ePaper

La fraude, un danger qui rôde et menace sournoisement toute entreprise

Soyez sur vos gardes face à ces 7 formes de fraude

GRAYDON
open in business

La fraude, un danger qui rôde et menace sournoisement toute entreprise

Toute entreprise peut être victime de fraude. Il y a quelque temps, la multinationale du divertissement, Studio 100, s'est ainsi retrouvée dans l'œil du cyclone : des flux de factures fictives, ayant permis à l'ancien directeur de subtiliser des millions d'euros, ont alors été mis à jour. La fraude du personnel n'est que l'une des formes d'escroquerie, mais c'est le type de fraude interne le plus courant.

Cependant, l'origine de la fraude est le plus souvent extérieure à la société. Aujourd'hui, les escrocs profitent de la très grande disponibilité des informations en ligne pour infiltrer silencieusement une entreprise. Ils deviennent aussi de plus en plus téméraires et créatifs. La fraude au CEO, une forme d'escroquerie numérique, dans le cadre de laquelle un collaborateur occupant une position stratégique joue inconsciemment le rôle de complice, devient de plus en plus fréquente.

On pourrait penser que seules les grandes sociétés et multinationales ont du souci à se faire, comme si leur taille empêchait leur transparence et ouvrait ainsi la porte aux escrocs, mais rien n'est moins vrai. De plus en plus de PME aussi sont la proie de personnes malintentionnées, provoquant des dommages financiers pouvant avoir des conséquences particulièrement désastreuses. Des années de fraude ininterrompue peuvent même entraîner la mort d'une société.

L'inventivité des escrocs semblant sans limite, un cynique pourrait décrire la lutte contre la fraude comme un combat perdu d'avance. Mais bien qu'il y ait un fond de vérité là-dedans, de nombreuses mesures peuvent heureusement être prises pour couper l'herbe sous le pied des fraudeurs. La vigilance et d'autres mesures permettent de limiter considérablement les risques.

Cet e-paper explique les différentes formes de fraude. Il évoque également les différentes mesures que l'entreprise peut prendre pour détecter la fraude à un stade précoce ou, mieux encore, la prévenir.

1

Fraude du personnel

Récemment, une entreprise belge a réalisé qu'en six ans, elle avait payé pour 1,2 million d'euros de factures de mazout. Une belle somme, d'autant plus étonnante que l'entreprise n'avait pas consommé une seule goutte de mazout pendant toutes ces années. C'était un collaborateur qui avait fait approuver ces fausses factures pendant tout ce temps. Tout comme chez Studio 100, des factures fictives avaient permis à un ancien collaborateur de faire disparaître des millions d'euros.

La fraude du personnel est une forme d'escroquerie peu connue auparavant, mais qui est aujourd'hui sous le feu des projecteurs. Comment un collaborateur réussit-il à subtiliser des millions à son employeur ? C'est la question qui se pose à chaque fois qu'un cas de fraude à grande échelle est mis à jour. Dans le passé, les entreprises étaient surtout vigilantes vis-à-vis de la fraude externe, comme la criminalité internet. Parce qu'elles avaient confiance dans leur personnel, elles étaient convaincues qu'elles ne devaient pas craindre la fraude interne et sous-estimaient ainsi gravement les risques.

Une étude a révélé que l'absence de trois facteurs peut pousser un collaborateur à la fraude : l'occasion, l'intention et le manque de contrôle. Ce n'est pas par hasard que les fraudes sont les plus fréquemment commises par des collaborateurs du département financier, de la comptabilité ou du contrôle interne. Dans la plupart des cas, ils ont fait un beau parcours sur l'échelle de l'entreprise. Car : plus vous montez dans l'organigramme d'une société, plus vous vous rapprochez de l'argent. Et plus vous avez vue sur les différents mécanismes de contrôle et de sécurité.

