Protégez votre entreprise contre la fraude.

1 La fraude aux entreprises

Qu'est-ce qu'il y a dans ce document ?

Ce livret traite des cas les plus fréquents de fraude qui peuvent toucher votre entreprise ainsi que des conseils pour vous en protéger. Vous allez le voir, les fraudeurs sont ingénieux et très organisés. Les cas de fraude présentés ne sont pas anodins, cela arrive tous les jours dans le monde entier. Soyez vigilants.

Une information importante !
Si une fraude est quand même détectée alors que le transfert a été effectué, avertissez immédiatement votre contact chez ING afin d'essayer de faire bloquer les fonds avant qu'ils ne disparaissent.
Sachez qu'après un délai de 24 heures, il est quasiment impossible de récupérer les sommes volées.

Comment utiliser ce document ?

Nous vous recommandons de faire circuler ce document dans votre entreprise. Conseillez-en la lecture à tous les membres de la direction ainsi qu'à toutes les personnes ayant des mandats sur les comptes de l'entreprise. Ce sont souvent ces dernières qui sont ciblées par les fraudeurs.

La protection totale n'existe malheureusement pas, car la fraude est souvent liée à un facteur humain. Toutefois, si vous communiquez et appliquez dans votre entreprise les recommandations présentées dans ce livret, vous limiterez sérieusement les risques. Ce livret vous est offert à titre purement informatif par ING et n'a aucune valeur contractuelle. Par conséquent, il ne peut en aucun cas servir de base à la mise en cause de la responsabilité d'ING, notamment si, malgré ces recommandations, votre entreprise est victime d'une des fraudes décrites dans ces pages.

2 Social Engineering ou fraude au CEO

Qu'est-ce que c'est ? Quelles sont les conséquences ?

Le social engineering est le fait de récolter des informations sur une entreprise cible afin de manipuler une personne interne à cette entreprise pour qu'elle effectue une action (souvent un paiement) ou divulgue des informations confidentielles.

Comment ça se passe ?

1 Les fraudeurs contactent votre entreprise par mail ou par téléphone en se faisant passer pour des auditeurs, des experts comptables ou encore pour une autorité qui mène une enquête. Par ce biais, ils vont récupérer des informations sur les procédures de paiement internes à votre entreprises ainsi que sur les personnes qui les effectuent.

2 Ils prennent alors contact avec les employés de votre entreprise qui ont les droits pour effectuer des paiements importants en se faisant passer pour le CEO ou le CFO (souvent en déplacement dans une autre entité du groupe). Ils font état de la possibilité de racheter un concurrent étranger pour lequel il faut effectuer une importante transaction. Ils peuvent aussi invoquer un contrôle fiscal dans une autre entité du groupe nécessitant un transfert de fonds vers cette entité. D'autres scénarios sont possibles. Dans chacun d'eux, il est expressément stipulé que la transaction doit être effectuée en urgence, et que le plus grand secret doit être gardé autour de cette opération.

3 Les fraudeurs vont même parfois jusqu'à faire intervenir un cabinet de conseil externe (dont ils ont usurpé l'identité) afin de rendre l'opération plus crédible. Ce cabinet de conseil prend alors contact avec l'employé de votre entreprise pour confirmer l'opération et insister sur la confidentialité et l'urgence du paiement. Si l'employé hésite, les fraudeurs vont utiliser plusieurs ruses telles que l'utilisation de noms importants dans l'entreprise, la flatterie, voire la menace.

Comment se protéger ?

- Soyez prudent lors de toute demande de transfert de fonds urgente et secrète.
- En cas de demande urgente, toujours rappeler la personne qui a fait la demande sur un numéro de téléphone connu.
- Ne laissez jamais les dispositifs de double signature (cartes, codes PIN) aux mains d'une seule personne.
- **Autre protection :** nommez une personne de référence (qui ne soit pas le CEO ou le CFO) vers qui se tourner quand une opération confidentielle ou urgente est reçue. Cette personne pourra contacter personnellement le dirigeant de l'entreprise pour vérifier l'authenticité de la demande. Attention, cette compétence ne doit pas être connue en dehors de l'entreprise.

3 E-fraude

Qu'est-ce que l'e-fraude ? Quelles sont les conséquences ?

L'e-fraude regroupe les cas de phishing et d'infection par un malware. Cela peut toucher votre entreprise ou vous toucher personnellement dans votre vie privée.

Dans tous les cas de figure, les fraudeurs essaient de voler de l'argent en récupérant les codes d'identification et de signature électronique de leur victime. Avec ces codes, ils effectuent un transfert d'argent vers leurs comptes en vidant vos comptes bancaires.

Comment ça se passe ?

1 Vous recevez un email émanant prétendument de votre banque prétextant une vérification de sécurité, un compte qui va être bloqué ou une modification des services offerts par la banque. D'autres motifs sont possibles. À chaque fois, le but est de vous amener à cliquer sur le lien contenu dans le mail pour vous envoyer vers une fausse page d'identification à votre espace bancaire.

2 Sur cette page, vous entrez vos codes d'identification que les fraudeurs récupèrent, puisque vous êtes sur leur site et non sur le site de votre banque. Avec ces codes, ces personnes malveillantes peuvent entrer dans votre espace bancaire en ligne et préparer des transactions. Pour ce faire, il leur faut maintenant un code de signature afin de transférer l'argent à partir de vos comptes.

