8 conseils pour éviter la fraude dans votre entreprise

WHISTLEBLOWER PARTNERS

La fraude d'entreprise est un problème majeur qui se développe au rythme de la mondialisation, de la numérisation et d'une plus grande complexité dans de nombreux domaines, tandis que le coronavirus a exacerbé le problème.

La fraude au sein des entreprises est un problème plus important que ce que beaucoup de gens pensent. Une entreprise peut perdre jusqu'à 5 % de ses recettes annuelles à cause de la fraude interne. C'est ce qu'ont montré des études internationales. Les entreprises danoises connaissent également une forte augmentation de la cybercriminalité financière, qui consiste à inciter les employés à verser de l'argent à des criminels externes.

Le contrôle est manifestement essentiel, mais même si les outils d'audit permettent d'aller loin, la solution n'est pas aussi simple. Une bonne culture de travail est tout aussi importante : les employés sont encouragés et incités à faire les bons choix afin de ne pas commettre d'erreurs intentionnelles ou involontaires qui peuvent coûter cher à l'entreprise.
Depuis que l'épidémie de COVID-19 nous a frappés, le travail à domicile est devenu la nouvelle normalité, et cette tendance devrait se poursuivre. Cela a également créé de nouveaux risques pour les entreprises.

Voici quelques points à connaître en matière de fraude d'entreprise :

1. **Contrôle et sensibilisation accrus aux procédures dans l'entreprise**

La diminution des effectifs au bureau pourrait induire un assouplissement des procédures en interne afin que le quotidien se déroule sans encombres. Les mots de passe peuvent être partagés entre collègues, et il existe un risque que ce soit la même personne qui approuve les factures, modifie les coordonnées des créanciers et approuve les paiements.
Cela offre des possibilités évidentes de fraude financière qui permettent au fraudeur de couvrir ses traces. Si cela se fait de manière modeste sur une longue période, la fraude peut prendre une ampleur considérable avant d'être – peut-être – détectée.
Les entreprises ne doivent donc pas relâcher les procédures en interne, même si les employés travaillent de plus en plus individuellement depuis leur domicile, et doivent constamment « réguler » leurs activités de contrôle en fonction du risque.

2. **Forte sensibilisation au piratage, au hameçonnage (phishing) et autres escroqueries informatiques**

Les criminels tentent de plus en plus souvent de persuader les entreprises par la ruse à communiquer des informations ou des codes personnels au moyen d'appels téléphoniques (vishing), de SMS (smishing) ou d'e-mails (phishing). Le fraudeur se fait souvent passer, par exemple, pour un représentant de la banque de l'entreprise ou d'un partenaire commercial, des autorités publiques, de NemID ou de Nets.

Certaines entreprises se font directement pirater leurs systèmes de messagerie électronique, tandis que d'autres fraudeurs utilisent le phishing, par lequel un clic sur un lien ou un fichier dans un faux courriel peut donner accès aux systèmes informatiques de l'entreprise.
Il est très important de bien faire comprendre aux employés qu'ils doivent être sceptiques face à des contacts non sollicités ou des e-mails qui semblent inhabituels ou étranges, et qu'ils ne doivent jamais donner d'informations ou de codes personnels. En cas de doute, chaque employé doit toujours contacter le service informatique de son entreprise : mieux vaut trop vérifier que pas assez.

3. **Éviter la fraude au PDG**

La fraude au PDG consiste à amener un employé par la ruse à payer une fausse facture ou à effectuer un virement non autorisé du compte de l'entreprise vers un compte appartenant au fraudeur. Le fraudeur se fait passer pour un cadre supérieur de l'entreprise en question.
Il est important d'instaurer des procédures au sein de l'entreprise pour le paiement des factures et les transferts de fonds, et de s'assurer que toute demande inhabituelle est vérifiée, quelle que soit l'urgence d'un e-mail demandant le virement. Un appel téléphonique au PDG peut souvent révéler toute la fraude et sauver l'entreprise de pertes importantes.