Ces collaborateurs fraudeurs virent intelligemment de l'argent sur un autre compte, sur lequel ils ont un contrôle direct ou indirect. Ils commencent toujours 'petit'. Ils détournent d'abord des sommes relativement négligeables. Lors des transactions suivantes, ces sommes augmentent progressivement. Tant que la fraude n'est pas détectée et que personne ne pose de question, ces pratiques se poursuivent inexorablement. Mais l'appât du gain pousse le fraudeur à en faire toujours plus. Jusqu'à ce que la somme soit devenue trop importante pour rester inaperçue.

1 Fraude du personnel

Dans la plupart des cas, la sanction se limite à un licenciement pour faute grave. C'est la procédure la plus rapide. De nombreux employeurs renoncent à une plainte au pénal parce que la procédure est trop longue et que l'affaire serait ainsi rendue publique. Si l'employeur choisit quand même d'aller en justice, la chance qu'il récupère le montant détourné peut être totalement nulle. Car les fraudeurs internes ne sont souvent pas suffisamment solvables.

Studio 100 a choisi d'aller en justice. Le travailleur avait en effet quitté l'entreprise avant que la fraude ne soit mise à jour et la multinationale ne pouvait plus se rabattre sur le contrat de travail.

Si une telle fraude est détectée chez vous, ne vous en prenez pas au réviseur d'entreprise. S'il passe à la loupe les chiffres annuels de la société, ce n'est pas sa tâche de détecter les méfaits. Les transactions frauduleuses sont en outre réparties sur le plan comptable et intégrées ingénieusement dans les autres chiffres, de sorte que les magouillages sont très difficiles à détecter dans les chiffres.

Détail croustillant : en raison de la fonction qu'ils occupent, les fraudeurs internes sont souvent impliqués dans l'audit annuel. Ce qui rend encore plus difficile de mettre leurs agissements à jour.

Comment prévenir ce type de fraude ?

- *Une responsabilité partagée du paiement des fournisseurs est cruciale. Optez donc pour un système de double signature. Les paiements ne peuvent ainsi être effectués que lorsque deux personnes compétentes donnent leur feu vert.*
- *La culture d'entreprise est très importante. Adoptez un code déontologique condamnant sans appel la fraude, même à petite échelle.*
- *Créez un point de notification où les collaborateurs peuvent communiquer anonymement les (soupçons d') irrégularités.*
- *Faites le point du déroulement du trafic des paiements dans votre entreprise au moyen d'un petit audit interne. Vous verrez ainsi clairement qui a les compétences requises pour effectuer des versements d'argent. Et les éventuelles faiblesses du système seront ainsi mises à jour.*

2 Escroquerie numérique: de la fraude au CEO à l'exaction

L'époque où les pirates ne ciblaient que d'obscures entreprises internet est définitivement révolue. De plus en plus souvent, ils frappent des PME belges. En 2015, le nombre de fuites de données a augmenté de 10% par rapport à l'année d'avant. L'assureur Allianz a calculé que le cyber-crime lui coûte chaque année quelque quatre cents millions d'euros. Le plus inquiétant, c'est que les escrocs deviennent de plus en plus ingénieux dans leurs méthodes pour subtiliser de grosses sommes aux entreprises.

Cyber-fraude

La fraude au CEO est une méthode particulièrement ingénieuse, et en pleine expansion. C'est une forme de fraude numérique, également appelée cyber-fraude – où les pirates visent et manipulent le maillon le plus faible du réseau informatique d'une entreprise : l'être humain. Ils approchent les collaborateurs afin de leur faire communiquer des informations sensibles ou entreprendre inconsciemment des actions dommageables pour l'entreprise. Les escrocs opèrent non seulement de manière très sécurisée, mais ils profitent aussi de la disponibilité accrue d'informations en ligne pour s'infiltrer dans une entreprise.