3 Pour obtenir ce code de signature, ils vont soit vous téléphoner et vous demander d'insérer votre carte dans votre lecteur de cartes (c'est ce qu'on appelle le vishing), soit vous verrez un écran vous demandant de patienter quelques minutes. Une fois le temps écoulé, vous verrez apparaître un nouvel écran qui vous demande le code de signature (phishing dynamique)

Comment se protéger ?

- Ne donnez jamais vos codes d'accès à qui que ce soit. Si quelqu'un vous demande de mettre votre carte dans votre lecteur et de lui donner le code qui s'affiche sur l'écran, c'est suspect.
- Ne signez jamais une transaction que vous n'avez pas effectuée vous-même (on vous demande de créer un code avec votre lecteur de carte en utilisant la touche pour les signatures, qui est différente de la touche pour l'identification, alors que vous n'êtes pas en train d'effectuer un paiement).

La bonne gestion des moyens de paiement en ligne :

Certains comportements en entreprise peuvent faciliter la tâche des fraudeurs et augmenter votre exposition à la fraude :

- **La mauvaise gestion de la double signature :** la double signature est aussi un moyen de repérer la fraude. La personne qui devra apposer sa seconde signature a un regard extérieur sur la transaction et peut détecter la fraude plus facilement. Ne laissez jamais les deux signatures dans les mains de la même personne et vérifiez ce que vous signez.
- **Le partage des accès aux comptes de l'entreprise** : il est parfois plus facile de partager l'accès à l'espace bancaire de l'entreprise. Une personne possède cet accès et laisse ses codes à ses collègues. Seulement, cela augmente les risques de fraude et ne permet pas de savoir qui a été victime des fraudeurs.
- **Le mauvais usage des mandats sur les comptes :** en partageant son accès électronique aux comptes de l'entreprise, on partage aussi ses mandats. Vous donnez aussi accès à vos comptes personnels. Chaque mandataire doit avoir son propre accès aux comptes de l'entreprise. C'est une sécurité pour l'entreprise et aussi pour la personne qui ne pourra effectuer que les comptes de votre entreprise.

4 Fraude à la facture

Qu'est-ce que c'est ?
Quelles sont les conséquences ?
Les cas de fraude à la facture sont nombreux. Dans tous les cas, les fraudeurs vont modifier les coordonnées bancaires de la société émettrice de la facture pour y faire figurer les leurs et ainsi recevoir les montants facturés.

Comment ça se passe ?

1 Les fraudeurs interceptent la facture entre le moment de l'envoi par la poste et la réception ou en hackant les boîtes mails pour les envois par courrier électronique.

2 Les fraudeurs modifient la facture afin d'y faire figurer leurs propres coordonnées bancaires. Ils peuvent le faire de différentes manières : une nouvelle facture est éditée avec de nouvelles données, un autocollant (souvent fluorescent) avec les coordonnées bancaires des fraudeurs invoquant un changement de banque est apposé sur les coordonnées bancaires réelles, etc. Puis la facture est renvoyée.

3 La facture est reçue et payée au nouveau numéro de compte. Il y a de grandes chances que les factures suivantes le soient aussi jusqu'à ce que le vrai émetteur de la facture se rende compte que ses factures ne sont pas payées et contacte la société débitrice.

Les variantes de cette fraude

Il existe plusieurs variantes de la fraude à la facture. Par exemple, la société débitrice reçoit un email de ce qu'elle croit être son fournisseur, attestant d'un changement de banque et donc de numéro de compte. Cette communication comporte l'en-tête du fournisseur et a l'air légitime. Dans ce cas-ci, il n'y a pas d'interception de facture, mais un simple message avec de nouvelles coordonnées bancaires. Toutes les factures en suspens ainsi que les factures ultérieures doivent être payées sur le nouveau numéro de compte.

Dans tous ces cas de figure, le but des fraudeurs est d'effectuer une modification dans ce qu'on appelle les données statiques du fournisseur (numéro de téléphone, références bancaires, adresse email) afin de voler de l'argent.

Comment se protéger en tant qu'émetteur de facture ?

Afin de limiter les risques d'interception de vos factures, évitez de les envoyer dans une enveloppe contenant votre logo ou tout nom pouvant identifier votre entreprise.

Il est recommandé d'envoyer chaque facture par deux moyens différents. Par exemple, par mail et par la poste. Votre débiteur devra alors être informé qu'il ne devra payer les factures que si les deux factures reçues sont identiques. En inscrivant les coordonnées bancaires en rouge sur la facture, vous facilitez la vérification avant paiement.

Comment se protéger en tant que récepteur de facture ?

Il est très simple de se protéger contre ce genre de fraude par un appel de confirmation (call back). Toute modification dans les données statiques de vos fournisseurs (adresse, téléphone, email, numéro de compte, etc.) doit faire l'objet d'un appel téléphonique au numéro usuel (et pas au numéro mentionné sur la facture). Ainsi, les tentatives de fraude peuvent être rapidement détectées.

5 Qui contacter en cas de doute ou de fraude ?

- Votre Relationship Manager

Ou l'adresse email générique :

- cs.fr@ing.com

Si vous constatez une tentative de fraude ou si une fraude a eu lieu dans votre entreprise, contactez immédiatement votre contact ING. En alertant votre banque rapidement, vous augmentez les chances de récupérer les sommes détournées.

D'autres formalités envers les autorités peuvent être aussi nécessaires (porter plainte à la police, etc.). Nos spécialistes peuvent vous conseiller sur les démarches à accomplir.