4. **Éviter la fraude à la facture**

Dans le cas de la fraude ou de l'arnaque à la facture, le fraudeur prétend représenter un client ou un fournisseur de l'entreprise et demande que les futures factures soient payées sur un nouveau compte bancaire – appartenant au fraudeur.
Il est important de veiller à ce que les employés concernés soient informés et sensibilisés à ce type de fraude et aux moyens de l'éviter. Il est donc essentiel de demander au personnel chargé de payer les factures de toujours les vérifier pour détecter les irrégularités, d'établir des procédures fixes pour le traitement des paiements manuels et de vérifier la légitimité des demandes de paiement.
Il est avantageux d'utiliser un système de paiement automatisé afin de limiter au maximum le nombre de paiements manuels.

5. **Sensibiliser aux fraudes liées aux changements de coordonnées bancaires (arnaque aux faux RIB)**

Il est important d'être conscient de l'existence d'une fraude liée aux changements de coordonnées bancaires et de s'assurer que cette connaissance est partagée avec les fonctions au sein de l'entreprise qui peuvent en être des victimes potentielles.
Si l'entreprise reçoit un e-mail concernant un changement de coordonnées bancaires, il convient de toujours contacter le fournisseur pour qu'il confirme la véracité du changement auprès de l'interlocuteur habituel de l'entreprise.

6. Éviter la fraude à la TVA

Il existe un risque important d'exposition des entreprises à la fraude à la TVA lorsqu'elles opèrent, sous la forme de carrousels à la TVA. Les carrousels à la TVA se caractérisent par l'échange de biens ou de services au-delà des frontières nationales. En général, les biens sont échangés par l'intermédiaire d'un homme de paille qui ne déclare ni ne comptabilise la TVA lors de la revente des biens. Ces derniers sont ensuite échangés par un ou plusieurs intermédiaires avant d'être à nouveau envoyés hors du Danemark et de continuer le carrousel.
Ces intermédiaires peuvent être de véritables entreprises danoises. Cela signifie que les entreprises danoises peuvent facilement se retrouver dans un piège qui peut entraîner des pertes financières, par exemple sous la forme de pertes de déductions de TVA, de marchandises invendables, d'une mauvaise réputation ou de concurrence déloyale dans le secteur. Dans certains cas, un marché entier peut être miné avant que la fraude ne soit détectée.
S'il y a le moindre doute sur le fournisseur ou sur les marchandises que l'entreprise achète, vous devez éviter de conclure l'affaire. Et il est recommandé de toujours vérifier si les entreprises avec lesquelles l'entreprise fait du commerce sont enregistrées à la TVA. Pour ce faire, l'entreprise fait une recherche sur les numéros de TVA du fournisseur.
Le site Web de SKAT énumère également un certain nombre de points spécifiques à prendre en compte lors de l'achat et de la vente de marchandises.

7. Se méfier des imprimantes

Les imprimantes dans les entreprises peuvent représenter un risque important pour la sécurité si la prudence n'est pas de mise.

L'évolution de la technologie des imprimantes, notamment le fait qu'elles contiennent les mêmes composants matériels qu'un ordinateur, tels qu'un lecteur, un panneau de commande et un clavier, signifie que les entreprises doivent protéger les imprimantes contre les attaques de la même manière qu'elles le font pour les PC. Cet aspect est souvent négligé, même si les entreprises danoises sont généralement très conscientes de la cyber-menace.

8. Contacter la banque et signaler la fraude ou la tentative de fraude à la police

Si la fraude a été commise par l'intermédiaire de la banque de l'entreprise, celle-ci doit toujours être contactée en vue de récupérer le montant. De même, contactez toujours la police en cas de fraude ou de tentative de fraude, même si vous n'en avez pas été réellement victime. N'oubliez pas de conserver les documents et de les inclure dans la déclaration à la police.