Un exemple concret pour illustrer l'inventivité de leur méthode :

Le collaborateur financier d'une multinationale reçoit un e-mail personnel du CEO. Ce dernier lui demande sa collaboration pour un deal important. Il s'agit d'une reprise à l'étranger qui doit rester secrète pour l'instant. Pour pouvoir conclure le deal, il faut libérer rapidement - et discrètement - une somme de 500.000 euros. Le collaborateur se sent flatté par la confiance que lui témoigne le CEO. Sans poser de questions, il verse le montant sur le compte indiqué. Et c'est seulement quelques semaines plus tard qu'il s'avère qu'il n'a jamais été question de reprise.

Sachez que les pirates ne laissent rien au hasard. Grâce aux informations sur les réseaux sociaux, aux organigrammes disponibles en ligne ou aux données sur le site web de l'entreprise, ils savent exactement comment se déroulent les procédures de paiement d'une entreprise donnée. Ils savent ainsi qui a la compétence pour transférer de grosses sommes d'argent. Mais ils apprennent également à connaître le style de communication de l'entreprise. Ils parviennent, à l'aide d'une fausse adresse e-mail, à se faire passer de manière parfaitement crédible pour le CEO ou un autre membre de la haute direction.

2 Escroquerie numérique: de la fraude au CEO à l'exaction

La fraude au CEO est probablement née en France, où des bandes ont ainsi jusqu'à présent réussi à escroquer de cette façon plus de trois cents entreprises. Au total, elles ont détourné une somme de 250 millions d'euros. Plusieurs cas sont également connus en Allemagne et aux Pays-Bas entre-temps. Notre pays n'y échappe pas non plus. Dans les cercles judiciaires, il se dit que plusieurs dizaines d'entreprises belges sont victimes de cette forme d'escroquerie. Les escrocs sont parvenus à détourner entre 500.000 et trois millions d'euros. Mais le nombre réel de dossiers - et donc également le butin - est sans doute plus élevé. La plupart des entreprises préfèrent ne pas communiquer à propos des pratiques qui ont permis aux escrocs de les mener par le bout du nez.

La fraude au CEO n'est pas la seule forme d'escroquerie numérique. Les pirates prennent également l'identité d'un travailleur, pour obtenir des informations sensibles et escroquer l'entreprise. Les groupes de pirates essaient aussi de subtiliser de l'argent aux entreprises au moyen de cyber-attaques : ils menacent de détruire les systèmes informatiques si les entreprises ne paient pas de grosses sommes. Ils exigent généralement des bitcoins, une sorte d'argent électronique. Au départ, ces pirates visaient exclusivement des casinos et des entreprises du secteur du bitcoin. Mais de plus en plus souvent, ils dirigent leurs flèches sur des banques, des entreprises boursières et des sociétés de paiement.

Comment prévenir ce type de fraude ?

- *Mettez en œuvre une culture d'entreprise ouverte, afin que les collaborateurs puissent s'adresser à un dirigeant pour éclaircir la situation au moindre doute.*
- *Faites le point des processus de paiement de votre entreprise, pour pouvoir mettre à jour les faiblesses éventuelles.*
- *Optez pour un système de double signature. Les paiements ne peuvent ainsi être effectués que lorsque deux personnes compétentes donnent leur feu vert.*
- *Dans le cas de la fraude au CEO interviennent souvent des personnes intermédiaires qui se font passer pour un important homme d'affaires, manager ou juriste. Vous pouvez toujours étudier le passé de vos relations d'affaires grâce à des entreprises comme Graydon. Vous saurez ainsi à qui vous avez à faire.*

3 Fraude à la facture & factures fantômes

Une forme de fraude bien connue est la fraude à la facture (appelée aussi : fraude à la boîte aux lettres). C'est un phénomène qui dure depuis un moment déjà. Les factures sur papier envoyées par la poste sont interceptées, et le numéro de compte est modifié. Ne se doutant de rien, l'entreprise paie la facture sur un compte frauduleux. Et l'argent, ainsi que les auteurs de la fraude parfois, disparaissent des écrans radar avant même que qui que ce soit ne se rende compte de quoi que ce soit. Ce genre de fraude donne immanquablement lieu à de vives discussions entre le client et le fournisseur, parce qu'il n'est pas clair si le premier a satisfait à son obligation de paiement, ou pas.

