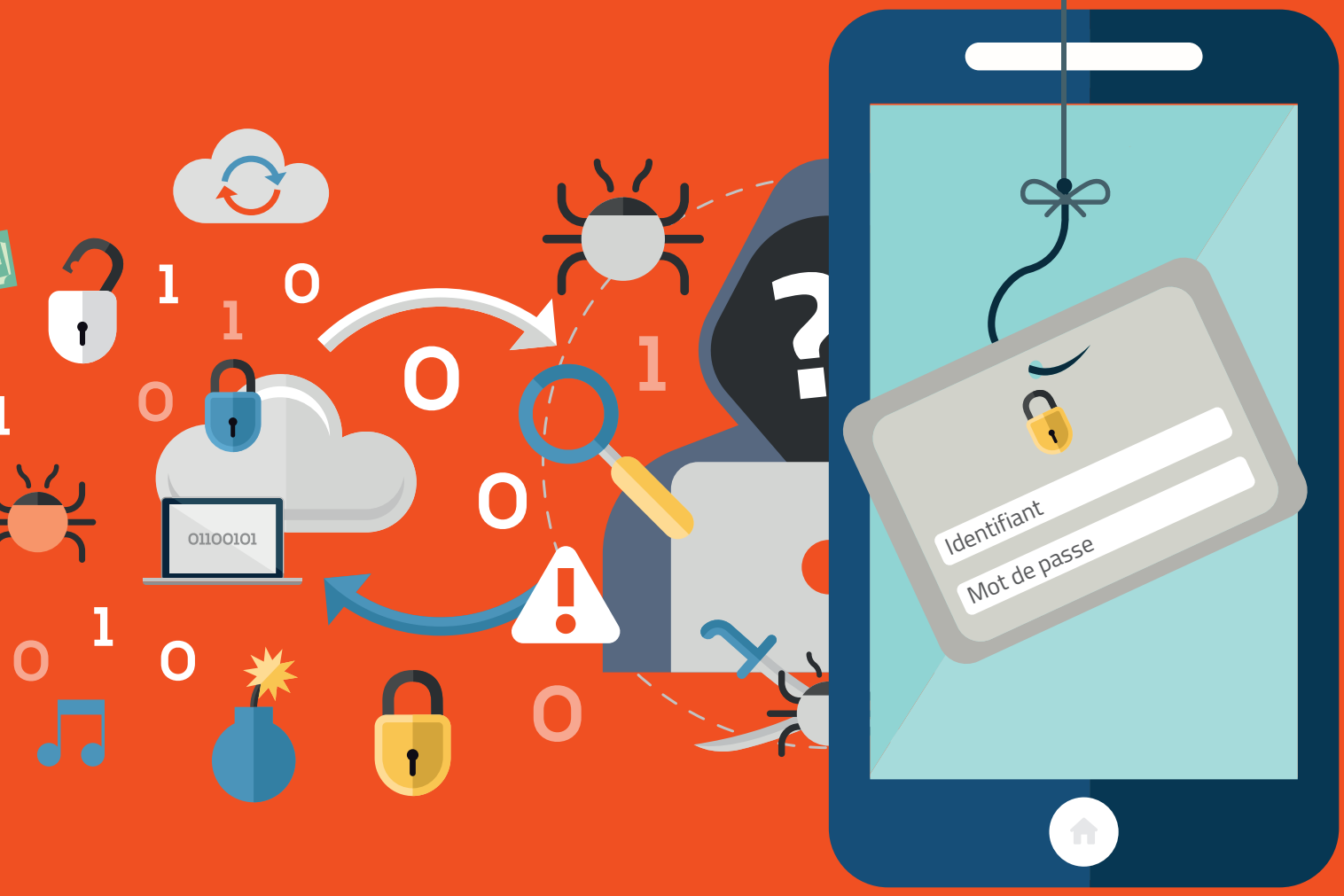
LES ENTREPRISES, VICTIMES D'ESCROQUERIES AU PAIEMENT : COMMENT SE PRÉMUNIR ?



expert-comptable conseil fiscal iec
BeExcellent.be!
ucm
BIBF IPCF
unizo
VERSTERKT ONDERNEMERS
Institut des Réviseurs d'Entreprises
Institut Royal
febelfin
VBO Verbond van Belgische Ondernemingen | FEB Fédération des Entreprises de Belgique
isabel
beyond banking

Les entreprises sont de plus en plus souvent confrontées à diverses formes d'escroquerie au paiement. Celles-ci sont organisées au niveau international et structurées sur la base de véritables *business models* attestant d'une connaissance préalable approfondie des entreprises visées. Connaissance acquise généralement sur internet et via les réseaux sociaux.

