de vérification pour 51% des entreprises et les appels téléphoniques (49%). Pour plus d'une entreprise sur deux, un contrôle de RIB dure moins de 15 minutes. Ces **méthodes manuelles ne peuvent pas faire face à la sophistication croissante de fraudeurs** qui s'appuient sur des technologies de pointe. Seul le recours à des solutions de prévention automatisées comme Trustpair pourra éradiquer le phénomène.

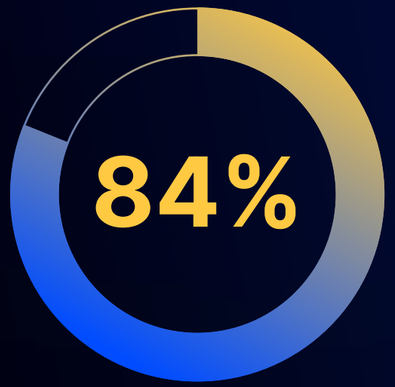
trustpair

> **Une des raisons au manque d'équipement des entreprises est un manque de connaissance de ce qui existe sur le marché. Il y a aussi la question de la bande passante et de la priorisation du projet anti-fraude par rapport aux autres projets. La transformation numérique est déjà coûteuse en termes de budget et de ressources.**

Baptiste Collot
Co-fondateur et CEO
Trustpair

#7 2024 : entre appréhension et approche proactive

1



des entreprises ont déjà reçu ou vont recevoir une ou plusieurs formations pour détecter et prévenir les cyberfraudes

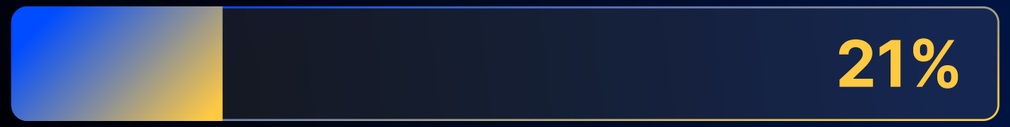
2

44%

des entreprises utilisent déjà un outil de contrôle automatisé contre la fraude

3

d'entre elles sont en phase avancée d'un projet anti-fraude et...



étudient le sujet pour 2024

Questions & répondants :

- 1. Pensez-vous que la fraude va augmenter dans les 12 prochains mois ? Répondants : 151
- 2. Quelles méthodes utilisez-vous pour contrôler les coordonnées bancaires de vos tiers ? Répondants : 151
- 3. Et votre entreprise a-t-elle entrepris un projet de lutte contre la fraude au virement pour 2024 ? Répondants : 151

ANALYSE

Face aux nombreux défis posés par une fraude plus complexe et digitale, les entreprises sont pessimistes. 83% d'entre elles anticipent une **augmentation des tentatives de fraude dans les 12 prochains mois**. Leurs craintes sont loin d'être infondées. Les fraudeurs ont plusieurs longueurs d'avance et cela restera le cas si les entreprises ne s'équipent pas d'outils suffisamment performants pour leur faire face.

Heureusement, certains signaux sont positifs. 44% des entreprises utilisent déjà un outil de contrôle automatisé pour vérifier les données bancaires de leurs fournisseurs et 56% d'entre elles sont déjà en phase avancée d'un projet anti-fraude. 21% étudient le sujet pour 2024. Ces chiffres soulignent une **volonté de prendre le contrepied de la menace** et d'adopter une approche proactive pour 2024.

> Les anciens process sont trop lents pour intercepter les attaques. L'avenir de la lutte contre la fraude, c'est l'automatisation et l'IA. Elles seules sont capables d'identifier les fraudes et de corriger les vulnérabilités. Il faut automatiser au maximum pour allouer plus de ressources humaines aux cas les plus difficiles et sensibles.

Slim Trabelsi
Senior Security Architect
SAP

trustpair

Synthèse

Face à l’escalade de la fraude, les entreprises françaises sont à un carrefour décisif. Les fraudeurs utilisent des schémas de plus en plus sophistiqués et des outils qui s’appuient sur des technologies de pointe. Pour les dirigeants financiers, adopter des solutions automatisées et une approche transversale pour combattre la fraude est une nécessité.
Si certains signaux sont positifs - formations à la cybersécurité, augmentation du budget - une partie considérable des entreprises s’appuient encore sur des méthodes manuelles de prévention, largement insuffisantes face à une fraude entrée dans une “cyber ère”. 2024 doit être l’année du tournant : celui vers des mesures de sécurité plus proactives et automatisées.

> **La fraude est désormais complètement entrée dans l'ère digitale. Nous avons assisté au passage de la fraude manuelle à la fraude numérique : c'est désormais chose faite. La fraude est une industrie : une industrie mature et équipée, avec des organisations de fraudeurs spécialisées.**

Baptiste Collot
Co-fondateur et CEO
Trustpair

Ce Rapport 2024 a été crée en collaboration avec :

trustpair

En savoir plus

SAP

En savoir plus

opinionway

En savoir plus

trustpair

Secure B2B payment, goodbye fraud.

Trustpair est la plateforme leader mondiale de la prévention contre la fraude au virement pour les grandes entreprises. Notre solution vous accompagne dans la gestion de vos risques tiers grâce à un contrôle continu des données fournisseurs.
La plateforme permet une gestion systématique et intuitive du risque de fraude, en cohérence avec les outils et process existants. Trustpair s'intègre aux principaux outils métiers - ERP, TMS, Portail d'Achat.

Avec la plateforme, plus de 200 Directions financières ont déjà éradiqué la fraude au virement.

Parlez à un expert