Une version numérique

La fraude à la facture connaît maintenant une version numérique. Un pirate pénètre dans le système informatique d'un fournisseur et intercepte des mails de facturation ou d'autres données comptables. Il arrive aussi qu'un système IT soit infecté par un virus. Il s'agit souvent d'un 'ver', qui permet au pirate de modifier à distance un numéro de compte dans le système ou les e-mails.

Les factures fantômes constituent une forme de fraude apparentée. Il s'agit de factures pour des produits ou services qui n'ont jamais été livrés. Dans la plupart des cas, ceux-ci n'ont même jamais été commandés. Elles sont envoyées à des sociétés qui, de par leur taille ou leurs activités, reçoivent beaucoup de factures. Il s'agit généralement de factures dont le montant est suffisamment réduit pour ne pas susciter de méfiance. Par exemple une facture de 120 euros pour le prolongement tacite d'une publication dans l'un ou l'autre guide d'entreprises. Pour nombre d'entreprises, il est pratiquement impossible de rechercher à chaque fois d'où provient la facture exactement. Et cela, les expéditeurs de factures fantômes ne le savent que trop bien.

Le Secrétariat général de l'Union Benelux a effectué une étude parmi plus de 1.100 entreprises en Belgique, aux Pays-Bas et au Luxembourg. Elle a révélé que chacune d'elles recevait en moyenne une facture fantôme par an. Les dommages financiers consécutifs sont estimés à 1 milliard d'euros par an au Benelux. Si vous êtes confronté à la fraude aux factures ou à des factures fantômes, ne manquez pas de le signaler. Vous aiderez ainsi à éviter à d'autres entreprises d'en être les victimes.

3 Fraude à la facture & factures fantômes

Comment prévenir ce type de fraude ?

- *Optez pour des factures numériques, plus difficiles à intercepter.*
- *Dans votre système comptable, associez les numéros de compte aux entreprises. Si une facture mentionnant un autre numéro de compte arrive soudainement, vous en êtes averti automatiquement dans ce cas. Prenez contact avec votre fournisseur via un numéro connu et demandez si cette modification est normale. Si vous fournisseur n'a pas changé son numéro de compte, il s'agit sans doute d'une tentative d'escroquerie.*
- *Sachez avec qui vous travaillez. Surtout s'il s'agit de vente par téléphone ou d'entreprises que vous ne connaissez pas : contrôlez le (futur) fournisseur. Vous pouvez effectuer gratuitement un tel contrôle chez Graydon.*
- *Prêtez attention aux factures mentionnant explicitement une modification de numéro de compte et la demande de payer sur un autre compte que l'habituel. En cas de doute, prenez contact avec le fournisseur.*
- *Soyez vigilant face aux factures dont les montants sont soudainement très divergents. N'hésitez pas à prendre le téléphone et à demander des éclaircissements.*
- *Soyez toujours très prudent en cas de paiement unique d'un montant important.*
- *Convenez avec vos clients habituels d'un code à mentionner sur la facture.*
- *Attirez l'attention des collaborateurs de l'administration financière sur les mentions ou données sur les factures. Comme les fraudeurs ne sont pas informés de ces accords, les factures qui n'y sont pas conformes deviendront particulièrement visibles.*
- *Dans le cas des factures fantômes, les escrocs osent parfois prendre contact par téléphone pour se donner de la crédibilité. Demandez-leur simplement un accord écrit.*

4 Abus du Moniteur belge

Une forme de fraude bien organisée utilise le Moniteur belge pour escroquer les entreprises. Via une publication officielle, l'escroc se fait nommer administrateur de l'entreprise. Pour ce faire, il imprime le formulaire standard et se fait enregistrer au greffe du tribunal du commerce comme étant le nouvel administrateur délégué. Généralement, personne ne voit que la signature des administrateurs actuels sur le formulaire est fausse.