C'est pourquoi la FEB, l'UNIZO, l'UCM, les banques, les professions économiques et la Police judiciaire de Bruxelles (NIFO – *National and International Fraud Office*) unissent leurs forces dans la lutte contre ce fléau susceptible de toucher toutes les entreprises.

Les conséquences de ces arnaques peuvent être dramatiques, tant au niveau de l'impact financier pour l'entreprise, qui a peu de chances de récupérer les sommes transférées à l'étranger, qu'au niveau de l'impact humain pour l'employé, qui n'a pas vu venir l'arnaque et s'est laissé duper.

LES EMPLOYÉS DES SERVICES COMPTABLES ET FINANCIERS DES ENTREPRISES BELGES ABUSÉS

Les employés des services financiers, mais aussi des services informatiques et juridiques, doivent être informés de façon prioritaire. Une vigilance renforcée et un esprit critique aiguisé devraient leur permettre de repérer les scénarios des arnaques auxquelles ils risquent d'être confrontés un jour ou l'autre.

Quelques chiffres

Rien que pour l'arnaque dite « au président » (voir infra), depuis septembre 2010, 32 enquêtes ont été ouvertes à la Police judiciaire fédérale de Bruxelles, pour un montant de plus de 37 millions d'euros, dont plus de 13 millions ont été effectivement transférés sur des comptes étrangers appartenant aux escrocs, les 24 millions restants représentant des tentatives de transfert.

Pour la même période en Wallonie, les chiffres non exhaustifs qui sont connus actuellement (Marche-en-Famenne, Neufchateau, Huy, Mons, Tournai, Nivelles, Liège et Charleroi) concernent 31 dossiers pour un montant total de tentatives de 24 millions d'euros dont un peu plus de 4 millions ont été versés aux escrocs.

En Flandre, d'après les chiffres partiels connus pour l'instant (Anvers, Turnhout, Louvain, Audenarde et Halle) 8 enquêtes ont été ouvertes pour un montant de 3 millions et demi d'euros de tentatives dont près de 2 millions ont été transférés en faveur des escrocs.

Ces chiffres ne représentent que la partie visible de l'iceberg : de nombreuses entreprises, soucieuses de leur image, préfèrent ne pas révéler qu'elles ont été abusées. D'autres types d'arnaques, telles que la falsification de factures, ne sont pas incluses dans ces chiffres, faute de statistiques précises à ce sujet et en dépit des milliers de cas déjà portés à la connaissance des autorités de police.

De quelles escroqueries s'agit-il ?

Les formes prises par ce type d'escroqueries peuvent être déclinées à l'infini. Nous distinguons essentiellement deux types d'arnaques, les unes fondées sur l'usurpation d'identité et les autres sur l'interception de documents.

Une troisième catégorie d'arnaques utilisant des logiciels malveillants visant à contaminer les systèmes informatiques des entreprises (« *malware* ») est également présente.

1. Arnaques fondées sur l'usurpation d'identité, dont font partie les arnaques dites « au Président »

Ces arnaques sont parfois précédées d'une phase préparatoire. Voici quelques scénarios récurrents vous permettant de détecter une possible arnaque :

PHASE PRÉPARATOIRE

Prétexte utilisé :
l'audit et l'analyse des processus de paiement

- L'escroc contacte l'entreprise, éventuellement filiale d'un groupe international, par téléphone ou par e-mail.
- Il se fait passer pour une autorité, un auditeur ou un réviseur chargé(e) d'analyser les processus de paiement internes.
- Son objectif consiste à obtenir de la sorte des informations précieuses, telles que l'identité des personnes autorisées à exécuter les paiements.

Prétexte utilisé : le test informatique

- L'escroc prend également contact par téléphone ou par e-mail avec l'entreprise.
- Il se fait passer pour un informaticien de la société chargée de sécuriser les paiements.
- Prétextant exécuter certains « tests », il requiert de la « victime », employé au service comptable ou financier la plupart du temps, qu'elle lui communique des informations sensibles (procédures de paiement, solde des comptes, numéros de compte, etc.).