Quelques semaines plus tard, l'escroc est mentionné au Moniteur belge comme le nouvel administrateur délégué. Dans les statuts d'une entreprise, que chaque banque peut demander, sont indiquées les personnes pouvant représenter la société. Avec un peu d'adresse, l'escroc peut prélever pas mal de capital sur les comptes sans que personne ne s'en rende compte.

Lorsque la fraude est mise à jour, le mal est déjà fait. En outre, la 'nomination' de l'escroc administrateur ne peut pas être révoquée en deux temps trois mouvements. Tout d'abord, les comptes sont bloqués. Ensuite, une nouvelle publication au Moniteur belge doit faire état du licenciement de l'escroc administrateur. Bref : c'est compliqué.

Une dizaine de chefs d'entreprise des régions de Termonde, Furnes et Anvers ont été confrontés ces derniers mois à ce nouveau type de fraude. Les tentatives des escrocs ne seraient pas tellement fructueuses pour l'instant, mais leur mode opératoire démontre à quel point il est facile de manipuler les statuts des entreprises, ce qui ne manque pas d'inquiéter. Le contrôle des publications par les greffes des tribunaux du commerce n'est pas efficace.

Et dans les Pays-Bas?

Les Pays-Bas prouvent pourtant qu'il peut en être autrement. Dans ce pays, les changements de direction ne sont pas publiés dans le Journal officiel, mais dans le Registre du commerce, comparable à la Banque Carrefour des Entreprises chez nous. Les modifications d'administrateurs doivent être transmises à la Chambre du Commerce par voie numérique et par la poste. Un système de contrôle simple, mais efficace est prévu : un deuxième administrateur doit toujours signer le formulaire et accompagner celui-ci d'une copie de sa preuve d'identité.

4 Abus du Moniteur belge

L'absence d'un tel système de contrôle n'est pas le seul handicap du Moniteur belge. À une époque de numérisation exponentielle et d'infinies possibilités de communication, il est frappant de voir que dans notre pays, les modifications et d'autres opérations soient toujours réglées via l'ancien système sur papier. Lorsqu'il est possible de publier un document contraignant uniquement sur la base d'un extrait sur papier facile à falsifier du procès-verbal du Conseil d'administration, il n'est guère étonnant que les fraudes soient nombreuses.

Comment prévenir ce type de fraude ?

- *Des entreprises spécialisées proposent des systèmes de monitoring permettant de suivre tous les changements de la direction ou des statuts. Vous êtes ainsi immédiatement informé lorsqu'un mandat est modifié. Et vous pouvez réagir directement lorsqu'il est avéré qu'il s'agit d'une tentative de fraude.*

5 Les escrocs se font passer pour des agents des instances publiques

L'une des formes de fraude les plus récentes prouve bien que les escrocs agissent avec intrépidité et témérité. Ils appellent les entreprises et se font passer pour des agents du SPF Finances. Ils proposent à l'entreprise en question d'insérer une publicité dans le 'Livret bleu' du fisc. Ils ne négligent aucune possibilité de mettre davantage de pression. Ils expliquent aux entreprises que si celles-ci ne donnent pas suite, elles se retrouveront sur la liste noire du fisc. Plusieurs entreprises de notre pays ont été approchées de cette manière ces derniers temps.

Il y a un an, l'ombudsman flamand faisait état de factures d'un faux démarcheur publicitaire utilisant le logo du Gouvernement flamand. La lettre faisait référence à « De adressengids.vlaanderen », qui n'existe pas. D'autres sociétés ont reçu une lettre leur demandant de transmettre leurs données via le site web www.fodconsumentenzaken.be. L'Inspection économique a communiqué que ce site Internet avait été créé par des escrocs.

Comment prévenir ce type de fraude ?