PHASE D'EXÉCUTION

- L'auteur de l'escroquerie contacte par téléphone une personne du service financier de l'entreprise visée.
- Il se fait passer pour le CEO, le CFO ou une personne de confiance de l'entreprise.
- Il exige la plus grande confidentialité par rapport à son appel.
- Sous couvert, par exemple, de contrôle fiscal ou de rachat d'une entreprise, la finalité de l'appel est toujours d'exécuter un paiement dans l'urgence.
- L'escroc exigera de la victime de contourner les procédures de paiement en place, en utilisant tantôt la flatterie, tantôt l'agressivité.

L'imposteur se montrera très persuasif, faisant intervenir un pseudo avocat dans la conversation, envoyant un e-mail à la victime depuis une adresse ressemblant à celle du président, du directeur financier, d'un avocat ou autre professionnel, et exigeant, sous un faux prétexte, la confidentialité la plus totale.

S'étant généralement bien renseigné sur sa victime avant son appel (en utilisant par exemple les données accessibles sur internet), son ascendant sur celle-ci est encore renforcé.

Isolée dans le secret auquel elle s'est laissée confiner, la victime est sous une pression maximale.

2. Arnaques fondées sur l'interception de documents et notamment de factures

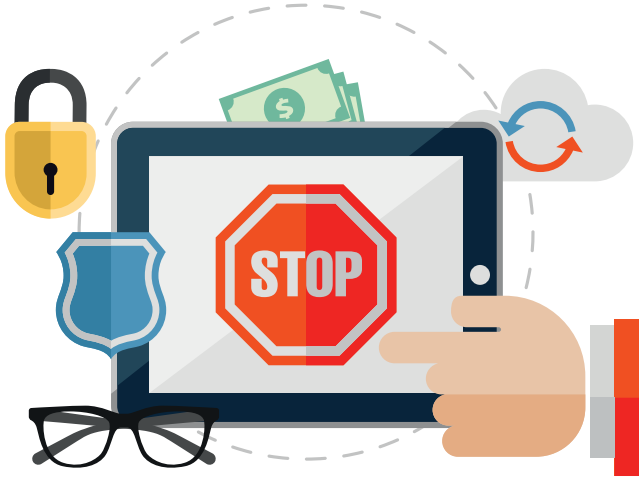
Les auteurs de cette forme d'escroquerie sont également bien organisés :

- parvenant à intercepter des factures, ils modifient le numéro de compte du bénéficiaire ;
- dans certains cas, les coordonnées de l'émetteur de la facture (numéros de téléphone ou adresse e-mail) sont également modifiées afin de dévier les éventuelles demandes d'information (visant à valider la facture) vers les escrocs eux-mêmes ;
- dans d'autres cas, les escrocs à l'œuvre prétendent que les locaux loués par la victime ont changé de propriétaire et fournissent de nouvelles – et fausses – coordonnées pour le paiement du loyer.

Lorsque le comptable croit contacter la société émettrice de la facture afin de s'assurer que le numéro de compte a bien changé, il s'entend répondre « *oui, oui, nous avons bien changé de numéro de compte* »…

3. Arnaques fondées sur des logiciels malveillants ou arnaques dites « *malware* »

Malware est le nom générique désignant toutes sortes de logiciels malveillants. Le plus souvent, ces logiciels sont installés sur un ordinateur à l'insu ou contre la volonté de son utilisateur, par exemple à l'occasion de l'ouverture d'un e-mail ou d'un lien suspect. Parvenant à voler des informations sensibles ou même à générer des ordres de paiement lors des sessions de *e-banking*, ces arnaques peuvent nuire gravement à l'entreprise qui en est victime.



Comment déjouer ces escroqueries ?

L'INFORMATION :

Pour déjouer ces arnaques, la diffusion d'une information circonstanciée à tous les niveaux de la hiérarchie de l'entreprise est primordiale.

LES PROCÉDURES ADMINISTRATIVES :

Les procédures administratives de la société doivent être conçues de manière à limiter les risques d'escroquerie, notamment par la vérification et l'approbation des factures et par le strict respect des pouvoirs de signature concernant les transferts de sommes d'argent. Ces procédures doivent être écrites et communiquées au personnel, et leur bonne application doit être régulièrement contrôlée.