- *La vigilance est le maître-mot. Il importe de savoir que les services publics mentionnent toujours leur numéro d'entreprise dans leurs communications officielles. Vous pouvez facilement contrôler ce numéro dans la Banque Carrefour des Entreprises.*
- *En cas de doute, les entreprises peuvent également consulter la page Web du SPF Économie, qui reprend une liste de démarcheurs publicitaires suspects, « bien connus » de l'Inspection économique.*
- *Les services publics ne vont jamais vous menacer de vous mettre sur liste noire.*

6

Fraude à la faillite

La fraude à la faillite est une forme de fraude connaissant plusieurs variantes, mais le résultat est toujours le même : les créanciers sont abusés par des escrocs, qui s'arrangent pour que leur gouvernance d'entreprise paraisse saine ou qui magouillent avec les actifs de l'entreprise.

Dans le premier cas, on parle aussi de faillite avec préméditation. Les escrocs créent des sociétés les unes après les autres. Au fil du temps, ils ne paient plus les fournisseurs, les collaborateurs, etc. et accumulent sciemment une dette énorme. Ce n'est qu'une question de temps pour que le tribunal prononce la faillite. L'entrepreneur escroc tâche alors de se faire déclarer excusable, afin d'être exempté du paiement de ses dettes. Les créanciers peuvent alors partir du principe qu'ils ne reverront jamais l'argent qui leur est dû.

Certains escrocs n'hésitent pas à laisser au fil des ans une trace de plus d'une douzaine d'entreprises tombées en faillite. La chance, pour les entrepreneurs, de se faire dédommager, est vraiment très minime. Même lorsque les escrocs sont déclarés coupables par le juge : les parties qui pratiquent cette forme de fraude se sont arrangées depuis longtemps pour qu'il n'y ait plus d'argent pour dédommager les victimes.

Dans le deuxième cas, la fraude s'accomplit au moment où la société ne peut plus payer ses créanciers et que la faillite est inévitable. L'entrepreneur tente de cacher certains biens au curateur ou les vend - de préférence peu de temps avant la faillite officielle - pour un faible montant à un membre de la famille ou à des amis, afin d'éviter que leurs biens soient saisis pour rembourser les dettes. Dans cette situation aussi, les créanciers ne revoient pas grand-chose, voire rien du montant dû.

Comment prévenir ce type de fraude ?

- *Encore une fois, la vigilance peut éviter un scénario catastrophe. Ne travaillez pas avec n'importe qui. Soyez sur vos gardes face à ce gigantesque bon de commande qui tombe 'soudainement' du ciel.*
- *Faites-vous informer au préalable sur l'identité de vos partenaires. La personne avec laquelle vous voulez travailler est-elle vraiment à la tête de la société, ou est-ce plutôt un homme de paille ?*
- *Si le chef d'entreprise ou l'un des créateurs a été impliqué dans une autre faillite, vous devez faire attention : une étude plus approfondie est alors absolument nécessaire.*

7

Adresses à risque

Lorsqu'ils créent une société, les créateurs sont obligés d'indiquer une adresse. Pourtant, très peu d'attention est prêtée à cette adresse précise indiquée par le créateur. Bref, il peut y avoir n'importe quoi à l'adresse indiquée.

Certains entrepreneurs escrocs indiquent parfois l'adresse d'une prison, un domicile temporaire, aléatoire ou même fictif. Ou même l'adresse d'un particulier, qui ne se doute de rien. Il arrive aussi que toute une série d'entreprises suspectes soient inscrites à la même adresse à risque. Il s'agit d'une adresse connue pour avoir accueilli des fraudeurs par le passé. Plus concrètement, il s'agit d'un endroit où ont été par exemple effectuées des livraisons qui n'ont jamais été payées par le passé. Ou bien où étaient établies des entreprises ou des personnes impliquées dans une faillite frauduleuse.