PRINCIPAUX CLIGNOTANTS :

- Un **transfert d'argent inhabituel**, que ce soit en raison du motif, du montant, des circonstances, etc. ;
- Le **secret** (exigence de confidentialité, utilisation d'un code secret, demande de contacter l'interlocuteur sur son GSM ou sur son adresse e-mail privée) ;
- L'**urgence** (besoin urgent de liquidités) ;
- Toute **pression inhabituelle** afin d'obtenir une information sensible ou un paiement (prise de contact inhabituelle par le CEO ou le CFO, intervention d'un avocat) ;
- Transfert vers des **comptes bancaires étrangers** (Europe ou hors Europe) ;
- Transfert de liquidités le **vendredi** ou la **veille d'un jour férié** (rendant impossible le blocage des fonds par la banque) ;
- La **modification des coordonnées de paiement** d'un fournisseur régulier ;
- Un e-mail contenant un **lien vers le site internet de votre banque** et vous demandant d'introduire vos codes d'accès.

CONSEILS PRATIQUES POUR PRÉVENIR CES ESCROQUERIES:

- Appliquer de manière stricte les **règles de sécurité** et les **procédures** prévues pour les paiements ; respecter en particulier les règles relatives à la **séparation des tâches** et aux **pouvoirs de signature**, et ce, **en toutes circonstances**. Le système qui requiert la signature de plusieurs personnes pour les paiements à partir d'un certain montant, offre une meilleure protection ;
- **Sécurisez** suffisamment son ordinateur (e.a. via un scanner anti-virus à jour et une connexion WIFI bien protégée).

- Ne pas divulguer d'informations internes à l'entreprise (structure hiérarchique, pouvoirs, personnes absentes, liquidités disponibles, etc.) lorsqu'elles sont demandées par téléphone ou par e-mail ;
- Vérifier l'identité de **l'interlocuteur** lors du moindre soupçon ;
- Vérifier **l'origine des appels téléphoniques** ;
- Vérifier **l'exactitude des adresses e-mails, et dans le doute, les adresses IP** à partir desquelles les mails sont envoyés (www.whois.com);
- Contacter le donneur d'ordre via un **autre numéro de téléphone** ou mail que celui communiqué par l'appelant ;
- Contacter systématiquement le fournisseur lorsque les c**oordonnées de paiement** sont modifiées (attention, le numéro de téléphone sur la facture peut aussi avoir été modifié et il est parfaitement possible qu'un numéro d'appel utilisant par exemple le préfixe « 02 » parvienne en réalité à des milliers de kilomètres de Bruxelles) ;
- Redoubler de prudence lorsqu'un paiement doit être effectué sur un numéro de compte qui n'est pas encore encodé dans le **système de paiement** habituel ;
- Ne pas hésiter à vérifier les numéros de compte et de téléphone d'une société via les **moteurs de recherche d'internet** ;
- En ce qui concerne les paiements des **taxes** fédérales (par exemple la TVA), vérifier que les numéros de compte commencent bien par BExx679x... ;
- Ne pas se soumettre à la pression ;
- **Communiquer** avec son supérieur ou avec un collègue, même si la plus grande discrétion est exigée (ne pas s'isoler) ;
- Désigner une **personne de confiance** au sein de l'entreprise, vers laquelle l'employé pourra se tourner lors du moindre soupçon de fraude ;
- Ne pas ouvrir les **liens ou annexes envoyés via un e-mail** qui paraît suspect ;
- Ne jamais introduire ses **codes d'accès au système de *e-banking*** via un lien dans un e-mail vers le site internet de la banque ;
- Les pop-up vous demandant d'exécuter un « **macro** » ne doivent pas être acceptés si les e-mails desquels ils sont issus paraissent suspects.

EN CAS DE TENTATIVE D'ESCROQUERIE, IL EST TRÈS IMPORTANT

- d'en informer la **police** ;
- d'en informer les entreprises ou professionnels dont l'identité paraît usurpée ou dont les données sont falsifiées sur les factures par exemple.

SI LE PAIEMENT A ÉTÉ EXÉCUTÉ, IL VOUS FAUT IMMÉDIATEMENT :

- **Contacter votre banque** afin qu'elle s'efforce de récupérer les fonds engagés dans l'opération de paiement
- Et déposer **plainte**.

CONTACT

Police judiciaire fédérale de Bruxelles
National and International Fraud Office (NIFO)
pjfgp.bru.dirops@police.belgium.eu
InPP LECROART (02/223.93.54) et CP LECOMTE Serge (02/223.93.69)

expert-comptable conseil fiscal iec
BeExcellent.be!

UCM

BIBF IPCF

unizo
VERSTERKT ONDERNEMERS

Institut des Réviseurs d'Entreprises
Institut Royal

febelfin

VBO Verbond van Belgische Ondernemingen | FEB Fédération des Entreprises de Belgique

isabel
beyond banking