Ce qui ne veut pas dire que toute entreprise établie à une adresse à risque commette automatiquement des fraudes. Certaines entreprises sont établies à de telles adresses sans le savoir vraiment. Mais l'expérience apprend que le risque de fraude est plus grand quand ont fait des affaires avec une société établie à une adresse à risque.

Comment prévenir ce type de fraude ?

- *En tant qu'entrepreneur, il importe que vous n'évaluiez pas seulement les finances de vos partenaires. Certaines données peuvent servir d'indicateurs de pratiques frauduleuses éventuelles. L'adresse d'une société est l'un de ces indicateurs.*

Conclusion

Entreprendre implique des risques. Multinationale ou PME, toute entreprise peut être la victime d'une fraude. Il importe de comprendre que le phénomène représente un danger sournois, pouvant adopter de nombreux visages. La vigilance est requise à tout moment.

La fraude peut aussi se pratiquer en interne. Lorsqu'un collaborateur subtilise des (grandes) sommes d'argent pour les verser sur son compte personnel, on parle de fraude du personnel. L'entreprise Studio 100 y a été confrontée récemment. C'est une forme d'escroquerie qui est longtemps restée dans l'ombre. Les employeurs étaient persuadés qu'ils pouvaient faire confiance à leur personnel et sous-évaluaient ainsi gravement le risque.

Mais généralement, le danger est tapi à l'extérieur de l'entreprise. La fraude externe adopte de nombreuses formes. Les escrocs profitent de la disponibilité croissante des informations en ligne pour 'plumer' une entreprise. Ils sont inventifs et téméraires, et ne laissent rien au hasard. Ils ne recherchent pas seulement des informations, des données et des organigrammes en ligne : ils apprennent aussi à connaître le style de communication de l'entreprise.

La fraude au CEO est une fraude externe qui a fait son apparition récemment. Les escrocs visent et manipulent le maillon le plus faible de la société: l'être humain. Sans s'en rendre compte, un collaborateur diffuse des informations sensibles ou entreprend une action dommageable. Les escrocs parviennent en effet, à l'aide d'un compte e-mail falsifié, à se faire passer pour le CEO ou un autre top manager et à ainsi donner l'ordre de procéder au paiement de grosses sommes, sous de faux prétextes.

Dans d'autres formes de fraude externe, des factures sont interceptées et falsifiées, ou les escrocs se font passer pour des représentants des services publics. Ils n'hésitent pas non plus à se faire nommer administrateurs délégués d'une société, par publication au Moniteur belge. Ce qui leur offre alors la possibilité de piller les comptes en banque de cette société.
Bref, les escrocs ne manquent pas d'inventivité ou de bravoure.

Pourtant, il n'y a aucune raison que vous vous laissiez décourager : vous pouvez étouffer dans l'œuf de telles tentatives de fraude.

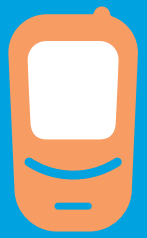
Il s'agit de ne rien laisser au hasard et de prendre les mesures requises à l'avance. Comment faire ?

- *Restez toujours vigilant.*
- *Contrôlez toujours vos interlocuteurs (clients et fournisseurs) avant de travailler avec eux.*
- *Intégrez des sécurités supplémentaires, comme par exemple un système de double signature.*
- *Misez sur la transparence et l'ouverture.*
- *Gardez le contrôle de la situation.*

Graydon propose nombre de possibilités pour mettre en pratique les points d'action précités et permettre ainsi à l'entrepreneur de faire face au danger sournois qu'est la fraude.

Envie d'en savoir plus ? Informez-vous auprès de collègues entrepreneurs pour savoir comment ils procèdent. Ou contactez l'un de nos spécialistes, qui vous conseillera, sans engagement, une approche adaptée pour prévenir toute forme de fraude.

Encore des questions?



Graydon Belgium SA
Uitbreidingstraat 84/b1
2600 Berchem

Téléphone: 03 280 88 62
E-mail: info@graydon.be